Administration for Community Living

COMMUNITY CARE HUB IT PLAYBOOK

Best Practices and Tools for Transforming Information and Technology

Administration for Community Living

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The *Community Care Hub IT Playbook: Best Practices and Tools for Transforming Information and Technology* (Playbook) is a self-guided tool on the technical and information technology (IT) infrastructure necessary for efficient service delivery and fostering interoperability between CCHs, community-based organizations (CBOs), and healthcare providers.[1]

There has long been a disconnect between the health, public health, and social care sectors, with these "worlds" having different funding and payment mechanisms, goals, metrics and reporting systems, and terminology. Over the past decade, there has been a drive toward alignment of these sectors to address social risk factors and better meet the holistic health-related social needs (HRSNs) of older adults, people with disabilities, and other populations with complex care needs. This movement has been catalyzed by technology developments, new payment and delivery system models, a drive toward health equity, and an increasing recognition by the healthcare sector that upstream, community-level social determinants of health (SDOH) (i.e., food deserts, lack of affordable housing and transportation, etc.) and downstream, individual-level HRSNs (i.e., food insecurity, housing instability, etc.) have tremendous impact on a person's health, quality of life, and mortality risks. These determinants and risks also negatively impact the cost of healthcare and the ability of at-risk individuals to remain at home where studies show they overwhelmingly prefer to be. Research conducted by the Assistant Secretary for Planning and Evaluation in 2022 demonstrates that clinical care affects only 20% of county-level variation in health outcomes, but SDOH impact as much as 50%.

This recognition has yielded increasing attention to screening and referrals for services and interventions related to HRSNs. Healthcare providers, health plans, hospitals, Accountable Care Organizations (ACOs), public health departments, and other types of healthcare organizations (collectively, "healthcare contractors") are now being measured on their efforts to screen for HRSNs across the populations they serve. Beginning in 2024, the Centers for Medicare & Medicaid Services (CMS) is requiring hospitals to report two new SDOH measures – screening for SDOH (i.e., food, housing, utilities, transportation, and safety needs) and screening positive for SDOH. CMS also issued new guidance in early 2023 to address HRSNs through Medicaid 1115 demonstration waivers and In Lieu of Services (ILOS) under Medicaid. In an effort to reduce health disparities, the Joint Commission now requires organizations seeking accreditation to screen for patients' HRSNs and provide information about community supports. Similarly, the National Committee for Quality Assurance (NCQA) has added a new social need screening and intervention measure to the Healthcare Effectiveness Data and Information Set (HEDIS), with the goal of identifying and addressing members' food, housing, and transportation needs.

These changes are bringing increased demand for the services offered by a network of community-based organizations, or community care hub (CCH). A CCH is defined as a community-focused entity that organizes and supports a network of community-based organizations providing services to address HRSNs. A CCH centralizes administrative functions and operational infrastructure, including but not limited to:

- contracting with healthcare organizations;
- payment operations;

[1] For purposes of this Playbook, healthcare providers include but are not limited to managed care organizations, accountable care organizations, hospitals, health systems and other types of provider organizations.

- management of referrals;
- service delivery fidelity and compliance;
- technology, information security, data collection, and reporting.

A CCH has trusted relationships with and fosters cross-sector collaborations of local community-based and healthcare organizations.

The Playbook focuses on the crucial aspects of IT infrastructure and technology that support CCHs in their service delivery, including data management, network and security, hardware and software requirements, interoperability, and staff training. It outlines approaches to implement and manage IT systems and processes and addresses common challenges and barriers to success. It is tailored to help stakeholders understand the advantages and processes of integrating business functions with IT solutions.

Part I of the Playbook provides a holistic understanding of how to leverage IT and shared services to enhance operational efficiency and service delivery. Part II delves into more technical details and addresses regulatory compliance, technical requirements, data requirements, and contract preparation.

Part I: Business Functions for Integration, Shared Services, and Information Sharing

Chapter 1—explores multiple dimensions of business functions supported by IT systems, beginning with program operations and reporting. This encompasses the financial aspects of IT integration, including revenue cycle management. The chapter offers a comprehensive discussion of case management systems, insights into claims processing for CCHs, and ways to integrate these systems with existing information and referral platforms.

Chapter 2—focuses on the concept of shared services and information sharing with a discussion on coordination with federally funded programs. The chapter provides tools on data collection and collaboration to better integrate with health information exchanges (HIEs) and partner more effectively with aging and disability network partners.

Part II: Compliance, Tech, and Contracts

Chapter 3—addresses compliance and regulations, beginning with an overview of federal regulations that are pertinent to IT system integration and information sharing. It provides tools, resources, and promising practices that have been effective in meeting regulatory requirements.

Chapter 4—describes technical requirements, delving into security and data privacy considerations when designing and implementing IT systems. It also discusses the elements of system architecture and infrastructure, providing a technical perspective on the foundations of IT systems.

Chapter 5—focuses on data requirements. The Playbook explains data architecture, data structure, and data standards associated with IT integration. It provides best practices for data collection and reporting, making it a valuable guide for organizations seeking to streamline their data practices.

Chapter 6—"Preparing for Contractual Relationships," discusses key considerations when entering contracts related to IT services. It outlines system architecture considerations in such contracts, ensuring that technical aspects are well taken care of in contractual agreements.

Conclusion—The Conclusion underscores the vital role of interoperability and data sharing in elevating the quality of care provided by CCHs and the aging and disability organizations they

represent. Investing in a flexible IT infrastructure that supports data sharing and is compatible with partner systems promotes a collaborative approach to foster care coordination and improve client health outcomes.

Appendix A: Glossary of Terms—provides brief definitions of terms and acronyms used throughout the document. It serves as a reference to help readers understand the terminology used in the context of the subject matter.

Appendix B: Additional Resources—includes a compilation of references and additional resources that were consulted or cited in the main document. It provides readers with the opportunity to explore further information related to value-based purchasing, HIPAA toolkits, and CCH spotlights.

Appendix C: IT System Functionality Checklist for Community Care Hubs—outlines potential features and capabilities that a CCH's IT infrastructure could have to effectively support its operations.

Appendix D: Sample Templates and Checklists—includes a collection of sample templates and checklists that can be used as reference tools or starting points for various tasks or assessments.

Appendix E: Sample IT Security Contract Terms—provides sample contract terms related to IT security.

ACKNOWLEDGEMENTS

This Playbook was developed by the Administration for Community Living (ACL), its contractors, and technical expert partners. ACL recognizes the following contributors and reviewers:

- Kelly Cronin, Administration for Community Living
- Joseph Lugo, Administration for Community Living
- Ami Patel, Administration for Community Living
- Lauren Solkowski, Administration for Community Living
- Caroline Ryan, Administration for Community Living
- Kristie Kulinski, Administration for Community Living
- Steven Verber, Administration for Community Living
- Office of Policy and Evaluation staff, Administration for Community Living
- Kazi Ahmed, FEI Systems
- Chirag Bhatt, FEI Systems
- Jay Bulot, Guidehouse
- Tim McNeill, Freedmen's Health
- Brahma Sen, Consultant
- Greg Bloom, Inform USA
- Evelyn Gallego, EMI Advisors
- Gordon Campbell, FEI Systems
- Mim Landry, FEI Systems
- Serafina Versaggi, Book Zurman
- Expert contributors from the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology (ONC) and Office for Civil Rights (OCR)

INTRODUCTION

The shift from fee-for-service to value-based healthcare is driving an increased emphasis on the roles of social, economic, and environmental conditions in improving the health and wellbeing of high-risk populations. Health-related social needs (HRSNs) are social and economic needs experienced by individuals that affect their ability to maintain their health and well-being, such as food insecurity, housing instability, transportation instability, and lack of social connection. HRSNs also directly contribute to the development and exacerbation of chronic health conditions. Healthcare organizations have been increasingly contracting with CBOs across the country to address HRSNs, often preferring to work with a central coordinating entity, or community care hub, for effective ways of coordinating aging and disability organizations that provide services to older adults, people with disabilities, and other vulnerable populations. CCHs can help identify financing sources and inform decisions regarding the best methods for screening, managing referrals, coordinating care, and delivering services across a network of aging and disability organizations. They can also ensure that referral technology platforms and workforces are utilized in a coordinated and equitable manner. CCHs can play key roles in the following:

- Coordinate funding streams from multiple payors (private and public) to develop hub infrastructure, manage a network, and finance services
- Offer a single point of contracting for CBOs of all sizes with healthcare entities
- Provide support to CBOs to implement the requirements of performance measures for value-based contracts
- Leverage trusted relationships and network members' existing assets, including workforce, service delivery expertise, and cultural competency to coordinate care in collaboration with healthcare partners
- Empower CBOs and the communities they serve to be represented at the table with healthcare providers in their communities for decision making purposes
- Coordinate community-based workforce development and training
- Identify and address gaps in service delivery by assessing community needs and evaluating the effectiveness of existing programs
- Strengthen communication and collaboration among stakeholders, including healthcare providers, CBOs, public health agencies, and community members, to ensure a comprehensive approach to improving population health.

CCHs aim to align health and social services for both individuals and communities by establishing sustainable partnerships among healthcare organizations, housing providers, public health systems, and CBOs. This often depends on the development of data and financing infrastructures to support these partnerships. This ensures that a coordinated system of health and social care is working equitably to meet an individual's needs and can help identify sources of financing to support care coordination and service delivery while ensuring equitable use of referral technology platforms and the workforce. CCH's support frequent and systemic level collaborations to help form the partnerships and hold them together over time.[2]

[2] Butler, S.M. and Maguire, M. (2022). *Building Connective Tissue for Effective Housing-Health Initiatives*. The Brookings Institute. Accessed at https://bit.ly/3nUke3c

Exhibit 1. Conceptual Model of Community Care Hub

Exhibit 1 is a conceptual model developed by Chappel et al. (2022) and captures the key roles and functions of a CCH.[3] CCHs collaborate with a wide range of CBOs to provide integrated, coordinated care and support services that address HRSNs and improve health outcomes for individuals and communities. By working together, CCHs and CBOs can create a more comprehensive and effective system of care that meets the needs of diverse populations.

These hubs coordinate federal, state, local, and private funding through braiding and blending. They often leverage resources from ACL, the Administration for Children and Families (ACF), and the Department of Housing and Urban Development (HUD) to facilitate their functions, such as coordinating access to services and supports. Other potential funding sources include hospital community benefit spending, Medicaid 1115 demonstrations, Medicare Advantage Special Supplemental Benefits for the Chronically Ill, philanthropies, employers, and municipalities. ACL focuses on supporting CCHs that align health and social services for individuals and communities, particularly older adults and individuals with disabilities.

ACL, in partnership with colleagues at the Centers for Disease Control and Prevention and other federal agencies, are accelerating efforts to develop communitywide approaches to address HRSNs and inequities through the CCH model. These efforts, in addition to existing community care hubs that area agencies on aging, aging and disability resource centers, centers for independent living, and other CBOs have developed over the last decade, are resulting in increased access to social care, including the delivery and financing of services with a culturally competent workforce that is trusted in the

[3] Chappel, A., Cronin, K., Kulinski, K. Whitman, A., DeLew, N., Hacker, K., Bierman, A.S., Meklir, S.W., Monarez, S.C., Johnson, K.A., Whelan, E-M., Jacobs, D., & Sommers, B.D. (2022). Improving Health and Well-being Through Community Care Hubs. *Health Affairs Forefront.* Accessed at: https://bit.ly/3On3Kdl

community. CCHs are partnering with healthcare organizations and coordinating funding from social services, Medicaid, Medicare, housing, transportation, and other sources to provide comprehensive services to individuals in need.

PART I:
BUSINESS SUPPORT FUNCTIONS FOR INTEGRATION, SHARED SERVICES, AND INFORMATION SHARING

Chapter 1: Business Support Functions for IT System Integration

There are a number of business processes supported by IT tools that can help CCHs manage the flow of information and enable efficient service delivery. Some key business IT functions of CCHs include managing referrals from electronic health record (EHR) systems, scheduling, integration with health information exchange systems, appointment management, billing and payment management (revenue cycle management), and reporting and analytics.

- EHR management involves implementing an electronic system for managing patients' health records, including their medical history, lab results, diagnoses, medications, and other relevant information. EHRs enable healthcare providers to access patient information quickly and easily, which can improve the quality of care and reduce errors. CCHs can either obtain role-based access to healthcare provider EHRs as necessary to ensure appropriate planning and coordination of services or receive electronic referrals from EHRs.
- Scheduling and appointment management involves implementing an electronic system for managing appointments, including scheduling, rescheduling, and canceling appointments. It can also involve managing waitlists and/or ensuring that persons are seen in a timely manner.
- Billing and payment management is another key CCH business function. This means implementing an electronic system to help with tracking charges, submitting claims, and managing reimbursements. It can also involve managing individual financial records, analyzing claim rejections and denials, and ensuring that payments are made in a timely manner.
- Health information exchange (HIE) systems can provide access to technical, legal, secure, and private exchange of health information. Integration with HIEs can offer opportunities for CCHs for connecting directly with healthcare providers for referrals, receiving alerts when someone is admitted, discharged, or transferred to or from a hospital, as well as access to data assessing the effectiveness of delivered services.

The business IT functions of CCHs are critical for enabling effective and efficient delivery of healthcare and social services. By leveraging technology to manage information and streamline processes, CCHs can help healthcare providers deliver high-quality care and improve person outcomes. Further details on program operations and reporting, value-based purchasing, revenue cycle management, cost accounting methodology, and case management system and tracking are addressed below.

Program Operations and Reporting

CCHs generally operate as a single lead entity with numerous CBOs contracted as part of their broader provider network. While both CCHs and CBOs may be responsible for various levels of reporting, the following list apply to both types of organizations. In order to effectively manage contracts with healthcare providers and other programs it operates, CCHs may need robust reporting functions to track program operations and client outcomes. The reporting functions required by CCHs will depend on the specific services and programs they provide, as well as the reporting requirements of their funders and other stakeholders.

- **Program operations tracking** Tracking program operations and monitoring program performance can help ensure that services are delivered effectively and efficiently. This may involve tracking metrics such as scheduling and service utilization, coordination of activities, efficiency in service delivery, client demographics, and program outcomes.

- **Client tracking and case management** Tracking client information and outcomes can help provide effective case management and demonstrate the impact of their programs. This may include tracking client demographics, service utilization, and client outcomes over time.
- **Grant and funder reporting** CCHs often receive funding from multiple sources, each with different reporting requirements. Tracking specific requirements of each funder, which may include data on program operations, client outcomes, and financial performance can help with efficient reporting.
- **Performance measurement and evaluation** Measuring and evaluating the impact of their programs can help CCH's improve services and demonstrate value to funders and other stakeholders. This could involve collecting data on program outcomes, conducting surveys or focus groups with clients, and analyzing data to identify areas for improvement. Additionally, it may be helpful for CCHs to prioritize quality and continuous quality improvement (CQI) as they enter into contracting relationships with health organizations. High-quality services and programs are essential for achieving positive health outcomes for community members and maintaining a strong reputation with funders. Adopting a culture of CQI within CCHs and contracted CBOs can enhance effectiveness and sustainability in the face of increasing demand for evidence-based practices.
- **Staff training and development** Tracking staff training and development data can help CCHs ensure staff members have the necessary skills and knowledge to provide high-quality services to clients.
- **Partnership development and management** CCHs often work in partnership with other organizations and agencies to provide services to clients. CCHs can leverage IT tools to develop and manage these partnerships effectively, which may involve identifying potential partners, negotiating agreements, and ensuring that partnerships are aligned with the goals and objectives of the CCH.
- **Financial management and budgeting** CCHs can leverage IT tools to help track and manage their finances effectively to provide high-quality services to clients while remaining financially sustainable. This may involve developing and managing budgets, tracking expenses, and ensuring compliance with financial regulations and reporting requirements.
- **Technology and data management** CCHs can leverage IT systems to manage data effectively and use technology to support their operations. This may involve implementing EHRs, developing data management systems, and ensuring that staff members have the necessary technology and training to use these systems effectively.

Resource Highlight

A new report, Lifting the Veil: How Networks Form, Operate, Struggle and Succeed, from the Aging and Disability Business Institute and the Scripps Gerontology Center at Miami University, shines a light on the diverse ways that networks of CBOs are operated and managed. The report shares the findings from interviews with 23 representatives of eight CBO networks—Community Care Hubs/Network Lead Entities and CBO network members.

Examples of reporting functions for CCHs can be found in various resources, including National Performance Indicators (NPIs) and the Uniform Data System (UDS) developed by the Health Resources

and Services Administration (HRSA).[4] These resources provide a standardized set of performance measures and reporting requirements that CBOs can use to demonstrate their impact and meet the reporting requirements of funders and other stakeholders. There are several software platforms and data management tools available that can help CCHs to manage their reporting functions more efficiently and effectively.

Revenue Cycle Management for Community Care Hubs

When CCHs contract with healthcare providers to deliver services to beneficiaries, it is important that the CBO understand the revenue cycle management (RCM) process and the variables that impact provider reimbursement. New billing codes and payment mechanisms for addressing HRSNs, such as community health integration (CHI) services, require CCHs that contract directly with health insurance plans or as third-party contractors to an eligible provider, should be cognizant of the revenue cycle management process and vigilant of the impact of timely filing, claim rejections, and claim denials on the revenue that is required for program sustainability.

CCHs that contract to deliver services that are reimbursable based on claims must engage with the RCM process and understand the impact of each essential step of the RCM cycle. RCM involves several processes, including billing, coding, claims submission, and insurance eligibility verification, ensuring that providers receive accurate and timely payments. In the context of CCHs, RCM plays a vital role in efficiently allocating resources and delivering care to vulnerable populations.

Overview of RCM for Community Care Hubs

CCHs serve vulnerable populations such as older adults, individuals with disabilities, and people with low incomes. Traditionally, the partners involved in developing a CCH excel in delivering quality care and services to these individuals under state and/or federal grants. Grant-based revenue management for many traditional CCH partner organizations often involves serving as many people as possible within their allocated budget. The shift from grant-based reimbursement to claims-based reimbursement requires new financial acumen. As a result, CCHs should evolve and adapt an approach to RCM that aligns with a claims-based revenue model. Implementing key aspects of RCM is crucial in for several reasons:

- **Financial Stability** Successful capture of claims-based reimbursement requires all persons involved in the delivery of reimbursable services to participate in some aspects of the RCM process. The RCM process begins with capturing and verifying accurate insurance information to ensure appropriate billing for services. When the point of care extends into the community, RCM often extends to community providers. Effective RCM ensures a steady stream of income, leads to stability, and enables CCHs to invest in improving the quality of care and expanding their range of services.
- **Operational Efficiency** A sound RCM process can streamline workflows, automate routine tasks, and reduce the administrative burden on the CCH and partner staff. It can enable all parties to focus on more critical aspects of service delivery, resulting in improved overall efficiency.

[4] Health Resources and Services Administration. (2023). Uniform Data System (UDS) Modernization Initiative. Accessed at: https://bphc.hrsa.gov/data-reporting/uds-training-and-technical-assistance/uniform-data-system-uds-modernization-initiative

- **Data-Driven Decision-Making** RCM provides valuable insights into the financial performance of CCHs and partner organizations, helping leadership make informed decisions about resource allocation, process improvements, and strategic planning.

Revenue Cycle Management: Roles and Responsibilities of the CCH

The CCH serves as the legal entity that has the contract with the healthcare provider and the ACO or MCO. As the central contracting entity, the CCH is responsible for performance on the contract terms. The CCH centralizes referral management, contract performance monitoring, invoicing, and collections. Upon receipt of collections, the CCH reconciles payment with each individual CBO that performed services on behalf of the contract.

The CCH should be actively involved in the revenue cycle management process to ensure proper invoicing for services, collections, and disbursement of payments to the CBOs in the network. The CCH holds the master contract with the payor or provider. The CCH then has a subcontract with the individual CBOs based on the terms in the master contract between the CCH and the provider.

The CCH receives the invoice from the CBO. The invoice should reflect the labor provided by the CBO staff performing services defined in the subcontract agreement. The CCH reviews the invoice from the CBOs and creates a prime contract invoice to the plan or medical provider.

KEY TERMS

- **Deductible:** A health insurance deductible is the out-of-pocket expense that must be paid by the beneficiary before a health insurance plan will cover any health insurance claims. For example, the CY2023 Medicare annual deductible for all Part B beneficiaries is $226. Therefore, every Medicare Part B beneficiary must pay $226 in out-of-pocket expenses for Part B services annually or have a Medigap plan that covers the annual deductible, before Medicare will pay for any reimbursable Part B claims. Please note the Medicare annual deductible amount can change each calendar year. Applicable deductibles, copayments, and coinsurance payments are dependent on each individual health insurance plan.
- **Copayment:** An out-of-pocket expense bore by a beneficiary for a fixed amount for services, in addition to the amount covered by an insurer. An example of a copayment is a fixed payment for Medicare Part D brand name drugs. When a beneficiary must pay $6 for each brand name drug that is covered by their Part D plan, the beneficiary is making a copayment as a fixed amount paid along with the health insurance coverage. In general, copayments are a fixed amount regardless of the reimbursable cost of the service.
- **Coinsurance:** Insurance coverage that requires the beneficiary to pay a percentage of all services covered by the health plan. For example, all Medicare Part B beneficiaries are required to pay a coinsurance of 20%. Therefore, a Medicare beneficiary that receives a Part B benefit is required to pay 20% towards the total cost of the reimbursable service. Many Medigap plans cover the cost of the Medicare Part B co-insurance. In absence of a secondary Medigap plan, all Medicare Part B beneficiaries are required to pay the 20% coinsurance every time they receive a Medicare Part B benefit. In general, coinsurance is a fixed percentage amount based on the total reimbursable cost of the services rendered.

The CCH should ensure that there is a regular review of services rendered based on the contract terms. The review should occur at least monthly and more frequently as determined. During the review, the CCH and the provider should review services rendered during the performance period, the status of claims submitted, rejections or denials for claims submitted, actual collections, the aging report for outstanding claims, and uncollectable claims. The CCH should play an active role in monitoring the fiscal performance on the contract. If there are delays in collections or if the percentage of uncollectible services increases, the fiscal viability of the contract is at risk. The CCH should communicate any potential issues of collections with the CBO and the provider. During the meeting with the provider, there should be a reconciling of services rendered with claims, and collections.

During the monthly claims reconciling meeting, the CCH and the provider should review the status of collections. For claims that are not collected, the CCH and the provider should review the steps of the revenue cycle management process to ensure that all proper steps were implemented to ensure collections. Uncollectible or delayed collections should be addressed with plans for how ongoing requests for services will be managed.

The CBO directly manages the staff assigned to provide services under the terms of the subcontract. The assigned staff should be directly managed to determine if they are meeting the expectations of the contract. This management should include weekly reviews of assigned caseloads, billable services rendered, and expense management. If the ratio of nonbillable services to billable services skews greater to nonbillable services, the viability of the contract is jeopardized. Any issues with the continued performance on the subcontract should be reviewed with the CCH, at the earliest possible moment.

RCM is vital for sustaining and scaling CCH operations and maximizing their impact. The following key components of RCM in CCHs should be considered:

- **Referral from Health Care Partner** The RCM process starts when a CCH receives a referral from a healthcare partner that includes essential information on the health insurance coverage for the person listed in the referral. This referral forms the basis for subsequent steps in the RCM process. The referral should include accurate and complete information, including demographics and insurance details, to ensure efficient billing and reimbursement. If there is incomplete or incorrect information in the referral, it is incumbent on the CCH to alert the referring provider about the noted discrepancies. It is important to note that the primary cause of initial claims rejections is inaccurate health insurance or demographic data listed on the claim. The CCH should implement a process to verify the accuracy of the demographic and health insurance information listed on the referral. Verification of the health insurance and demographic data on the referral can identify and correct errors in the information listed to prevent or reduce the percentage of claim rejections. Claims rejections have a negative impact of cashflow since rejected claims cannot be processed for payment by the health insurance plan.
- **Insurance Verification** This step involves verifying the person's insurance coverage before services are provided to ensure accurate billing and reduce the likelihood of claim rejections or denials. CCH staff should check the person's insurance plan, coverage, and benefits to determine the person's health insurance coverage requirements. Some health insurance plans require the beneficiary to pay a deductible, copayment, or co-insurance. It is the financial responsibility of the beneficiary to pay all applicable deductibles, copayments, or co-insurance payments before the health insurance plan will provide claims-based reimbursement. This step is crucial for ensuring that the person's insurance information is accurate and up to date.
- **Benefits Eligibility Verification/Collection of Copayments** This step involves verifying the person's benefits eligibility and collecting all relevant deductible payments, copayments, or coinsurance payments before services are provided. CCH staff should check the person's insurance plan, coverage, and benefits to determine the person's financial responsibility for the services provided. All relevant deductible, copayment, or coinsurance collections should occur prior to rendering any reimbursable services to the beneficiary. If the CCH is supporting a provider under a third-party contract in the delivery of reimbursable services that are billed through the provider organization, the CCH should be aware of the deductible and copayment/coinsurance collection process. Since the collections of all relevant deductible payments, copayments, and coinsurance payments must occur at the point of care, the CCH should determine the role of the CCH in supporting the healthcare provider in collecting the

required beneficiary out-of-pocket expenses. Beneficiary out-of-pocket expenses should be collected each time the CCH renders reimbursable services to a covered beneficiary. This step is crucial for ensuring that the person's financial responsibility is accurately determined and collected.

Failure to collect relevant deductible payments, copayments, or coinsurance payments threatens the financial sustainability of the CCH to deliver services. All relevant deductibles, copayments, or coinsurance requirements cannot be waived and should be collected at the point of care, prior to rendering reimbursable services to the covered beneficiary.

Scheduling Services Upon receiving a referral, CCHs should schedule an appointment for the person. Accurate and complete personal information, including demographics and insurance details, are essential for efficient billing and reimbursement. This step is crucial for ensuring that the person's appointment is scheduled accurately, and that the person's insurance information is up to date. The start date of coverage must be aligned with the date of the scheduled service. For example, if a coverage date begins on January 1, any service that is scheduled prior to the start of coverage date will not be reimbursable. Claims submitted for dates of services that occur prior to the start of coverage date will be denied. Denied claims that are uncollectable lead to bad debt that threatens program sustainability. For Medicare beneficiaries, there is the most potential for coverage changes after the Medicare open enrollment period. When services are scheduled during the open enrollment and coverage year start, it is incumbent on the CCH to verify the insurance coverage and the insurance coverage start date when scheduling services.

Documenting Services Rendered/Coding This step involves documenting the services provided to the person and assigning the appropriate codes, including diagnosis codes and procedure codes. Insurance claims use a series of codes to determine if covered services are delivered to an eligible beneficiary. The codes include ICD-10 diagnosis codes and CPT/HCPCS procedure codes. These codes must be listed on every claim. The health insurance plan will process the claims by reviewing the codes that are listed on each individual code and compare the codes with the coverage rules for the individual beneficiary. Accurate documentation and coding are crucial for submitting correct claims and receiving proper reimbursement. The documentation must define the extent of services rendered and should directly correlate with the procedure codes that are listed on the claims. The documentation must substantiate the services that are listed in the claims. For example, the community health integration (CHI) Medicare Part B HCPCS codes reimburse for an initial 60 minutes of CHI services rendered to a beneficiary to address identified HRSNs. The documentation should clearly reflect the CHI services rendered, the time spent rendering these services, and how the CHI services align with the overall plan of care. This is an example of the steps that a CCH should take to ensure that the documentation of services rendered should align with the codes listed on the claims for reimbursement. This step ensures that the person's medical record is accurate and up to date.

Charge Capture/Charge Posting This step involves capturing charges for the services provided and posting them to the appropriate individual accounts. Accurate charge capture and posting are crucial for submitting correct claims and receiving proper reimbursement. Each service rendered has an associated financial charge. The charges to each patient account are additive to provide an account balance. Capturing charges and posting the charges to the individual beneficiary account is a critical step for ensuring that the person's charges are accurately captured and posted to their account. The charge for each service should be closely matched with the reimbursement received to cover the charges. Beneficiary payments received (deductibles, copayments, or coinsurance payments) should be applied

against charge postings to beneficiary accounts. The balance after beneficiary payments should be collected against applicable insurance. Failure to collect insurance payments or beneficiary payments for services rendered causes bad debt. Bad debt threatens the financial sustainability of the CCH. If a CCH has a third-party contract with a healthcare provider and the healthcare provider fails to collect applicable charges, the financial viability of the third-party contract is jeopardized.

Timely Claim Submission/Billing Submitting claims in a timely and accurate manner is critical for receiving prompt payments. Many health insurance plans have a timely filing deadline. All claims submitted after the timely filing deadline are denied and not reimbursable. It is critically important to note the timely filing deadline for all applicable insurance plans and deploy a policy to ensure that all timely filing requirements are met. For example, Medicare has a one-year timely filing requirement. In contrast, many Medicaid policies and commercial health plans have a 90-day timely filing requirement. Billing should also be timely and accurate to ensure prompt payment. Insurance payments are reimbursement for services rendered. The CCH expends labor to deliver the service to the beneficiary. This labor expense is reimbursable to cover the cost of extending the service. Failure to promptly collect the reimbursement for the cost of labor to deliver the service negatively impacts cashflow. As a result, it is recommended that a CCH work to collect all reimbursable claims from insurance as close to the time that services are rendered as possible. Delays in filing claims threatens the financial viability of the CCH by negatively impacting cashflow. This step is crucial for ensuring that the person's claims are submitted accurately and on time.

Denial/Rejection Analysis/Resubmission CCHs should have a process for managing and appealing denied claims, including identifying the reasons for denials, correcting errors, and resubmitting claims as needed. If a CCH has a third-party contract with a healthcare provider, the CCH must participate in reviewing all rejections and denials for services rendered by the CCH network. This step involves reviewing denied claims, identifying the reasons for denials, and taking appropriate action to correct errors and resubmit claims. The electronic claim filing process includes the submission of claims to the health insurance plan's claim processing center. The claims processing system will submit a report back to the rendering provider on all claims submitted. This report will include the listing of all claims that are approved for payment, claim rejections, and claim denials. Each claim rejection and denial will have a denial code that explains the reason for the rejection or denial. The report will have an associated key that explains the definition of each rejection or denial code. The CCH should compare the rejection or denial codes with the information provided in the claim report. The CCH should review and address each rejection or denial or forfeit the reimbursement associated with the relevant claim. Failure to collect health insurance reimbursement threatens the financial sustainability of the CCH because the CCH incurred the cost of labor to deliver the service and the failure to collect reimbursement associated with that labor leads to bad debt. This step of reviewing rejections and denials, addressing rejections and denials, and resubmitting all corrected claims is crucial for ensuring that the person's denied claims are managed appropriately.

Remittance Review/Collections Posting Aging Analysis. This step involves reviewing remittance reports to ensure that payments received match the expected amounts. Health insurance plans submit an electronic remittance advice (ERA) to the rendering provider explaining the status of all claims submitted. If the CCH has a third-party contract with a provider to render services, it is important that the CCH request access to review the remittance report for all relevant claims that the CCH expended labor to provide. CCHs should also manage outstanding balances, including sending account balance statements and making collection calls to beneficiaries for all balances owed. The review of remittance advice reports should also include an analysis of timely payments or no payments for eligible services.

The CCH should track the average time to collect insurance payments by payer. Some payers will pay faster than others. Payers that pay in a timely manner are beneficial to the cashflow of the CCH. Health insurance payers that provide slow or no payment jeopardize the sustainability of the CCH. CCHs should take steps to mitigate their exposures to health plans that provide slow or no payment for eligible services rendered to beneficiaries. This step is crucial for ensuring that the person's payments are accurately recorded and that outstanding balances are managed appropriately.

Review Remittance Report with CBOs CCHs should review remittance reports with their CBO partners to ensure that payments received match the expected amounts. If the CCH has a third-party agreement with a healthcare provider, the CCH should initiate a process to review remittance reports with the eligible provider. When the CCH has a third-party contract with a provider, the remittance goes directly to the provider. The CCH should request access to the remittance from the eligible provider organization. The CCH should do their own independent analysis of the remittance advice report, even when the report is delivered to the contracted provider organization. This step is crucial for ensuring that the CBO's financial records are accurate and up to date.

Addressing Aging Report Discrepancies The aging report categorizes processed claims based on how long it takes the claim to be paid. The time between the date the claim is submitted to the health insurance plan and the payment receipt date is defined as the "Age" of the claim. The aging report outlines the age of all claims that are waiting to be paid. The general categories of an aging report are as follows:

1. Less than 30 days
2. 30 – 60 days
3. 61 – 90 days
4. 91 – 120 days
5. Greater than 120 days

CCHs should address any discrepancies found in aging reports to ensure that outstanding balances are managed appropriately. The analysis of the aging report should also include tracking slow payments that threaten the financial sustainability of the CCH. Claims that extend beyond 60 days should be flagged to determine why the claims are not paid in a timely manner. This step is crucial for ensuring that the person's outstanding balances are managed appropriately and that discrepancies are addressed promptly.

Bank Deposit Verification This step involves verifying bank deposits to ensure that payments received match the expected amounts. The remittance report should match the bank deposit verification report. If there are discrepancies between the amount the health insurance plan approves for payment and the amount that is actually paid, it is incumbent on the CCH to address the discrepancy with the payer. If the CCH has a third-party agreement with a healthcare provider, the bank deposit should occur in the verified bank account of the healthcare provider. The verification of bank deposits, in a third-party arrangement, requires the CCH to rely on the provider to provide transparent access and information to the CCH on actual collections. This step is crucial for ensuring that the person's payments are accurately recorded and that financial records are accurate and up to date.

Remit Payment to CBOs The verified bank deposits for services rendered is reimbursement for labor and materials expended to deliver services to the beneficiary. The CCH's CBO network expends the labor and

materials to deliver services to the beneficiary. The services rendered to the beneficiary should be tied to the rendering CBO in the CCH accounting system. The CCH must have an accounting process in place to match CBO expenses to beneficiary account balances. When payment is received it must be posted to the patient account. When payments are posted to a patient account, it should immediately trigger payment to the CBO that expended the labor and materials to deliver the relevant service. CCHs should remit payments received from their CBO partners to ensure that financial records are accurate and up to date. This step is crucial for ensuring that the CBO's financial records are accurate and up to date.

Restricting Scheduling of Non-Payers CCHs should restrict scheduling of non-payers or slow payers that fail to render timely payments to the CCH. The failure of health insurance plans to render payment to the CCH threatens the financial sustainability of the CCH. When a health insurance plan fails to pay claims or has significant delays in rendering payment, it is incumbent on the CCH to address the no pay or slow pay with the insurance plan to determine if an amicable resolution can be achieved. If the CCH is unable to address the no pay or slow pay with the health plan, the CCH will have to decide on restricting the delivery of services to beneficiaries covered by the plan. This step is crucial for ensuring that the CCH's financial resources are used efficiently and that services are provided only to persons who can pay for them.

Reporting and Analytics Regularly analyzing RCM data helps CCHs identify trends, track performance, and make data-driven decisions to improve their financial and operational performance. The CCH should take actionable steps based on the analysis of the reports. If the CCH has a third-party contract with a provider, the CCH should discuss the impact of the report analysis on the ability of the CCH to accept referrals for beneficiaries covered by contracted health insurance plans. This step is crucial for ensuring that the CCH's financial and operational performance is tracked.

Exhibit 2. Example of Revenue Cycle Management Process for Community Care Hubs

Revenue cycle management can be critical for the financial stability and operational efficiency of healthcare organizations and providers. By implementing effective RCM processes and systems, CCHs

can ensure that they have the resources necessary to continue providing essential services to their communities. **Exhibit 2** depicts one example of how RCM might work for CCHs.

As CCHs consider implementing a RCM program, there are several technology considerations to take into account. These technology solutions can help improve efficiency, streamline processes, and ensure seamless communication with healthcare partners:

- **EHR Integration-** EHR systems allow CCHs to store, manage, and share patient information with healthcare partners electronically. Integrating RCM processes with EHR systems can help ensure that the patient data used for billing and reimbursement is accurate and up to date, reducing the likelihood of errors and claim denials.
- **Practice Management Software-** Practice management software can help CCHs handle scheduling, registration, insurance eligibility verification, and billing. Choosing a system that integrates with EHR and RCM processes is vital to ensure seamless data flow and minimize manual data entry.
- **Electronic Referral Management Systems-** To efficiently receive and manage referrals from healthcare partners, CCHs may consider implementing an electronic referral management system. This system should allow for easy referral tracking, follow-up reminders, and communication between the referring provider and the CCH, ensuring timely access to care.
- **Medical Billing and Coding Software-** Accurate medical billing and coding are crucial for proper reimbursement. CCHs could invest in medical billing and coding software that supports the latest coding standards and integrates with EHR and practice management systems to automate charge capture and claims submission processes.
- **Claims Management and Denials Management Software-** Claims management software can help CCHs track and manage claims submissions, identify errors, and follow up on outstanding claims. Denials management software can assist in identifying reasons for claim denials, correcting errors, and resubmitting claims as needed. Integration with EHR and practice management systems is essential for a seamless workflow.
- **Patient Portal-** A patient portal can provide patients with online access to their health information, appointment scheduling, insurance information, and billing details. This can help improve patient engagement and allow for easier communication between patients and CCH staff regarding insurance coverage and outstanding balances.
- **Analytics and Reporting Tools-** CCHs could consider investing in analytics and reporting tools to gain insights into their RCM performance. These tools should integrate with existing systems to provide real-time data and enable data-driven decision-making to improve financial and operational performance.

For CCHs considering software and/or vendor solutions to assist with RCM, it is important to consider the core functionality necessary to operate, as well as additional features that may help improve communication with health systems and other partners.

RCM Considerations for CCHs

- Integration with EHRs:
  - ✓ Accurate and up-to-date patient data exchange for billing and reimbursement
  - ✓ Reduction of errors and claim denials
- Compatibility with Practice Management Software:
  - ✓ Compatibility with existing practice management software
  - ✓ Streamlined scheduling, registration, insurance eligibility verification, and billing
- Electronic Referral Management Systems:
  - ✓ Support for electronic referral management
  - ✓ Efficient receipt and management of referrals from healthcare partners
  - ✓ Referral tracking, follow-up reminders, and communication with referring providers
- Medical Billing and Coding Support:
  - ✓ Incorporation of the latest coding standards
  - ✓ Integration with EHR and practice management systems
  - ✓ Automation of charge capture and claims submission processes
- Claims and Denials Management:
  - ✓ Robust claims and denials management features
  - ✓ Integration with EHR and practice management systems
  - ✓ Improved communication with health systems and partners regarding claim submissions and denials
- Health System and Partner Connectivity:
  - ✓ Secure, efficient communication with health systems and other partners
  - ✓ Data sharing, messaging, or real-time notification features
- Analytics and Reporting Tools:
  - ✓ Comprehensive analytics and reporting tools
  - ✓ Data-driven decision-making support
  - ✓ Enhanced communication with health systems regarding financial and operational performance
  - ✓ Integration with existing systems for real-time data and insights

Please note that the RCM software considerations above are intended to serve as a starting point and include some important considerations for CCHs. However, this list is not exhaustive, and each CCH may have unique needs and requirements that should be considered when evaluating RCM software

solutions. It is essential for the CCH to conduct thorough research and consult with experts, if necessary, to ensure that they make the most appropriate decision for their organization.

Case Study

A Medicare Shared Savings Program (MSSP) ACO has participated in the MSSP program for three years without realizing any shared savings. In CY2024, the MSSP ACO moved to a two-sided risk model. There are 7,245 Medicare beneficiaries in the MSSP ACO with two participating hospitals in the ACO provider list. The ACO executive reviewed their prior year's demographic breakdown and noted 19% of beneficiaries assigned to the ACO were dually eligible for Medicare and Medicaid. Prior performance on key quality measures revealed a 16% 30-day readmission rate, 41% all unplanned admissions for patients with multiple chronic conditions and 64% controlling high blood pressure.

The ACO leadership recognize that they must do something different to generate shared savings now that they are in a two-sided risk model and could lose money. They reviewed a CMS analysis of the Medicare Advantage program which found low income subsidy/dually eligible or disabled beneficiaries have a statistically poorer performance on medication adherence for diabetes, hypertension and cholesterol, all cause readmissions, diabetes control, and arthritis management.

The ACO medical director also reviewed a fact sheet from the CMS showing 27% of dually eligible beneficiaries have six or more chronic conditions compared to 15% of beneficiaries with Medicare only. Based on the CMS and ACO analyses, the ACO decides to deploy targeted interventions to address the needs of their dully eligible and disabled ACO patients.

The ACO medical director then learns through a CMS value-based care webinar about a MSSP ACO that contracted with a local community care hub (CCH) to provide services to their members. Based on these successful examples the ACO executive reached out to a local CCH with a network that includes the area agency on aging, center for independent living, United Way, the local food bank and Meals on Wheels program, and other non-profits. The ACO also identified two medical practices that have a high percentage of patients, aligned with their ACO, that are duals or have a history of heart failure with high re-admission rates. The ACO medical director and lead physicians at each of the two clinics meet with the CCH executive to discuss the needs of the priority population and learn that the lack of adherence to scheduled follow-up visits and accessing their medication post-discharge contributes to a disproportionately high readmission rate. The clinic is connected to the state health information exchange (HIE) and they receive electronic notification alerts for each emergency department visit or acute hospitalization.

The ACO and CCH developed a model where persons that have heart failure and a recent acute hospitalization are referred to the CCH. The CCH received an electronic referral through the HIE. The CCH assigned each referral to a CBO partner within the CCH. A community health worker (CHW) from the CBO completes an initial HRSN screen prior to hospital discharge and collaborates with the ACO provider to determine the impact of identified HRSNs on the treatment plan. The CHW assists in implementing a transitional care management (TCM) intervention that includes coordinating a face-to-face visit with the ACO provider within a week of discharge and facilitating transportation for the follow-up visit and the pharmacy to obtain discharge medications. At the time of the TCM face-to-face visit, the treating provider will review the Identified social needs from the CHW screening and complete a SDOH risk assessment. The CHW and the treating provider collaborate to develop a plan to address the HRSNs which they document in the EHR. The CHW then addresses the identified HRSNs with a focus on the impact of transportation security, food insecurity, medication access, and housing insecurity have on the management of heart failure.

Benefits of Outsourcing Claims Processing for CCHs

In some cases, outsourcing claims processing can result in substantial cost savings for CCHs. By partnering with experienced third-party vendors, CCHs can avoid expenses associated with hiring, training, and retaining in-house staff for claims processing tasks. Additionally, outsourced services can leverage economies of scale to further reduce costs.

- **Increased Efficiency -** Claims processing requires specialized knowledge and expertise in medical billing, coding, insurance regulations, and claims submission. Outsourcing this function to expert third-party vendors can help CCHs improve efficiency and accuracy, resulting in faster claims processing and fewer denials. This streamlined process allows CCH staff to focus on person care and other essential aspects of their operations.
- **Access to Expertise -** By outsourcing claims processing, CCHs can tap into the expertise of experienced professionals in the field of medical billing and coding. These experts stay up to date on the latest industry standards, regulatory changes, and best practices, ensuring that claims are processed accurately and in compliance with all relevant regulations.
- **Scalability -** As CCHs grow and evolve, their claims processing needs may change. Outsourcing this function provides the flexibility to scale up or down as needed without significant investments in additional staff or resources. This scalability is particularly beneficial for CCHs, which often serve vulnerable populations and may experience fluctuations in volume.
- **Enhanced Focus on Core Competencies -** Outsourcing claims processing allows CCHs to better allocate their resources and staff to focus on their core competencies, such as individual care, community engagement, and strategic planning. This enables CCHs to prioritize their mission and deliver better outcomes for people served and their communities.
- **Improved Analytics and Reporting -** Outsourced claims processing services often include access to sophisticated analytics and reporting tools, which can provide valuable insights into the CCH's financial performance. These insights can inform data-driven decision-making and help CCHs identify areas for improvement in their RCM processes.

Outsourcing specific aspects of RCM, such as claims processing, is a promising practice that has proven successful for several CCHs. By leveraging the capabilities of expert third-party vendors, CCHs can streamline their operations, improve communication with health systems and partners, and focus on providing essential services to their communities. This approach ultimately benefits both the CCHs and the vulnerable populations they serve.

Cost Accounting

Cost accounting is a specialized branch of accounting that focuses on capturing, analyzing, and allocating an organization's costs associated with the production of goods or the delivery of services. It helps organizations understand the true cost of their operations, products, or services by examining direct costs, such as raw materials and labor, and indirect costs, such as rent, utilities, and administration. By providing detailed insights into the cost structure, cost accounting enables organizations to identify inefficiencies, set accurate pricing, make informed decisions, and improve overall financial performance.

It is important for CCHs to know the costs of their goods and services; cost-based accounting plays a crucial role in managing the financial aspects of delivering healthcare and social services to vulnerable populations. By accurately capturing and allocating costs related to various programs, services, and

partnerships, CCHs can gain a better understanding of the resources required to operate efficiently and effectively.

For example, cost accounting can help CCHs track expenses associated with staff salaries, office space, technology, and other resources necessary for providing care coordination, case management, and other essential services. By identifying the costs associated with each service or program, CCHs can develop budgets, allocate resources, and make strategic decisions that align with their goals and objectives. Additionally, cost accounting enables CCHs to evaluate the financial feasibility of implementing new programs, expanding existing services, or forming partnerships with other organizations, ultimately supporting their mission to improve the health and well-being of the communities they serve.

As CCHs contemplate transitioning to cost accounting, they should consider several crucial factors to guarantee a successful and efficient implementation:

- **Assess the Current Organizational Structure -** Evaluate the existing structure, including departments, programs, services, and sub-units, to establish appropriate cost centers and allocate costs accordingly.
- **Compile Comprehensive Financial Data -** Accurate and up-to-date financial records, such as revenues and expenses, are vital for determining costs associated with different activities and services within the CCH.
- **Identify Cost Drivers -** Recognize the factors that generate costs, such as labor hours, materials, equipment usage, or client numbers, to allocate costs to specific cost centers, programs, or services accurately.
- **Examine Resource Usage -** Investigate the resources used in delivering programs and services, including personnel, materials, equipment, and facilities, to allocate costs based on resource consumption accurately.
- **Review Budget and Financial Planning Processes -** Understand the CCH's budgeting and financial planning procedures to integrate cost accounting seamlessly, enabling informed decision-making and resource allocation.
- **Evaluate Performance Metrics and Outcomes -** Data on program outcomes and performance metrics can help assess the effectiveness of programs and services and identify areas for cost savings and improvements.
- **Clarify Staff Roles and Responsibilities -** Ensure a clear understanding of staff roles and responsibilities involved in various activities and services to allocate costs accurately based on labor hours or other relevant cost drivers.
- **Understand External Funding Sources and Restrictions -** Information on external funding sources, such as grants or contracts, and any associated restrictions or reporting requirements, is essential for compliance and accurate cost allocation.
- **Analyze Existing Accounting Systems and Software -** Familiarize yourself with the current accounting systems and software used by the CCH to determine whether they can support cost accounting or if additional tools or software are needed.

Addressing these key factors will help CCHs achieve a smooth and effective transition to cost accounting, leading to improved financial management and decision-making.

Unit Cost Methodology

While cost-based accounting is essential for understanding the overall costs of the CCH and appropriately allocating costs across different departments and various partners, it is also crucial to recognize that both the CCH and its partners will be delivering direct services under contract with various payors. Understanding both the overall costs of running the CCH and the unit cost for specific services is vital for several reasons, particularly when receiving referrals from health systems and delivering contracted services. There are many reasons why it is important for CCHs and their partners to know the unit cost for certain services. Several key considerations include:

- **Efficient Allocation of Resources -** Knowing the unit cost for specific services enables CCHs and their partners to make informed decisions about allocating resources efficiently. This information helps prioritize services that deliver the most value and impact while minimizing costs. Effective resource allocation can lead to better outcomes for clients and improved overall performance for the CCH.
- **Pricing and Contract Negotiation -** When working with health systems and other partners, understanding the unit cost of services is crucial for pricing and contract negotiations. CCHs need to ensure that the reimbursement rates they negotiate with health systems cover the actual costs of providing the services. Accurate unit cost information helps CCHs, and their partners, establish fair and sustainable pricing structures.
- **Performance Measurement and Improvement -** Unit cost information can also serve as a valuable performance metric for CCHs and their partners. By tracking and comparing unit costs for different services and over time, CCHs can identify areas for improvement, assess the efficiency of various programs or interventions, and adjust their service delivery models accordingly. This continuous monitoring and evaluation process helps CCHs enhance their services, reduce costs, and ultimately deliver better care to clients.
- **Demonstrating Value to Stakeholders -** Accurate unit cost data is essential for CCHs to demonstrate their value to health systems, funders, and other stakeholders. By showing that they can deliver high-quality services at a competitive cost, CCHs can attract more referrals from health systems, secure funding, and strengthen their reputation as effective providers of care.

Understanding both the overall costs of running a CCH and the unit cost for specific services is crucial for efficient resource allocation, accurate pricing and contract negotiation, performance measurement and improvement, and demonstrating value to stakeholders. By focusing on these aspects, CCHs and their partners can ensure that they deliver high-quality, cost-effective services to vulnerable populations and build strong relationships with health systems and other partners.

Case Study: A CBO's Financial Loss Due to Inadequate Unit Cost Knowledge

In the competitive world of healthcare services, it is crucial for CBOs to have a firm grasp of their unit costs when negotiating contracts with health systems. This cautionary case study highlights the financial consequences a CBO faced when they failed to understand their unit costs before entering a contract with a health system to provide intensive case management services.

A fictional CBO, KaziCare, entered a contract with a health system to provide intensive case management services to a vulnerable population. KaziCare's leadership negotiated a rate with the health system, believing it would be sufficient to cover their expenses. However, they did not have an accurate understanding of the unit cost required to deliver these case management services.

As KaziCare began delivering the contracted services, they quickly realized that their negotiated rate was significantly lower than their actual unit cost. Despite the financial strain, they were contractually obligated to continue providing these services, which led to a growing deficit with each case managed.

By the end of the contract, KaziCare had suffered a staggering loss of over $100,000 due to the mismatch between the negotiated rate and their true unit cost. This financial blow severely impacted KaziCare's ability to serve its clients and threatened its sustainability as an organization.

This unfortunate situation could have been avoided if KaziCare had accurately calculated the unit cost of delivering case management services before entering the contract with the health system. With a clear understanding of their actual costs, KaziCare could have negotiated a fair and sustainable rate, prevented the financial loss, and ensured the continued viability of their organization.

Key Takeaways. Understanding unit costs for specific services, accurately calculating these costs prior to contract negotiations, and ensuring fair rates are negotiated with health systems are crucial factors for CBOs. This case study serves as a powerful reminder that prioritizing financial management and cost analysis is essential for protecting the long-term success and capacity of CBOs to support vulnerable populations.

CBOs can determine the unit cost of delivering case management services and make informed decisions about pricing, resource allocation, and contract negotiations with health systems and other partners. The SCAN Foundation has several pricing/cost resources, such as a budget assumption worksheet, indirect cost worksheet, etc. compiled in their Budget and Financial Planning Tool. HealthBegins also has a ROI calculator which considers more information than just determining the unit cost of delivering a social service and includes CBO fixed and variable costs as part of the ROI calculation. It includes a Quick Calculator that prepopulates healthcare utilization and cost data to give the CBO an estimated ROI for specific interventions, including care management (it also includes "Deep Dive" calculator that allows the CBO to input their own data). The tool also includes case studies of CBOs that have used the ROI tool.

Case Management Systems and Tracking[5]

Introduction to Case Management

CCHs are a network of CBOs that provide a range of health and social care services to individuals and families. CCHs play a vital role connecting people with the care they need and improving the overall health and well-being of communities. However, coordinating care across multiple providers and

[5] In this context, the term "case management" is used in a broad generic sense to refer to the coordination of and provision of services. It is not intended to represent or imply the specific certification offered by the Commission for Case Manager Certification https://ccmcertification.org).

organizations can be challenging, especially for persons with complex medical needs. That's where case management comes in. Case management is a collaborative process that helps patients navigate the healthcare system and access the services they need. Case managers work closely with patients and their families to develop care plans and coordinate services across different healthcare providers and community organizations. Case management may be provided by the CCH itself, or the CCH may interact with case management that is being provided in a healthcare setting, such as an interdisciplinary team. By providing patients with comprehensive, coordinated care, case management can improve patient outcomes and reduce healthcare costs. For example, in one study, a housing case management program was associated with a reduction of 29% in hospitalizations, 29% in hospital days, and 24% in emergency department visits among homeless adults who were chronically ill.[6]

This section will explore the role of case management, including MLTSS[7] contracts or other such policies. The concepts apply whether the case management is being provided by the CCH or if the CCH is participating with a healthcare provider as part of larger interdisciplinary team. This section will cover such topics as defining case management, roles and responsibilities, communication and collaboration, technology, tools, and privacy and security.

Defining Case Management for Community Care Hubs

Case management is a collaborative process that involves assessing, planning, implementing, coordinating, monitoring, and evaluating the services and resources required to meet the health and social care needs of a person. Case managers work closely with persons and their families to develop care plans that account for medical, social, and emotional needs. Effective case management may improve care and outcomes in several ways. For example, case managers can:

- **Ensure Persons Receive the Right Care at the Right Time -** By coordinating care across different providers and organizations, case managers can ensure that persons receive the appropriate services and treatments when they need them.
- **Improve Adherence to Treatment Plans -** Case managers can work with individuals to develop care plans that are tailored to their individual needs and preferences. By involving them in the care planning process, case managers can improve person engagement and adherence to treatment plans.
- **Reduce Health Care Costs -** By coordinating care and reducing unnecessary hospitalizations and emergency department visits, case management can help reduce healthcare costs.

Case management has been successfully implemented in a variety of settings, including hospitals, primary care clinics, and CCHs.

Role and Responsibilities

Effective case management generally requires a team-based approach, with different professionals having specific roles and responsibilities. This approach can be particularly valuable for a CCH, as it allows for a more comprehensive and coordinated approach to care. Depending on the types of contracts and/or deliverables your CCH is providing, a team approach may be more effective than

[6] Sadowski, L.S., Kee, R.A., & VanderWeele, J. (2009). Effect of a Housing and Case Management Program on Emergency Department Visits and Hospitalizations Among Chronically Ill Homeless Adults A Randomized Trial. JAMA Network. Accessed at: https://bit.ly/41vQ9oq

[7] https://www.medicaid.gov/medicaid/managed-care/managed-long-term-services-and-supports/index.html

having single individuals providing case management. By working collaboratively, team members can share information, identify gaps in care, and develop more effective care plans. This can lead to improved outcomes, increased satisfaction, and reduced healthcare costs. Here are some of the key roles you might find in effective case management and the responsibilities involved:

- **Case Manager -** Case managers are responsible for overseeing the care of patients and coordinating services across different healthcare providers and community organizations. They work closely with patients and their families to develop care plans that consider the person's medical, social, and emotional needs. Case managers also monitor the person's progress and help to ensure that the care plan is being followed.
- **Care Coordinator -** Care coordinators work closely with case managers to coordinate services and resources for individuals. They help to ensure that people have access to the services they need, such as transportation, home health services, and medical equipment. Care coordinators also help to monitor progress and communicate with other healthcare providers and community organizations involved in the person's care.
- **Social Worker -** Social workers provide emotional and social support to individuals and their families. They help people cope with the emotional and psychological effects of their illness or condition and provide counseling and support as needed. Social workers also help people access community resources and services, such as housing assistance and financial support.
- **Other Support Staff -** Other support staff, such as nurses, dietitians, and administrative staff, also play important roles in case management. Nurses may provide clinical support to patients, may conduct medical assessments, or assist with medication management. Dietitians may review dietary restrictions and help plan medically tailored meals. Administrative staff may help with scheduling appointments, managing records, and submitting claims for payment.

When working with a hospital case management team, a CCH may find itself collaborating with a variety of healthcare professionals, including case managers, physicians, nurses, social workers, dietitians, pharmacists, physical therapists, occupational therapists, speech therapists, psychologists, and psychiatrists. Each of these professionals has a critical role in ensuring that the person receives the care and services they need to achieve optimal health outcomes.

When it comes to case management, effective communication and collaboration between healthcare professionals from both the CCH and hospital staff are crucial. By working together as a team, they can ensure that all persons, including persons with limited English proficiency and people with disabilities, receive meaningful access to the appropriate services and treatments in a timely manner and that the care plan is being followed. In the following sections, we'll delve deeper into the importance of communication and collaboration in case management.

Communication and Collaboration

Effective communication and collaboration are essential for successful case management. Case managers and healthcare providers should work together as a team to ensure that people, including people with limited English proficiency and people with disabilities, receive meaningful access to the appropriate services and treatments when they need them. Here are some best practices for sharing individual information, coordinating care plans, and ensuring that everyone is on the same page:

- **Centralize Patient Records-** Use a centralized system to ingrate patient/person health and social data. Having a centralized system for gathering and integrating information can help to ensure

that all providers involved in the person's care have access to the same information. This can include EHRs, case management systems, secure messaging systems, and other communication tools. Case managers should ensure that all providers involved in the person's care have access to these systems and are trained in how to use them effectively.

- **Develop a Comprehensive Care Plan-** Case managers should work with persons and their families to develop a comprehensive care plan that accounts for the person's medical, social, and emotional needs. The care plan can be shared with all healthcare providers involved in the person's care, and updates shall be made as needed.
- **Schedule Regular Team Meetings-** Regular team meetings can help to ensure that everyone is on the same page and that the care plan is being followed. Case managers should schedule regular team meetings with all healthcare providers involved in the person's care. During these meetings, providers can discuss the person's progress, review the care plan, and identify any issues or concerns.
- **Encourage Open Communication-** Encouraging open communication between healthcare providers can help to ensure that everyone is aware of the person's needs and concerns. Case managers should encourage healthcare providers to communicate openly with each other and to share any concerns or issues that arise. This can help to prevent misunderstandings and ensure that the person's needs are being met.
- **Respect Privacy-** It is important to respect individual privacy when sharing information and communicating with other healthcare providers. Case managers should ensure that all healthcare providers involved in the person's care are aware of the person's privacy rights and are trained on how to handle personal information appropriately.

These best practices are just some of the considerations that a CCH might evaluate when implementing effective case management practices. Healthcare providers that are covered entities must adhere to the HIPAA Privacy Rule's minimum necessary standard which limits patient information to only the minimum amount of protected health information needed to accomplish the intended purpose of the use or disclosure. While you may think you need more patient information, your healthcare partner determines the minimum necessary. By following these practices, case managers and healthcare providers can work together effectively to provide persons with comprehensive, coordinated care. Effective communication and collaboration among healthcare providers can help to ensure that persons receive meaningful access to the appropriate services and treatments when they need them. This can improve outcomes, reduce healthcare costs, and increase satisfaction. Technology should be used to help facilitate and support effective communication and collaboration among healthcare providers.

Technology and Tools

As technology continues to advance, it is becoming increasingly important for CCHs and healthcare organizations to leverage technology and tools to support effective and nondiscriminatory case management. Technology and tools can help case managers and healthcare providers to coordinate care, communicate with each other, and share person information securely. Here are some examples of technology and tools that can be used to support case management:

- **Cloud-based Case Management Systems -** These systems are web-based software solutions that allow case managers and healthcare providers to manage person information, track services provided, and streamline workflows. Cloud-based systems can be accessed from anywhere with

an internet connection, making it easier for case managers and healthcare providers to collaborate and share information.

- **Electronic Health Records -** EHRs are digital versions of a person's medical record. They can be accessed by healthcare providers in different locations and can help to ensure that all providers have access to the same information. Case managers can use EHRs to track progress, schedule appointments, and communicate with other healthcare providers. EHRs can also help to reduce errors and improve safety by providing accurate and up-to-date information.
- **Patient Portals -** Patient portals are secure online platforms that allow patients to access their medical information, communicate with healthcare providers, and schedule appointments. Case managers can use patient portals to share care plans, provide education materials, and communicate with patients and their families. Patient portals can help to improve patient engagement and satisfaction by giving patients more control over their healthcare.
- **Social Health Access Referral Platforms -** Social Health Access Referral Platforms (SHARPs) refers to a newer type of software platform designed to facilitate and streamline the process of social health referrals and coordination.[8] It helps healthcare providers connect persons with social services and community resources. Case managers can use SHARPs to identify patients' social needs and refer them to appropriate resources, such as food banks, housing assistance programs, and transportation services. By addressing patients' social needs, healthcare providers can improve outcomes and reduce healthcare costs.

Role of Interoperability in Case Management

Interoperability is defined as the ability of computer software or systems to exchange information and handle that information meaningfully. In the healthcare domain, interoperability helps clinicians deliver safe, effective, patient-centered/person-centered care. It also provides new ways for individuals and caregivers to access electronic health information to manage and coordinate care.

Consider a scenario where a CCH that serves as a central point for coordinating healthcare and social services for individuals with chronic conditions, such as diabetes. The hub works closely with various healthcare providers, including primary care physicians, specialists, and allied health professionals. Interoperability enhances case management in the following ways:

- **Seamless Exchange of Health Information -** Interoperability enables the CCH to access and share relevant patient health information with healthcare providers involved in the individual's care. Through interoperable EHR systems, the hub can securely exchange data, such as medical history, test results, treatment plans, and medication lists. This comprehensive information empowers the case manager to make well-informed decisions and collaborate effectively with healthcare providers.
- **Coordinated Care Planning -** Interoperability facilitates the coordination of care plans between the CCH and healthcare providers. The case manager can collaborate with primary care physicians, specialists, and other providers to develop an integrated care plan that addresses the individual's specific needs. Interoperability ensures that all stakeholders have access to the latest care plan, allowing for seamless updates, adjustments, and monitoring of progress.

[8] Aging and Disability Business Institute. (2022, February 18). SHARP Function Checklist: Decision Points for CBOs Considering Working with Social Health Access Referral Platforms. Washington, DC. Aging and Disability Business Institute.

- **Real-Time Communication and Alerts -** Interoperability enables real-time communication and alerts between the CCH and healthcare providers. For instance, if a patient experiences a significant change in health status or requires urgent intervention, the case manager can promptly notify the relevant healthcare providers. Conversely, healthcare providers can send updates, such as treatment modifications or upcoming appointments, back to the CCH. This timely exchange of information improves care coordination and ensures that interventions are promptly implemented.
- **Medication Management -** Interoperability plays a crucial role in medication management, especially when individuals receive care from multiple providers. Through interoperable systems, healthcare providers can view and update medication records, including prescriptions, dosage adjustments, and medication adherence data. The case manager at the CCH can access this information to monitor medication compliance, identify potential drug interactions, and intervene if necessary.
- **Referral Management -** Interoperability streamlines the referral process between the CCH and healthcare providers. When a patient requires specialized care, such as a referral to a cardiologist for cardiovascular issues, the case manager can electronically refer the patient, securely transmitting relevant medical information. Interoperability ensures that the specialist receives the necessary patient details, enabling them to provide targeted care without delay.
- **Outcomes Tracking and Reporting -** Interoperability supports outcomes tracking and reporting efforts. The CCH can collect data from various healthcare providers involved in the individual's care and aggregate it for analysis. This data can be used to evaluate the effectiveness of interventions, identify areas for improvement, and generate comprehensive reports on patient outcomes. Interoperability streamlines data collection and reporting processes, saving time and improving the accuracy of data analysis.

By leveraging interoperability between CCHs and healthcare providers, case management becomes more efficient, coordinated, and patient-centered. The seamless exchange of health information improves communication, facilitates care planning, supports medication management, enables timely interventions, and enhances the overall quality of care delivered to individuals within the community.

Although technology and tools can be helpful in supporting case management, they should not replace the human element of care. Effective case management requires a combination of technology and human interaction to provide patients with comprehensive, coordinated care. While technology can help to streamline workflows and improve communication, it cannot replace the empathy, compassion, and personal touch that healthcare providers bring to patient care. The human element of care is essential in building trust, establishing rapport, and understanding patients' unique needs and preferences. Therefore, it's crucial for healthcare providers to strike a balance between technology and human interaction to provide patients with the best possible care.

When selecting technology and tools to support case management, it is important to consider the needs of both the patient and the healthcare provider while also complying with relevant regulations and standards. For instance, HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) implementing regulations have requirements that may require case management systems to meet certain privacy and security requirements. Additionally, the Older Americans Act (OAA) confidentiality requirements may also need to be followed when working with older adults receiving services funded by the OAA. Health Information Trust Alliance (HITRUST) certification is becoming

increasingly important for healthcare organizations that need to demonstrate compliance with these requirements.

Additionally, when selecting technology and tools it is critical to consider health IT standards as part of health IT infrastructure or advancement activities and investments. As part of this process, CCHs may identify relevant, national standards such as those in the Office of the National Coordinator (ONC) Interoperability Standards Advisory and, as applicable, those that conform to ONC certification criteria in health IT products used or that will be used to support critical functions and interoperable data exchange. It is important to use health IT systems and products that meet standards and implementation specifications consistent with broader requirements applicable in federal programs and policies and for enabling interoperability.

CCHs may come across different types of software solutions when looking for technology to support their operations. Two common types of software are Commercial Off-The-Shelf (COTS) and custom software. COTS software is pre-built software that is designed to meet the needs of a wide range of users. It is typically less expensive and quicker to implement than custom software. However, COTS software may not be tailored to the specific needs of a CCH and may require additional customization to meet their requirements. Custom software, on the other hand, is designed specifically for the needs of a particular organization. It is typically more expensive and time-consuming to develop than COTS software. However, custom software can be tailored to the needs of a CCH and can provide a more personalized solution. Ultimately, the choice between COTS and custom software will depend on the specific needs and budget of the CCH.

To select and implement technology and tools effectively while meeting these requirements, here are some tips:

- **Assess Your Needs -** Before selecting technology and tools, assess your organization's needs and determine which tools will be most useful for your case management processes. Consider factors such as cost, ease of use, and compatibility with existing systems. It's important to involve all stakeholders, including case managers, healthcare providers, and patients in the needs assessment process to ensure that the selected tools meet everyone's needs.
- **COTS vs Custom Software -** Research and evaluate different technology solutions, including COTS and custom software. Consider the pros and cons of each option, such as cost, implementation time, customization options, and scalability. It's important to choose a solution that meets the specific needs of your organization while also complying with relevant regulations and standards.
- **Train Staff in How to Use the Tools -** Ensure that all staff members who will be using the technology and tools are trained in how to use them effectively. Provide training sessions and educational materials to help staff members learn how to use the tools. It's also important to provide ongoing support and resources to help staff members troubleshoot any issues that may arise.
- **Ensure that the Tools are Secure -** Ensure that the technology and tools used for case management are secure and meet all privacy and security requirements. This can include using encryption, firewalls, and other security measures to protect patient information. Additionally, the Interoperability Rule requires that healthcare organizations implement secure and standardized methods for exchanging patient information between different systems. It's

important to regularly review and update security measures to ensure that they remain effective.

- **Evaluate the Effectiveness of the Tools -** Regularly evaluate the effectiveness of the technology and tools used for case management. Solicit feedback from staff members and beneficiaries to identify areas for improvement and make changes as needed. It's important to continuously monitor and evaluate the tools to ensure that they are meeting the evolving needs of the organization and its patients.
- **Ensure that the Tools are not discriminatory -** Consider consulting tool developers and publicly available sources to ensure that patient care decision support tools as defined at 45 CFR 92.210 not discriminate against individuals based on race, color, national origin, sex, age, or disability. In addition, make reasonable efforts to identify whether any tools risk discrimination by evaluating whether the tools include input variables or factors that measure race, color, national origin, sex, age, or disability. If such tools are identified, make reasonable efforts to mitigate the risk of discrimination, for example, by reducing the use or stopping the use of such tools.

By following these tips, CCHs can make more informed decisions and select and implement technology and tools that support effective case management while also complying with relevant regulations and standards. Effective use of technology and tools can help CCHs to improve patient outcomes, increase efficiency, and reduce costs.

Privacy and Security

Privacy and security are critical considerations when sharing patient information across different organizations. In today's healthcare landscape, care coordination often requires the exchange of patient information between different healthcare providers and organizations. While this can improve patient outcomes and provide more comprehensive care, it can also present privacy and security concerns. Patient data must be protected and secured at all times to prevent unauthorized access or disclosure. Failure to do so can result in breaches of patient privacy, legal violations, and damage to the reputation of healthcare organizations. The following are some best practices for ensuring privacy and security when sharing patient information, including understanding relevant regulations and standards, using secure communication channels, implementing access controls, monitoring access to patient information, training staff on privacy and security, and conducting regular risk assessments. By following these best practices, CCHs can ensure that patient data is protected and secure when shared across different organizations, while providing patients with comprehensive, coordinated care.

- **Understand the relevant regulations and standards -** It is important to understand the relevant regulations and standards that apply to your organization, such as HIPAA Privacy Security Breach Notification and Enforcement Rules (HIPAA Rules). These regulations and standards provide guidelines for protecting patient information and ensuring that it is shared securely.
- **Use secure communication channels -** When sharing patient information, use secure communication channels such as encrypted email, secure messaging platforms, or secure file transfer protocols. This can ensure that patient information is protected from unauthorized access.
- **Use access controls -** Use access controls to limit access to patient information to only those who need it to provide care. This can include role-based access controls, two-factor authentication, and other security measures.

- **Monitor access to patient information -** Monitor access to patient information to detect any unauthorized access or use. This can include reviewing audit logs and implementing alerts for suspicious activity.
- **Train staff in privacy and security -** Ensure that all staff members who handle patient information are trained in privacy and security best practices. This can include providing regular training sessions and educational materials.
- **Conduct regular risk assessments -** Conduct regular risk assessments to identify and address any potential privacy and security risks related to sharing patient information. This can help to ensure that patient data is protected and secure at all times.

By following these best practices, CCHs can ensure that patient information is protected and secure when shared across different organizations. It is important to prioritize patient privacy and security when sharing information to provide patients with comprehensive, coordinated care.

Integrating Case Management with Information and Referral Systems

Integrating case management systems with information, referral, and assessment (IR&A) systems with social health and referral platforms can provide numerous benefits for CBOs and healthcare providers. By sharing patient information and coordinating care more effectively, organizations can improve patient outcomes and reduce healthcare costs. Integrating these systems can be challenging, but achieving interoperability can streamline workflows, reduce duplication of effort, and improve communication between organizations. A case management system also has the potential to serve as a centralized location for managing patient information, while IR&A systems and social health and referral platforms can provide insights into patient needs and resources available in the community. One suggestion is to consider using standardized assessment tools and referral criteria to ensure that patients are referred to the appropriate resources. This helps to reduce the burden on case managers and healthcare providers and ensures that patients receive the care they need in a timely manner. Investing in systems that help achieve closed loop referral may also help to ensure that patients receive the appropriate care and that referring organizations receive feedback on the outcome of the referral.

A software roadmap is a strategic plan that outlines the development goals and objectives of a software product over a specific period of time. It includes a timeline, list of features, and priorities to align everyone's expectations and ensure the development process is focused on achieving the most important goals.

However, achieving closed loop referrals between three potentially different systems (healthcare provider, CCHs, and CBO providing direct services) can be challenging. It requires a high level of coordination and communication between organizations, as well as the use of sophisticated interoperable technology solutions. It is important to establish clear protocols for sharing patient information and ensure that all organizations involved in the referral process are aware of their roles and responsibilities. Consent management is also an important aspect of the closed loop referral process. Individuals must provide informed consent for their information to be shared between organizations, and they must be informed of the purpose and scope of the referral. It is critical to establish clear consent management protocols and ensure that patients are fully informed of their rights and options. It is important to ensure that patient privacy and security are maintained throughout the referral process.

Interoperability

Interoperability standards are essential for integrating case management systems with IR&A systems and social health and referral platforms. These standards provide a common language and structure for exchanging data between different systems, ensuring that patient information is accurate, complete, and secure. More detailed information on the various leading standards being developed and in use today can be found in Chapter 5.

It is important to recognize that many of these standards and frameworks are still being developed. Likewise, it is critical to consider the level of engagement of various vendors in these initiatives and where compliance and support is relative to their technology or interoperability roadmaps for improvements. One should choose technology solutions that are interoperable and comply with relevant standards and regulations, such as HIPAA Rules and the Interoperability Rule.

Interoperability standards, such as, the Fast Healthcare Interoperability Resources (FHIR) standard, provides a standardized way to exchange healthcare information between different systems, while also ensuring that patient privacy and security are maintained.

In addition to broader healthcare-specific specifications the Human Services Data Specifications, developed by the Open Referral Initiative and endorsed by the Alliance of Information and Referral Systems, are another important set of interoperability specifications. These specifications are designed to make it easier for organizations to share data about human services, such as food banks, homeless shelters, and job training programs. The specifications define a set of classes and properties for describing human services, such as the name of the service, the location of the service, and the contact information for the service.

The Human Services Data Specifications are designed to be flexible and extensible, so that they can be used to describe a wide variety of human services. The specifications are also designed to be interoperable, so that data can be exchanged between different systems. Using these interoperability standards and frameworks can provide numerous benefits, including:

- **Improved Coordination of Care -** The specifications can help improve the coordination of care by making it easier for organizations to share data about human services. This can help to ensure that people receive the care they need and when they need it.
- **Easier Access to Services -** The specifications can make it easier for people to find the services they need by making it easier for organizations to share data about their services. This can help to reduce the number of people who are unable to access the services they need.
- **Improved Data Quality -** The specifications can help to improve the quality of data about human services by providing a common vocabulary and structure for data. This can help to ensure that data is accurate and consistent, which can make it easier to use.
- **Increased Interoperability -** The specifications can help to increase interoperability between different systems that use data about human services. This can help to improve efficiency and effectiveness by using these interoperability standards and specifications. Community-based organizations and healthcare providers can ensure that patient information and data about human services is shared securely and efficiently, enabling them to provide coordinated care and improve patient outcomes.

More details about Interoperability Standards can be found in the Data Standards section of Chapter 5.

Data Governance: Ensuring Accurate, Complete, and Secure Sharing

In today's healthcare landscape, the sharing of patient information between organizations is critical for improving patient care and outcomes. However, sharing this information also presents several challenges, including ensuring the accuracy, completeness, and security of the data. This is where data governance plays a critical role.

Data governance refers to the process of managing the availability, usability, integrity, and security of the data used in an organization. In the context of integrating case management systems with IR&A systems and social health and referral platforms, data governance is critical for ensuring the accuracy, completeness, and security of patient information when shared between organizations.

- **Ensure Accuracy-** One of the primary goals of data governance is to ensure the accuracy of the data being shared between different organizations. This means ensuring that the data is complete, up-to-date, and free of errors. Inaccurate data can lead to incorrect diagnoses, incorrect treatments, and other negative outcomes for the patient. To ensure the accuracy of patient data, organizations should establish data quality standards and processes. This includes developing data validation rules, instituting data cleaning processes, and implementing data quality monitoring and reporting. By implementing these processes, organizations can ensure that the data being shared is accurate and reliable.
- **Ensure Completeness-** Another goal of data governance is to ensure the completeness of the data being shared. This means ensuring that all relevant data is included in the shared information. Incomplete data can lead to missed diagnoses, poorly developed care plans, and other negative outcomes for the patient. To ensure the completeness of patient data, organizations should establish data mapping protocols and data sharing agreements. This includes identifying the specific data elements that need to be shared between different organizations and developing processes for mapping these data elements to the appropriate fields in different systems. By implementing these processes, organizations can ensure that all relevant data is included in the shared information.
- **Ensure Security-** Finally, data governance is critical for ensuring the security of patient information when shared between different organizations. This means ensuring that the data is protected from unauthorized access, theft, and other security breaches. Security breaches can lead to the exposure of sensitive patient information, which can have serious consequences for the patient and the organization. To ensure the security of patient data, organizations should implement appropriate technical and administrative safeguards. This includes implementing encryption, access controls, and audit trails to protect patient information from unauthorized access. Organizations should also establish data sharing agreements that define the roles and responsibilities of different stakeholders with respect to data security.

Data governance is critical for ensuring the accuracy, completeness, and security of patient information when shared between different organizations. By establishing data quality standards, data mapping protocols, and data sharing agreements, organizations can ensure that the data being shared is accurate, complete, and secure. This can help to improve patient outcomes and enhance the effectiveness of integrated care delivery systems.

However, implementing effective data governance processes can be challenging. It requires a commitment to data quality, a willingness to collaborate with other stakeholders, and a deep understanding of the technical and regulatory requirements for sharing a person's information. Organizations should work with experienced data governance professionals to develop and implement

effective data governance processes that meet their unique needs and requirements. By prioritizing data governance, organizations can ensure that the data being shared is accurate, complete, and secure, which can help to improve a person's care and outcomes.

Privacy and Security Considerations for Interoperability

Interoperability has the potential to improve individual care and outcomes by enabling healthcare providers and CBOs to share information securely and efficiently. However, sharing information presents several privacy and security challenges, particularly when sending and receiving referrals from other vendor systems. This section will explore the consent, privacy, and security considerations that must be addressed when sharing an individual's information between different systems and organizations and how to implement appropriate technical and administrative safeguards to protect individuals. Implementing interoperability for sharing information raises multiple consent, privacy, and security considerations, including the following:

- **Informed Consent—**Persons should not only give their consent for their data to be shared, but also fully understand the implications of this. For instance, a person should know how their data will be used, who will have access to it, and the benefits and risks of sharing their data. This can be ensured through transparent consent forms and education.
- **Minimum Necessary Rule—**According to the HIPAA Privacy Rule, only the minimum necessary information should be shared for a specific purpose. For example, if a specialist only needs a person's recent test results, there is no need to share their entire medical history.
- **Encryption—**Encryption converts data into a code to prevent unauthorized access. For instance, when transmitting data over the network, it should be encrypted to prevent interception. When stored, it should be encrypted to prevent access in case of a data breach.
- **Authentication—**Authentication methods can range from passwords to two-factor authentication (2FA), and even biometric scans. This ensures that only authorized individuals have access. For instance, a doctor could use a secure login and a fingerprint scan to access individual records.
- **Access Controls—It** is crucial to have clear roles and permissions defined. For example, a receptionist might only have access to contact information, while doctors have full access to medical records.
- **Audit Trails—**Keeping detailed logs of who accesses data and when helps in tracking any unauthorized access or breaches. For instance, if a data breach occurs, audit trails can help identify the source and take corrective actions.
- **Vendor Agreements—**Vendors that handle patient/person data should also comply with privacy and security standards. For example, a cloud storage vendor should provide assurance of their security measures and take responsibility in case of a data breach.
- **Training—**Staff should regularly be trained in data privacy and security regulations, as well as the organization's policies. For instance, training could include how to identify phishing attempts or how to securely handle individual data.
- **Risk Assessment—**Regular risk assessments can help identify potential vulnerabilities and allow CCHs to take preventative measures. For example, regular penetration testing could identify weak points in your network security that can be addressed before they are exploited.

By adhering to these considerations and adapting them according to an organization's specific needs and context, a secure environment for handling and sharing data can be created.

Regulatory Requirements

The regulatory requirements for privacy and security are primarily governed by the HIPAA Rules. These regulations establish the standards for the privacy and security of protected health information (PHI) and electronic protected health information (ePHI) and provide guidance on how to implement appropriate physical, technical, and administrative safeguards to protect this information.

Under HIPAA and HITECH, covered entities (such as healthcare providers that conduct HHS Secretary adopted standard transactions, health plans, and healthcare clearinghouses) and business associates (such as CCHs, CBOs, or other vendors and contractors that handle PHI on behalf of covered entities) must implement appropriate administrative, physical, and technical safeguards to protect PHI and ePHI. These safeguards include access controls, audit trails, and breach notification procedures.

Challenges Associated with Sending and Receiving Referrals

Sending and receiving referrals from other vendor systems can present several challenges from a privacy and security perspective. One of the primary challenges is ensuring that the information is transmitted securely and that only authorized individuals have access to the information. This requires implementing appropriate access controls, encryption, and audit trails to protect the information from unauthorized access, theft, and other security breaches.

Another challenge is ensuring that the information is transmitted accurately and completely. This requires implementing appropriate data quality standards and data mapping protocols to ensure that the information is mapped to the appropriate fields in different systems and that all relevant information is included in the referral.

Finally, there is a challenge in ensuring that the information is transmitted in compliance with regulatory requirements, such as the HIPAA Rules. This requires establishing data sharing agreements that define the roles and responsibilities of different stakeholders with respect to privacy and security and ensuring that all parties are in compliance with relevant regulations and standards.

Implementing Appropriate Technical and Administrative Safeguards

To address these challenges, organizations could implement appropriate technical and administrative safeguards to protect patient information when sharing referrals between different systems and organizations. This includes implementing access controls, encryption, and audit trails to protect the information from unauthorized access, theft, and other security breaches. It also includes implementing data quality standards and data mapping protocols to ensure that the information is transmitted accurately and completely.

Organizations may want to establish data sharing agreements that define the roles and responsibilities of different stakeholders with respect to privacy and security. These agreements could address issues such as data ownership, data quality, data security, and breach notification procedures. Organizations could also conduct regular risk assessments to identify potential vulnerabilities and implement appropriate risk management strategies to mitigate these risks.

Definition of Shared Services

In this context, shared services generally refer to shared business services and these can include a range of activities and functions such as human resources, finance, IT, marketing, and procurement. Essentially, any function that is not specific to the core mission of the CCH can be outsourced to a shared service provider. Shared business services can be provided internally within the CCH or through a third-party vendor. The key feature of shared business services is that they are centralized and standardized, enabling economies of scale and operational efficiencies.

Importance of Shared Business Services for CCHs

CCHs face unique challenges in delivering care and services to their communities. They often operate on tight budgets with limited resources and must navigate complex regulatory environments. By leveraging shared business services, CCHs can overcome some of these challenges by:

- **Reducing costs -** Shared business services can help CCHs save money by consolidating administrative functions, negotiating better pricing with vendors, and sharing infrastructure costs with other organizations.
- **Improving quality -** Shared business services can provide access to specialized expertise and technology, enabling CCHs to deliver higher quality care and services to their communities.
- **Streamlining operations -** Shared business services can simplify operations by eliminating redundancies and standardizing processes, freeing up time and resources for CCHs to focus on their core mission.

Promising Practice: CCH Partnering with a Third-Party Administrator

A CCH in a large metropolitan area may partner with a Third-Party Administrator (TPA) that specializes in billing and invoicing for healthcare organizations. The TPA would handle all invoicing and billing functions for the CCH partners, including insurance claims processing, patient billing, and collections. By centralizing these functions, the CCH can reduce the overhead costs associated with managing multiple billing systems and processes. The TPA would also have expertise in compliance and regulations related to healthcare billing, reducing the risk of errors and regulatory violations.

In addition, the TPA could provide detailed reporting and analytics on billing and invoicing trends, enabling the CCH to better understand the financial performance of the organization and make data-driven decisions to improve operations. This could include identifying areas where billing and invoicing can be optimized, as well as identifying trends in patient utilization and revenue streams.

Types of Shared Services

There are numerous business activities which may lend themselves to a shared services arrangement. Each CCH should consider its strengths and weaknesses as well as available resources when evaluating which services make sense to contract to other organizations, either within the CCH network or with external partners. Some of the functions which are commonly outsourced may include:

- **Human Resources -** Shared human resource services can help to reduce administrative overhead, improve employee engagement, and create efficiencies across the organization.

Services can include recruitment, payroll administration, benefits management, and training and development.

- **IT Services -** Shared IT services can provide a range of benefits including cost savings, improved performance and security, and better disaster recovery capabilities. Services can include network management, software applications, hardware and device management, and data management and analysis.
- **Financial Services -** Shared financial services can provide a range of benefits including cost savings, improved financial controls, and better cash management. Services can include bookkeeping and accounting, invoicing, and billing, accounts payable and receivable, and tax and audit services.
- **Marketing and Communications -** Shared marketing and communications services can help to improve the visibility of the CCH, increase public awareness, and attract more clients. Services can include branding and identity, website development, social media management, public relations, and event planning.

Benefits of Shared Business Services

CCHs can benefit greatly from shared business services, including:

- **Cost Savings-** Sharing business services can help to reduce administrative overhead, eliminate duplication, and improve economies of scale.
- **Improved Efficiency-** Shared services can provide more efficient and effective service delivery by streamlining processes and leveraging best practices.
- **Better Quality-** Shared services can help to improve the quality of care provided to vulnerable populations by providing consistent and standardized processes.
- **Increased Flexibility-** Shared services can help to increase flexibility and responsiveness to changes in demand, market conditions, or regulatory requirements.
- **Implementing shared business services-** While shared business services can provide many benefits, there are also several challenges that CCHs may face, including:
    - **Cultural Differences-** Different organizations may have different cultures, values, and ways of working, which can create challenges when trying to implement shared services.
    - **Communication-** Effective communication is essential when implementing shared services. Clear communication channels, shared goals, and a shared vision are critical to success.
    - **Integration-** Integration with existing systems and processes can be challenging, particularly if different organizations are using different systems and processes.
    - **Data Privacy and Security-** Sharing data across organizations can create privacy and security concerns, particularly if sensitive information is being shared.

By carefully evaluating the benefits and challenges of shared business services, CCHs can make informed decisions about which services to share and how best to implement them to improve efficiency and care delivery.

Promising Practice: Contracting for a Shared EHR

A CCH may consider contracting on behalf of its partners for a shared EHR system. By sharing a single EHR system, CCH partners can access and share patient data in real-time, leading to more coordinated and efficient care. This can also reduce the risk of errors and duplication, as well as improve outcomes. Additionally, the EHR infrastructure can provide cost savings for the CCH by reducing the need for each partner to purchase and maintain their own EHR system. This can also reduce the burden of IT support and maintenance for each partner, freeing up resources to focus on patient care. To ensure the success of a shared IT service, the CCH should consider factors such as data privacy and security, interoperability with other systems, and training and support for staff.

Establishing Shared Services Arrangements

The process of implementing shared services can be complex and requires careful planning and evaluation. In this section, we will provide recommendations for CCHs to consider when establishing shared business services. The first step in establishing shared business services is to identify which services are potential candidates for sharing. The CCH, along with their close business partners, should evaluate their organization's needs and determine which services are necessary for their operations. Once the needs are identified, the CCH should:

- **Assess Feasibility of Sharing Services -** After identifying potential shared business services, the CCH should evaluate the feasibility of sharing those services. This includes assessing the costs and benefits, determining which services are critical to their operations, and identifying potential partners for sharing services. The CCH should consider whether sharing services internally, on behalf of partners, leveraging another partner resource, or outsourcing would be the most effective option.
- **Develop a Plan for Shared Business Services -** After assessing the feasibility of sharing services, the CCH should develop a plan for shared business services. This includes outlining the scope of services to be shared, identifying partners for sharing services, establishing a governance structure for shared services, and determining how costs will be allocated among partners. The plan should also include a timeline for implementation and milestones to track progress.
- **Implement Shared Business Services -** Once a plan for shared business services has been developed, the CCH should begin implementing those services. This includes establishing shared systems and processes, training staff on shared services, and communicating the benefits of shared services to all stakeholders. Establishing effective communication channels and ensuring that all stakeholders are engaged and informed throughout the implementation process is essential. The CCH should also anticipate potential challenges and develop contingency plans to address them.
- **Monitor and Evaluate Shared Business Services -** After implementing shared business services, the CCH should regularly monitor and evaluate the effectiveness of those services. This includes measuring the impact of shared services on the organization's operations, assessing the quality of care delivered to vulnerable populations, and identifying areas for improvement. The CCH should also regularly communicate with partners to ensure that shared services are meeting their needs and adjust as necessary.
- **Foster a Culture of Continuous Improvement -** To ensure the long-term success of shared services, the CCH should foster a culture of continuous improvement. This involves regularly

reviewing and updating shared services processes, soliciting feedback from partners and staff, and identifying opportunities for innovation and enhancement. By actively engaging all stakeholders and prioritizing ongoing improvement, CCHs can maximize the benefits of shared services and create a more efficient, effective, and sustainable model for delivering care to vulnerable populations.

Evaluating opportunities to establish shared services arrangements can greatly benefit CCHs by streamlining and scaling operations, reducing costs, and promoting collaboration among partners. By carefully assessing feasibility, developing a comprehensive plan, implementing shared services, and fostering a culture of continuous improvement, CCHs can enhance their capacity to provide high-quality care and support to vulnerable populations. As the CCH navigates the process of establishing shared services, it is essential to maintain open communication, actively engage all stakeholders, and remain adaptable to ensure long-term success and sustainability.

Considerations for Sharing Business Services

When a CCH leads the initiative for sharing services, there are several important considerations that should be addressed. These considerations ensure that the CCH can make informed decisions and achieve successful implementation of shared services. The main considerations include legal and regulatory aspects, data sharing and privacy concerns, and financial considerations.

Legal and Regulatory Considerations - The CCH must ensure compliance with all relevant laws and regulations when sharing services. This includes understanding the regulatory framework governing shared services and the potential legal implications. CCHs should consult with legal experts to identify any potential risks and develop strategies to mitigate them. Some key legal and regulatory considerations include:

- Contracts and service-level agreements (SLAs) between the CCH and its partners, outlining the terms, conditions, and responsibilities of each party.
- Ensuring compliance with federal, state, and local laws, as well as industry-specific regulations that may apply to shared services.
- Identifying potential liability risks and determining strategies to minimize them, such as obtaining appropriate insurance coverage.
- Understanding licensing and accreditation requirements for specific shared services and ensuring all partners meet these requirements.

CAAs, like CCHs, are non-profit organizations that provide a range of services and programs to help low-income individuals and families overcome poverty and achieve economic self-sufficiency. CAAs work to address the root causes of poverty through a variety of services, such as job training, education, housing assistance, and healthcare. Much like CCHs, they are funded through a combination of federal, state, and local sources and often partner with other organizations to deliver services. As a result, these sample documents may prove valuable resources for CCHs looking to establish shared services or partnerships with other organizations.

Data Sharing and Privacy Considerations - When sharing services, CCHs must pay close attention to data sharing and privacy concerns. This includes ensuring compliance with relevant data protection

laws, such as HIPAA and the General Data Protection Regulation (GDPR). Key data sharing and privacy considerations include:

- Establishing clear data sharing agreements that outline the types of data to be shared, the purpose of data sharing, and the responsibilities of each party.
- Implementing robust data security measures, including encryption, access controls, and regular security assessments.
- Ensuring that all partners adhere to strict privacy policies and practices to protect sensitive information and maintain the trust of service recipients and stakeholders.
- Providing training and support for staff on data privacy and security best practices.

Financial Considerations - Implementing shared services often involves financial investments, including infrastructure, technology, and staff resources. The CCH should carefully consider the financial implications of sharing services to ensure a sustainable and cost-effective approach. Key financial considerations include:

- Assessing the costs and benefits of sharing services, including potential cost savings and improvements in service delivery.
- Developing a transparent and equitable cost-sharing model that fairly allocates expenses among partners.
- Identifying potential funding sources, such as grants or other financial incentives, to support the implementation of shared services.
- Regularly monitoring and evaluating the financial performance of shared services to ensure ongoing cost-effectiveness and efficiency.

Sharing business services can provide significant benefits for CCHs, including streamlined operations, ability to scale services, reduced costs, and improved collaboration more quickly among partners. As the CCH navigates the complex process of establishing shared services, it is essential to carefully consider legal and regulatory compliance, data sharing and privacy concerns, and financial implications.

Best Practices for Integrating CM Systems with IR&A and Referral Platforms

CCHs are designed to bring together healthcare providers and CBOs to improve individual care and outcomes. To achieve this goal, these organizations should be able to collaborate and share information effectively. Integrating case management systems with IR&A systems and social health and referral platforms is a critical step in achieving this goal. In this section, we will discuss some of the challenges and considerations for integrating these systems, including workflow, data mapping, data format, communication, user interface, exchange protocols, and point-to-point connections vs Application Programming Interfaces (APIs).

Workflow - Workflow is an important consideration when integrating different systems. One of the main challenges in this process is ensuring that the workflow of each system is compatible with the workflow of the other systems. This can be particularly challenging when integrating systems from different organizations or with different goals and objectives. To overcome these challenges, it is important to have a clear understanding of the roles and responsibilities of each system and how they will interact with each other. This includes identifying potential areas of overlap or conflict and developing strategies to address these issues.

One way to ensure successful integration is to establish clear communication channels between the different systems and the users of each system. This includes establishing protocols for sharing information and resolving issues. Another strategy for overcoming workflow challenges is to conduct thorough testing of the integrated systems in a test environment. This can help to identify any issues or areas of concern before the systems are fully implemented. It is also helpful to monitor the systems closely after implementation to ensure that they are working as intended and to address any issues that arise.

Overall, integrating different systems requires careful planning and coordination to ensure that the workflow of each system is compatible with the workflow of the other systems. By establishing clear communication channels, training users, and testing the systems thoroughly, CCHs can overcome these challenges and achieve a successful integration.

Data Mapping - Data mapping is a critical step in integrating different systems, as it involves converting data from one system to another. One of the main challenges in this process is ensuring that the data is mapped correctly so that it can be used by the receiving system. This can be particularly challenging when integrating systems with different data structures or formats.

To overcome these challenges, it is important to have a clear understanding of the data requirements of each system and how they will be mapped to each other. This includes identifying any potential data conflicts or inconsistencies and developing strategies to address these issues. It is also important to have a deep understanding of the data mapping process and to use appropriate tools and software to automate the process and reduce errors.

- **Data Mapping -** One technical issue that can arise during data mapping is data transformation, which involves changing the format or structure of the data to meet the requirements of the receiving system. This can be a complex process, particularly when dealing with large amounts of data or complex data structures.
- **Data Validation -** Another technical issue that can arise during data mapping is data validation, which involves ensuring that the data is accurate, complete, and consistent across different systems. This can be particularly challenging when dealing with data from multiple sources or with different levels of quality.

Overall, data mapping is a critical step in integrating different systems, but it can be challenging due to differences in data structures, formats, and quality. By having a clear understanding of the data requirements of each system, using appropriate tools and software, and testing the data mapping process thoroughly, CCHs can overcome these challenges and achieve a successful integration.

Data Format - The data format is a critical consideration when integrating different systems, as it involves ensuring that the data is in a format that can be easily used by the receiving system. One of the main challenges in this process is ensuring that the data is formatted correctly and consistently across different systems. To overcome these challenges, it is important to have a clear understanding of the data requirements of each system and how they will be formatted to each other. This includes identifying any potential data format conflicts or inconsistencies and developing strategies to address these issues.

- **Data Conversion -** One technical issue that can arise during data formatting is data conversion, which involves changing the data from one format to another. This can be a complex process, particularly when dealing with large amounts of data or complex data structures.

- **Data Normalization -** Another technical issue that can arise during data formatting is data normalization, which involves ensuring that the data is consistent across different systems. This can be particularly challenging when dealing with data from multiple sources or with different levels of quality.

Overall, data format is a critical consideration when integrating different systems, but it can be challenging due to differences in data structures, formats, and quality. By having a clear understanding of the data requirements of each system, using appropriate tools and software, and testing the data formatting process thoroughly, CCHs can overcome these challenges and achieve a successful integration.

Chapter 2: Information Sharing and Partnerships

CCHs play a crucial role providing coordinated care to vulnerable populations, including older adults and people with disabilities. To achieve this goal, CCHs often work closely with aging and disability network partners, such as Area Agencies on Aging (AAAs), Aging and Disability Resource Centers (ADRCs), Centers for Independent Living (CILs), and Continuums of Care (CoCs). These organizations provide a range of services, resources, and supports to help individuals live independently, maintain their health and well-being, and access the care they need. By partnering with these organizations, CCHs can leverage their expertise and resources to provide more comprehensive and effective care to the individuals and communities they serve. In this section, we explore the ways in which CCHs collaborate with states and aging and disability network partners.

Working with Aging and Disability Network Partners

CCHs play a crucial role in coordinating health and social services for diverse populations, including older adults, people experiencing homelessness, and individuals with disabilities. To maximize the impact of their efforts and improve the quality of care, it is essential for CCHs to collaborate effectively with states and other CBOs. Understanding the distinct functions, federal reporting requirements, and unique data needs of each organization is critical for fostering successful partnerships and implementing adaptable technology solutions.

Given the diverse federal reporting requirements and the range of services provided by these organizations, it is crucial for CCHs to adopt a flexible technology solution that can adapt to the data requirements of each partner organization. This adaptability enables CCHs to facilitate seamless data sharing, improve service coordination, and meet the reporting needs of each organization. Data sharing among state health and human service agencies and CCHs can dramatically enhance care delivery and coordination. It can aid in tracking and addressing social determinants of health, improving service delivery, and reducing duplication. In some states, integrated care coordination systems allow health and human service agencies to share information about a client's services and care plans. For example, North Carolina's NCCARE360 platform connects healthcare providers with CBOs to coordinate whole-person care. Providers can send and track referrals, ensuring that persons receive the services they need. In certain communities, community care hubs and CBOs share data to improve maternal health outcomes. For instance, in Memphis, Tennessee the Shelby County Department of Health shares data with local CBOs and community care hubs to identify at-risk pregnant women and connect them with supportive services.

Adopting a flexible technology solution has several advantages:

- **Enhanced Collaboration-** By understanding the unique functions and reporting requirements of AAAs, CoCs, and CILs, CCHs can establish more effective communication channels and foster stronger partnerships with these organizations. This, in turn, leads to better-coordinated care and improved outcomes for the populations served.
- **Efficient Data Sharing-** A flexible technology solution enables CCHs to adapt to the data requirements of each partner organization, streamlining the process of data sharing and reducing redundancies. This ensures that relevant, accurate, and secure data is exchanged effectively between all parties involved.
- **Meeting Federal Reporting Requirements-** Implementing a technology solution that can adapt to the distinct reporting requirements of each organization helps to ensure that CCHs and their partners can meet their federal reporting obligations in a timely and accurate manner. This can lead to increased funding opportunities and a better understanding of the impact of their services on the populations they serve.
- **Continuous Improvement-** A flexible technology solution allows CCHs to continuously evaluate and improve their data sharing practices, ensuring that they remain responsive to the evolving needs of their partner organizations and the populations they serve. This adaptability is essential for addressing emerging challenges and ensuring the long-term success of collaborative efforts.

State NWD System Alignment with CCHs

Organizations in the disability and aging networks provide access services or are a partner to a state's access system for long-term services and supports (LTSS). To address HRSNs, CCH's leverage a state's No Wrong Door (NWD) System assets. Local NWD partners, which include AAAs, ADRCs, CILs, and other CBOs, facilitate enrollment in public programs and provide person-centered counseling and follow-up for needed services. Supporting partnerships between CBOs and healthcare organizations prevent duplicative work within the access system and create more opportunities to blend and braid funding to support access to needed services. By engaging in these partnerships, states can enhance NWD functions including the adoption of person-centered principles and person-centered philosophies to better serve people seeking services. For harmonization across the state, state leadership leading NWD efforts could support coordination of referral platforms across the state and across both public and private payers. CCHs play a key role in information referral and assistance, a core component of NWD, and serve as access points to services within a state's NWD System. CCHs can leverage state-level efforts to improve workforce, enhance person-centered counseling, and improve data and IT infrastructure.

NO WRONG DOOR No Wrong Door is a network of state agencies and community-based organizations promoting access to LTSS through coordinated points of entry. A state's NWD system assists individuals navigating health and social care services through outreach, streamlined assessments, person-centered plans, information and referral to state and community-based resources, and a governance structure that ensures these functions are available and coordinated across the state.

Best Practices for Effective Collaboration and Information Sharing

Ensuring effective data sharing and collaboration between CCHs and their network partners is essential to enhance service delivery and contribute to better outcomes for all individuals served.

1. **Establish clear communication channels-** Regular communication between CCHs and their partners help ensure that both parties understand each other's data requirements and expectations. This can involve setting up regular meetings or check-ins to discuss data collection, reporting, and any challenges that may arise.
2. **Develop standardized data definitions and formats-** Developing standardized data definitions and formats can help ensure that the data collected by the CCH is easily understood and utilized by their partners. This can also help streamline the process of transforming the data for other federal reporting.
3. **Implement interoperable data systems-** Ensuring that the data systems are interoperable can significantly improve data sharing efficiency. This may involve adopting common data standards or using data integration tools that can seamlessly exchange data between different systems.
4. **Invest in data collection and reporting tools-** Investing in modern data collection and reporting tools can help automate and streamline the data collection and reporting processes. This may include using EHRs, customer relationship management (CRM) systems, or other data management systems that can handle the unique data requirements related to federal reporting systems
5. **Customization options-** Select a technology solution that can be customized to meet the unique data collection and reporting needs of the CCH and its partners.
6. **Scalability-** Choose a solution that can grow and adapt with the evolving needs of the CCH. This will help ensure that the technology remains relevant and effective in the long run.
7. **Provide training and support-** Ensuring that both CCH and partner staff are well-trained in data collection and reporting processes can help minimize errors and improve the overall quality of the data. This may involve providing regular training sessions, workshops, or access to online resources.
8. **Collaborate on data analysis and interpretation-** CCHs and their CBO partners can work together to analyze and interpret the data collected, helping to identify trends, gaps, and areas for improvement. This collaborative approach can help ensure that both parties have a shared understanding of the data and can work together to improve service delivery/outcomes for older adults and their caregivers.
9. **Establish Clear Communication Channels-** Open and transparent communication is vital for successful collaboration between CCHs and other CBOs. Establishing regular meetings or conference calls and designating liaisons from each organization can help to facilitate ongoing communication. This enables both parties to discuss challenges, share updates, and coordinate efforts effectively.
10. **Develop Data Sharing Agreements-** Data sharing agreements are essential for outlining the roles and responsibilities of each organization and for setting expectations for data exchange. These agreements could detail the types of data to be shared, the frequency of data exchange, data ownership, privacy and security measures, and any other relevant guidelines or protocols.

11. **Ensure Correct Data Mapping and Formatting-** To ensure data accuracy and consistency, CCHs and their partners could establish and maintain a shared understanding of data mapping and formatting. This involves developing a data dictionary that defines data elements and their corresponding codes or values, as well as outlining any required data transformations or conversions.
12. **Use Appropriate Data Sharing Tools and Software-** Leveraging suitable data sharing tools and software can facilitate a seamless data exchange process. Organizations could evaluate and select tools that meet their technical requirements, support secure data transfer, are compatible with each other's data systems, and do not result in discrimination or risk discrimination if such tools meet the definition of a patient care decision support tool at 45 CFR 92.210.
13. **Test the Data Sharing Process Thoroughly-** Before fully implementing data sharing practices, it is essential to test the process to identify and resolve any issues or inconsistencies. Conducting pilot tests or simulations allows both organizations to refine their data sharing procedures and ensure that the process operates smoothly.
14. **Continuously Evaluate and Improve Data Sharing Practices**- Ongoing evaluation and improvement are vital for maintaining effective data sharing practices between CCHs and their partners. Regular reviews of the data sharing process can help identify areas for improvement, address any emerging challenges, and continuously optimize the collaboration. This ensures that both organizations remain adaptive and responsive to the evolving needs of the individuals they serve, including those with disabilities.

Data Sharing to Support Coordinating with Continuums of Care

One type of CBO that CCHs may partner with is HUD-funded CoCs. CoCs are collaborations of public, private, and nonprofit organizations working together to prevent and end homelessness. The CoC designates the CoC Lead Agency, which is an organization or government agency that administers and manages the Homeless Management Information System (HMIS). The CoC Lead Agency administers the HMIS and is also referred to as the HMIS Lead Agency. This organization is required to develop and implement a plan to address homelessness in their communities, which must include a system for collecting and reporting data on the homeless population.

Below, we provide a comprehensive understanding of the importance of data sharing between CCHs and CoCs and the challenges and opportunities associated with achieving interoperability. We will also explore the challenges that can hinder effective collaboration and information sharing, such as data privacy concerns, technical barriers, and differing data collection methods. By analyzing these challenges, we will identify opportunities to improve data sharing practices between CCHs and CoCs.

Finally, the chapter includes best practices for CCHs to effectively collaborate and share information with CoCs, focusing on developing data sharing agreements, ensuring accurate data mapping and formatting, and utilizing appropriate data sharing tools and software. By following these best practices, CCHs can strengthen their partnerships with CoCs and enhance a person's care and outcomes.

Exhibit 3. Continuum of Care and Homeless Management Information Systems Terminology

Term	Definition
CoC	A collaboration of public, private, and nonprofit organizations that work together to prevent and end homelessness.
CoC Lead Agency	An organization or government department designated by a CoC to administer and manage the CoC's HMIS.
HMIS	A software system that collects and stores data on the homeless population.
HMIS Lead Agency	An organization or government department designated by a CoC to administer and manage the CoC's HMIS.

The CoCs play a vital role in addressing homelessness and housing insecurity in the United States. They collect and maintain data on individuals and families experiencing homelessness to inform policy and program development. CoCs use data to prioritize a limited pool of housing resources. One of the most common tools used to prioritize and allocate resources for housing is the VI-SPDAT (Vulnerability Index – Service Prioritization Decision Assistance Tool). The VI-SPDAT assessment provides an individual with a score that may increase their priority ranking for housing support services. CCHs often serve individuals and families experiencing homelessness or housing insecurity, making it essential for them to share data with HMIS systems. However, sharing data between these entities can be challenging due to differences in data collection and reporting requirements, data privacy and security concerns, and technical interoperability issues.

One of the main challenges of sharing data with HMIS is ensuring that the data is accurate, complete, and consistent. CCHs and HMIS may use different data collection and reporting methods, which can make it difficult to compare and analyze data. Additionally, data privacy and security concerns must be addressed to protect the sensitive information of individuals experiencing homelessness.

Despite these challenges, there are significant opportunities associated with sharing data with HMIS. Collaboration between CCHs and CoCs can help to identify gaps in services for individuals experiencing homelessness and inform the development of targeted interventions. Sharing data can also improve the coordination of services among healthcare providers, social service organizations, and CBOs.

To effectively share data with HMIS, CCHs collaborating with CoCs c may want to consider:

- Developing a data sharing agreement that outlines the roles and responsibilities of each party, the data that will be shared, and the security measures that will be used to protect the data.
- Ensuring that their data collection and reporting methods are consistent with those of the HMIS Lead Agency and CoC.
- Implementing data quality assurance procedures to ensure that the data is accurate, complete, and consistent.
- Using data sharing tools and technologies to facilitate the sharing of data.
- Collaborating with the HMIS Lead Agency and CoC to develop and implement data sharing policies and procedures.

By implementing these strategies, CCHs can overcome the challenges of sharing data with HMIS Lead Agencies and CoCs and leverage the opportunities for improved collaboration. Sharing data helps to identify service gaps, inform targeted interventions, and enhance coordination among various

stakeholders in addressing homelessness and housing insecurity. In doing so, CCHs contribute to the overarching goal of preventing and ending homelessness while also improving the quality of care and outcomes for individuals in need.

Best Practices and Technologies for Sharing Data with HUD Funded HMIS Lead Agencies

To effectively share data with HUD-funded HMIS Lead Agencies, CCHs may need to have the ability to transform data into a format that complies with the data elements and data fields required by the HMIS. In addition to this, CCHs should follow the best practices outlined below:

- **Standardize Data Collection and Reporting Methods-** To ensure that data is accurate, complete, and consistent, CCHs have the ability to export their data and standardize their data collection in a format that is accessible to the HMIS Lead Agency. This will ensure that data can be easily compared and analyzed, and that it meets federal and state requirements.
- **Implement Data Quality Assurance Procedures-** To ensure that data is accurate, complete, and consistent, CCHs could implement data quality assurance procedures. This can include training staff members on best practices for data collection and reporting, conducting regular data audits, and using data quality metrics to monitor data accuracy.
- **Use Data Sharing Tools and Technologies-** Most, if not all, HMIS vendors have standardized data elements and data fields, and several have developed APIs for sharing data. To facilitate the sharing of data, CCHs could use these data sharing tools and technologies. These tools can help to ensure that data is shared securely and efficiently between different systems.
- **Address Technical Interoperability Issues-** Technical interoperability issues can make it challenging to share data between different systems. To address these issues, CCHs could work with HMIS Lead Agencies to develop technical solutions that support data interoperability. This can include developing common data standards and using middleware to facilitate data exchange between different systems.

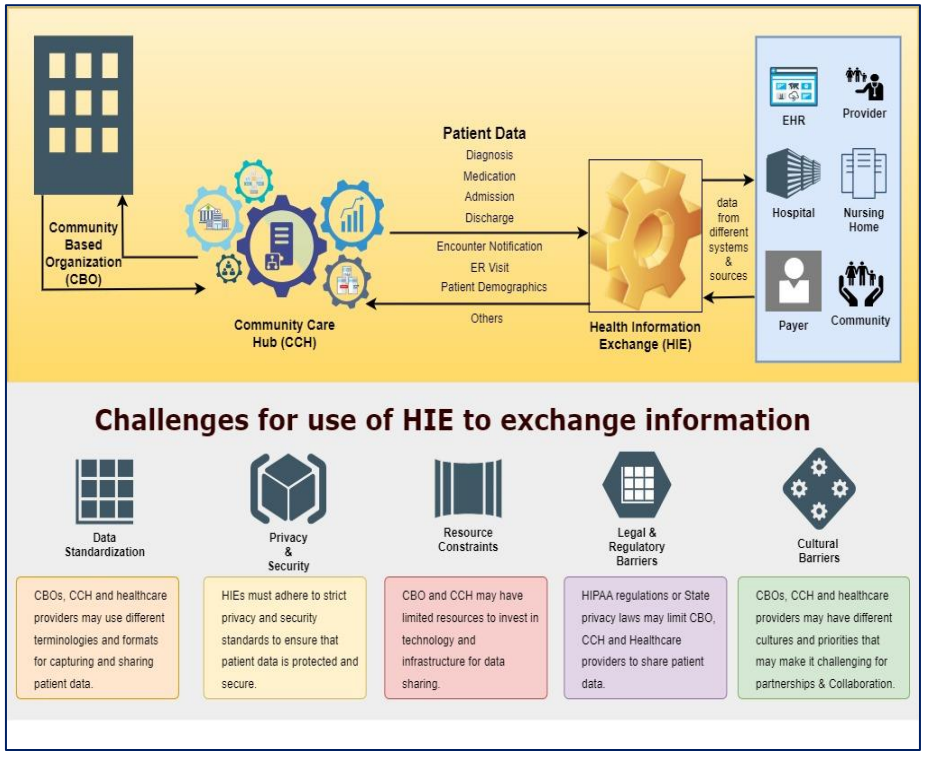
By following these best practices and using these technologies, CCHs can effectively share data with HUD-funded HMIS Lead Agencies. This will help to improve care and outcomes for individuals experiencing homelessness or housing insecurity.

In conclusion, the importance of CCHs working closely with AAAs, CoCs, and CILs cannot be overstated. By understanding the unique functions, federal reporting requirements, and data needs of each organization, CCHs can foster successful partnerships and implement flexible technology solutions that promote efficient data sharing, improve service coordination, and ultimately lead to better care and outcomes for the diverse populations they serve.

Integration with Health Information Exchanges

The use of HIEs across health and social services has gained popularity in recent years to improve coordination and information sharing between healthcare providers, payers, and other stakeholders in the healthcare system. Many states have implemented HIEs or are in the process of doing so, with the aim of improving healthcare quality, reducing costs, and promoting population health. However, there are often gaps in communication and information sharing between CBOs and healthcare providers, which can lead to fragmented and inefficient care. The use of HIEs to facilitate the exchange of information between CBOs and healthcare providers is one potential solution to this challenge.

Exhibit 4. Challenges for Integration with HIEs



Representative examples of states that have implemented initiatives to promote the use of HIEs for exchanging referral information between CBOs and healthcare providers include California, New York, and Maryland. However, a more comprehensive list of examples can be found in Appendix B of this Playbook. Despite the potential benefits of HIEs, there are several challenges surrounding the use of HIEs for exchanging referral information between CBOs and healthcare providers. These challenges include data standardization, privacy and security, resource constraints, legal and regulatory barriers, and cultural barriers.

- **Data standardization**—is a challenge because CBOs and healthcare providers may use different terminologies and formats for capturing and sharing data, which can make it difficult to exchange information between them. Standardizing data elements and formats across different systems and organizations can help to improve data interoperability and enable more seamless information sharing.
- **Privacy and security**—is another significant challenge because patient/person data is highly sensitive and must be protected from unauthorized access and disclosure. HIEs must adhere to strict privacy and security standards to ensure that data is protected and secure during transmission and storage.
- **Resource constraints**—are also a challenge because CBOs may have limited resources to invest in technology and infrastructure for data sharing, which can limit their ability to participate in

HIEs. Healthcare providers may also face resource constraints, particularly in smaller organizations, which can limit their ability to integrate with HIEs and share data with CBOs.

- **Legal and regulatory barriers—**may also limit the ability of CBOs and healthcare providers to share data, such as HIPAA Rules or state privacy laws. Addressing these barriers may require changes to policies and regulations, as well as improved education and training for stakeholders.
- **Cultural barriers—**may also exist because CBOs and healthcare providers have different cultures and priorities, which can make it challenging to establish effective partnerships and collaboration. Building trust and effective communication between stakeholders is essential for successful collaboration and information sharing.

One of the promising areas of HIE and CCH collaboration is related to the transmission of Admission, Discharge, and Transfer (ADT) alerts. ADT alerts provide real-time notifications to healthcare providers when a patient is admitted, discharged, or transferred to another facility.[9] This information is critical for CCHs as they work to address social determinants of health for persons discharging from hospitals or skilled nursing facilities.

The use of ADT alerts through EHR integration can help to improve care coordination and ensure that persons receive appropriate care, as well as help CCHs identify the payors for the individuals they might be serving. By providing real-time notifications to healthcare providers and CCHs, ADT alerts can help to ensure that persons receive timely and coordinated care, which can improve person outcomes and reduce healthcare costs. This is especially important for CCHs as they work to address social determinants of health and coordinate care across multiple organizations.

In addition to insurance information, ADT alerts can also provide valuable information about a person's medical history, medications, and allergies. This information can help CCHs to make informed decisions about a person's care and avoid potential adverse events. For example, if a person is admitted to a hospital and has a history of allergies to certain medications, the hospital can use ADT alerts to notify the care team, who can then ensure that the person does not receive those medications during their stay. The CCH can also use this information to provide additional support and resources to the person and their family.

Addressing these interoperability challenges requires a coordinated effort among stakeholders across the healthcare system, including CBOs, healthcare providers, policymakers, and technology vendors. Working together, stakeholders can overcome these challenges and realize potential benefits of HIEs for improving care coordination and addressing social determinants of health. CCHs can implement best practices for interoperability, such as a clear governance structure, establishing data-sharing agreements, implementing interoperability standards, ensuring data privacy and security, and providing staff training and support. In this way, CCHs can improve their ability to collaborate and share information, which can lead to better person outcomes and improved population health.

[9] Indian Health Service. (2023). National Patient Information Reporting System. ADT Segments: HL7 Data Transmission Guide-Appendix B. Accessed at: https://bit.ly/3O1QQ5F

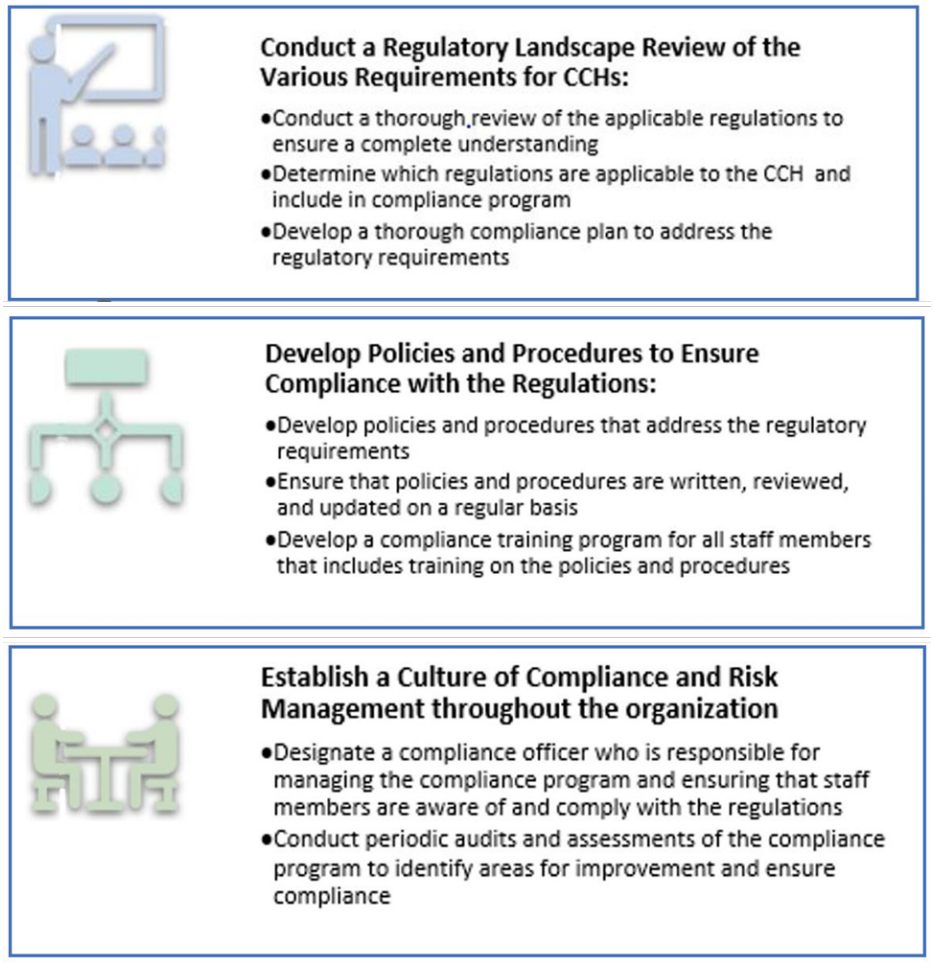
PART II:
COMPLIANCE, TECHNICAL, AND CONTRACTS: PLAYBOOK PRIMER

Chapter 3: Compliance and Regulations

Overview of Federal Laws and Regulations

Generally, CCHs must adhere to a variety of federal laws and regulations, including HIPAA, the HITECH Act, as well as the Interoperability Rule. Complying with these regulations is critical to protect the privacy and confidential information of clients and to ensure that CCHs and CBOs can share information with other entities in a secure and interoperable manner.

Exhibit 5. Compliance Framework



This chapter provides an overview of the federal regulations that CCHs and CBOs must comply with and provides best how to ensure compliance with these regulations. The chapter covers key regulations, including the HIPAA Rules, HITECH Act, OAA confidentiality, and the Interoperability Rule, and offers best practices for protecting confidential information, promoting interoperability, and developing a culture of compliance and risk management. By following the tools and resources in this chapter, CCHs and CBOs can establish robust compliance programs that protect their clients' privacy and confidential information, as well as promote information sharing and collaboration with other entities.

Interoperability and Regulation Compliance

Compliance with federal regulations is critical for CCHs to protect the privacy and confidential information of their clients, to ensure secure and interoperable information sharing, and to minimize risk. In addition to any unique requirements of partner entities, it may be helpful for CCHs to: (1) conduct a regulatory landscape review of requirements for CCHs, (2) develop policies and procedures to ensure compliance with the regulations, and (3) establish a culture of compliance and risk management throughout the

organization. A robust compliance program is essential to protecting the privacy and confidential information of clients and to ensuring secure and interoperable information sharing.

HIPAA Rules Compliance

HIPAA is a federal law that establishes national standards for protecting the privacy and security of protected health information (PHI). CCHs may or may not be a covered entity or may be working with a covered entity, such as a health plan or healthcare provider that bills electronically. Therefore, it is important to understand the HIPAA Rules to ensure compliance. If a CCH employs a healthcare provider who provides services and transmits covered transactions electronically (e.g., billing for Transitional Care Management, Chronic Care Management or Community Health Integration codes), then the CCH is considered a HIPAA covered entity and is subject to the related regulatory requirements. The Covered Entity Decision Tool is a helpful resource to identify whether an organization or individual is a covered entity under HIPAA provisions.

If a CCH needs to access PHI as a partner to a health care organization, they will first be required to sign a business associate agreement or contract. Business associate agreements are crucial for CCHs when partnering with covered entities. These contracts or written arrangements must contain the elements specified at 45 CFR 164.504(e). For instance, the contract must describe the permitted and required uses and disclosures of PHI by the business associate, provide that the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law, and require the business associate to use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by the contract.

If a covered entity knows of a pattern of activity or practice of the business associate that constitutes a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, termination of the contract or arrangement is required. If termination of the contract or agreement is not feasible, a covered entity is required to report the issue to the HHS Office for Civil Rights. To help CCHs create effective business associate agreements, HHS has provided a Sample Business Associate Contract that outlines key elements/provisions that should be included in these agreements.[10]

HIPAA regulations also include the Privacy Rule and Security Rule. The Privacy Rule sets forth regulations for the use and disclosure of PHI by covered entities and their business associates, including CCHs when applicable. The Security Rule requires covered entities and their business associates, including CCHs when applicable, to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. Failure to comply with HIPAA regulations can result in significant financial and legal penalties.

The HIPAA Privacy Rule Minimum Necessary Standard
The HIPAA Privacy Rule minimum necessary standard requires covered entities and their business associates to limit the use, disclosure, and request of protected health information to only what is necessary to accomplish the intended purpose. This protects patient privacy by limiting access to PHI to only those who need it to provide care or perform their job duties.

[10] U.S. Department of Health and Human Services. (2023). HHS Health Information Privacy. Accessed at: https://bit.ly/42I410j.

Exhibit 6. The Security Rule

The HIPAA Security Rule requires covered entities and their business associates, including CCHs when applicable, to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).

1. Administrative Safeguards:
   - ✓ Security Management Process: Identify and analyze potential risks to ePHI and implement security measures to reduce risks to a reasonable and appropriate level.
   - ✓ Security Personnel: Designate a security official responsible for developing and implementing security policies and procedures.
   - ✓ Information Access Management: Implement policies and procedures for role-based access to ePHI, limiting access based on the user's role.
   - ✓ Workforce Training and Management: Provide training on security policies and procedures, authorize and supervise workforce members working with ePHI, and apply sanctions against those who violate policies and procedures.
   - ✓ Evaluation: Periodically assess the effectiveness of security policies and procedures in meeting the Security Rule requirements.
2. Physical Safeguards:
   - ✓ Facility Access and Control: Limit physical access to electronic information systems and the facility or facilities in which they are housed while ensuring authorized access is allowed.
   - ✓ Workstation and Device Security: Implement policies and procedures for proper use of and access to workstations that access electronic protected health information and electronic media that contain electronic protected health information, as well as their transfer, removal, disposal, and reuse to protect ePHI.
3. Technical Safeguards:
   - ✓ Access Control: Implement technical policies and procedures to allow only authorized persons to access ePHI.
   - ✓ Audit Controls: Implement hardware, software, or procedural mechanisms to record and examine access and activity in information systems containing or using ePHI.
   - ✓ Integrity Controls: Implement policies and procedures to ensure ePHI is not improperly altered or destroyed and use electronic measures to confirm it.
   - ✓ Transmission Security: Implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic network.

In addition to these safeguards, covered entities and their business associates must also conduct regular security risk assessments, develop and implement contingency plans for emergencies or system failures, and manage electronic media and hardware containing ePHI. The Security Rule allows flexibility for covered entities and their business associates to implement measures appropriate for their specific environment, size, and resources. To locate a HIPAA Security Rule compliance checklist for basic system requirements, please refer to the **Appendix B - *HIPAA Security Rule Toolkit***.

Exhibit 7. The Privacy Rule

The HIPAA Privacy Rule establishes standards for the use and disclosure of PHI by covered entities, such as healthcare providers that bill electronically, health plans, healthcare clearinghouses and their business associates, and CCHs when applicable. The Privacy Rule aims to safeguard the privacy of individuals' health information while allowing the necessary flow of health data for treatment, payment, and healthcare operations. Key provisions of the Privacy Rule include:

1. **Standards for Use and Disclosure of PHI:**
   - ✓ The Privacy Rule limits and sets forth conditions on how covered entities and their business associates can use and disclose PHI. This includes obtaining proper authorization for purposes beyond treatment, payment, and healthcare operations or otherwise permitted or required by the Privacy Rule.
2. **Notice of Privacy Practices:**
   - ✓ Covered entities must provide a notice of privacy practices. This notice should describe how the organization uses and discloses PHI, individuals' rights concerning their PHI, and the covered entity's legal duties with respect to PHI.
3. **Minimum Necessary Standard:**
   - ✓ The Privacy Rule requires covered entities and their business associates to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose. Covered entities and their business associates must also develop and implement policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce.
4. **Safeguards to Protect PHI:**
   - ✓ Covered entities and their business associates are required to implement administrative, physical, and technical safeguards to protect the privacy of PHI. These safeguards should be tailored to the organization's size, complexity, and capabilities.
5. **Incident and Breach Response:**
   - ✓ The Security Rule mandates covered entities and their business associates to develop and implement procedures for responding to security incidents involving PHI. The Breach Notification Rule requires notification to the individual and the Department of Health and Human Services' Office for Civil Rights in the case of a breach of unsecured PHI.
6. **Business Associate Compliance:**
   - ✓ Covered entities must ensure that their business associates who handle PHI on their behalf also comply with the Privacy Rule. This is typically done through business associate agreements, which outline the responsibilities and expectations for both parties regarding PHI protection.

To find a sample HIPAA Privacy Rule compliance checklist for software systems, please refer to the **Appendix B - *Sample HIPAA Privacy Rule Compliance Checklist***.

Business Associate Agreement

A business associate agreement (BAA) is a written contract that specifies each party's responsibilities when it comes to PHI. Under the HIPAA Rules, covered entities are required to only work with business associates who sign a BAA and provide satisfactory assurances to protect PHI. These assurances must be in writing, in the form of a contract or other agreement between a covered entity and a business associate, such as the CCH. CCHs may contract with various other organizations to help coordinate care; in these instances, these CBOs would be considered business associate subcontractors and would also need to comply with the HIPAA Rules.

HHS can investigate business associates and subcontractors for HIPAA compliance, not just covered entities. This means that organizations must have a BAA for all three levels to meet the requirements of the HIPAA Rules. It is in the best interest of all parties to have an agreement since all three classifications are responsible for protecting PHI.

The business associate agreement with a subcontractor must include specific information, such as the permitted and required uses of PHI by the business associate/subcontractor, a requirement that the business associate and subcontractor will not use or further disclose PHI other than as permitted or required by the contract or as required by law, and a requirement that the business associate/subcontractor uses appropriate safeguards to prevent inappropriate PHI use or disclosure.

Having a signed agreement between covered entities, business associates, and business associate subcontractors documents that the business associate understands the necessity of safely handling PHI. It is crucial that CCHs work only with business associates/ subcontractors who are willing to commit to the safe handling of PHI and that these commitments are documented in a written agreement.

To comply with the HIPAA Rules, CCHs should develop and implement policies and procedures which comply with the Privacy Rule and Security Rule. This includes conducting a thorough risk assessment to identify potential vulnerabilities and implementing measures to mitigate risk. Staff members should be trained in HIPAA Rules and the organization's policies and procedures, and business associates and vendors should also comply with HIPAA Rules.

Best practices for protecting PHI include developing and implementing policies and procedures to protect PHI, assessing the security of electronic devices, developing policies and procedures for responding to security incidents and breaches of PHI, and conducting regular training for staff members on the importance of protecting PHI.

In summary, compliance with HIPAA Rules is required for HIPAA covered entities and their business associates, which may include CCHs. Understanding HIPAA Rules and requirements is essential to ensure compliance and protect the privacy and security of clients' PHI. Failure to comply with the HIPAA Rules can result in significant financial and legal penalties. By developing and implementing policies and procedures, assessing risk, and training staff members, CCHs can mitigate the risk of non-compliance and ensure the success of their organization.

Exhibit 8. Covered Entities and Business Associates

	Covered Entity	Business Associate
Definition	A health plan, healthcare clearinghouse, or healthcare provider that electronically transmits any health information in connection with transactions for which HHS has adopted standards.	A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of a covered entity.
Examples	Hospitals, physicians, health plans, healthcare clearinghouses.	CCHs, third-party billing companies, consultants, vendors that provide software or hardware used to store or transmit PHI*.
Compliance Requirements	Must comply with HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.	Must comply with their business associate agreement, the HIPAA Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule with respect to functions performed on behalf of a covered entity.
Required Contracts	Must have contracts or other arrangements in place that ensure the business associate also complies with the HIPAA Privacy Rule.	Must have contracts or other arrangements in place that ensure the business associate also complies with the HIPAA Privacy Rule.

	Covered Entity	Business Associate
Responsibility for PHI	The covered entity is responsible for ensuring the privacy and security of PHI.	The business associate is responsible for safeguarding PHI in the same way that the covered entity would. Business associate is also responsible for ensuring subcontractors are safeguarding PHI.
Reporting Breaches	Covered entities must report any breaches of unsecured PHI to the Department of Health and Human Services.	Business associates must report any breaches of unsecured PHI to the covered entity.

*While CCHs are required to sign a BAA when operating as a business associate to a covered entity, their CBO partners may be required to sign a BAA with the CCH or the covered entity depending on the relationship with the covered entity. The approach taken is generally dependent upon the covered entity.

Health Information Trust Alliance

HITRUST is a widely recognized, privately held organization that has established the Common Security Framework (CSF), a comprehensive, certifiable, and scalable security framework specifically designed for the healthcare industry. The HITRUST CSF was created to address the unique security and regulatory challenges faced by healthcare organizations and their partners, including protecting sensitive patient information and maintaining compliance with regulations such as the HIPAA Rules and the General Data Protection Regulation (GDPR).

While HITRUST certification is not mandated by law, it has become an increasingly important factor for healthcare providers, payors, and their partners as a means of demonstrating a commitment to robust security practices. Many healthcare organizations now require their partners and vendors to be HITRUST certified or adhere to the HITRUST CSF, as it provides a standardized approach to security and reduces the risk of data breaches and non-compliance.

The basic security requirements of HITRUST certification involve implementing and maintaining a set of controls and processes that encompass the following areas (not all inclusive):

- **Information Protection Program.** Establishing a comprehensive program to ensure the protection of sensitive information and maintain compliance with applicable regulations.
- **Endpoint Protection**. Implementing security measures for devices such as computers, servers, and mobile devices to prevent unauthorized access and data breaches.
- **Portable Media Security.** Securing portable media devices such as USB drives and external hard drives to protect data from unauthorized access and loss.
- **Mobile Device Security.** Ensuring the secure use and management of mobile devices, including smartphones and tablets, to prevent unauthorized access and data breaches.
- **Wireless Security.** Implementing security measures for wireless networks to prevent unauthorized access and protect sensitive information.
- **Configuration Management.** Maintaining a standardized and secure configuration for IT systems and applications to reduce vulnerabilities and prevent security incidents.
- **Vulnerability Management.** Regularly identifying, assessing, and remediating vulnerabilities in IT systems and applications to reduce the risk of security breaches.
- **Network Protection.** Implementing security measures to protect network infrastructure, including firewalls, intrusion detection and prevention systems, and network segmentation.

- **Transmission Protection.** Securing data transmission through encryption and other security measures to prevent unauthorized access and data breaches.
- **Password Management.** Establishing and enforcing strong password policies to protect user accounts and sensitive information.
- **Access Control.** Implementing a role-based access control system to restrict access to sensitive information and systems on a need-to-know basis.
- **Audit Logging and Monitoring.** Collecting, storing, and analyzing audit logs to detect security incidents, ensure compliance, and support investigations.
- **Third-Party Assurance.** Assessing and managing the security risks associated with third-party vendors and partners to ensure the protection of sensitive information.

By adhering to the HITRUST CSF and achieving certification, CCHs can demonstrate their commitment to protecting sensitive patient information and meeting the high security standards required by the healthcare industry. This can help build trust with healthcare providers, payors, and other partners, while also reducing the risk of security breaches and non-compliance.

HITRUST and HIPAA Security Rule

HITRUST and the HIPAA Security Rule both aim to protect sensitive health information, but they differ in scope, focus, and requirements. The HIPAA Security Rule is a federal regulation specifically addressing the protection of ePHI and is mandatory for covered entities and their business associates. On the other hand, HITRUST is a private organization that developed the CSF, a comprehensive, certifiable, and scalable security framework for the healthcare industry. While HITRUST certification is not legally required, it is considered a best practice and often demanded by healthcare organizations and their partners.

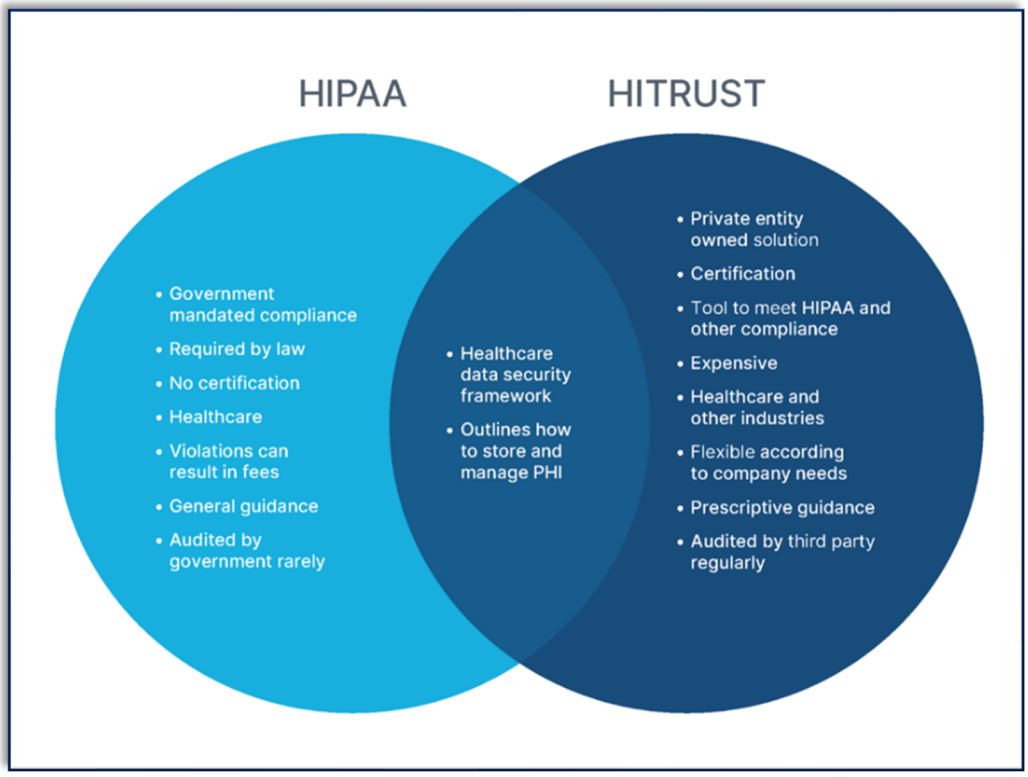
Exhibit 9. HITRUST Framework and HIPAA Security Rule.

	HITRUST	HIPAA Security Rule
Scope	HITRUST is a private organization that developed the CSF, a comprehensive, certifiable, and scalable security framework designed for the healthcare industry.	The HIPAA Security Rule is a federal regulation that addresses the safeguarding of ePHI. It is mandatory for all HIPAA covered entities and business associates.
Focus	HITRUST takes a more comprehensive approach, addressing not only ePHI but also other types of sensitive data, such as PII and financial data. It also aligns with other regulations and standards, such as GDPR, NIST, ISO, and PCI DSS.	The HIPAA Security Rule focuses on protecting the confidentiality, integrity, and availability of ePHI by implementing administrative, physical, and technical safeguards.
Requirements	The requirements are defined by the HITRUST organization and are more prescriptive than HIPAA, covering a broader range of security controls and risk management practices. The HITRUST CSF offers a more structured and detailed approach to implementing security measures.	The requirements are defined by HHS and include a set of required and addressable safeguards that covered entities and their business associates must implement for ePHI.
Certification	The HITRUST CSF offers a certification process that includes third-party assessments, providing a standardized method for demonstrating compliance with its framework.	There is no official certification process for HIPAA compliance. Organizations must conduct self-assessments and implement safeguards to demonstrate compliance.

	HITRUST	HIPAA Security Rule
Flexibility	HITRUST is more prescriptive, with a larger number of security controls and specific implementation guidance, which may be more rigid but also offers a clearer path to compliance.	The HIPAA Security Rule is more flexible in its requirements, allowing organizations to implement security measures that best suit their needs, resources, and risk profile.

*CCHs, as well as their BA subcontractors, when operating as a business associate are required to comply with the standard mandated by the covered entity as part of their business associate agreement.

Exhibit 10. HITRUST and HIPAA Scope (Source: https://bit.ly/3pBeBHy)



HITRUST and HIPAA Security are related but distinct frameworks. HITRUST provides a more comprehensive and detailed approach to security and risk management, while the HIPAA Security Rule focuses specifically on the protection of ePHI. Organizations that are compliant with HITRUST CSF are often well-prepared to meet HIPAA Security Rule requirements, but the reverse may not always be true due to the broader scope and additional controls in HITRUST.

Promising Practices

Promising Practice: Select Vendors Who Are HITRUST Certified

As CCHs collaborate with various healthcare providers, payors, and other partners, ensuring the security and compliance of sensitive health information becomes crucial. A promising practice is to select vendors who are already HITRUST certified and to engage a third party for monitoring downstream partners' adherence to HITRUST standards. This approach helps minimize security risks, demonstrate commitment to data protection, and build trust with partners and stakeholders.

Selecting HITRUST Certified Vendors

- **Develop Vendor Selection Criteria.** When evaluating potential vendors, include HITRUST certification as one of the essential criteria in the selection process. This ensures that vendors have already demonstrated their commitment to robust security practices and compliance with healthcare industry standards.
- **Request Evidence of Certification.** Ask potential vendors to provide their HITRUST certification documents or other evidence proving their adherence to the HITRUST CSF. This enables CCHs to verify the vendor's compliance and reduce the risk of partnering with a non-certified vendor.
- **Evaluate Vendor's Security Practices.** Assess the vendor's overall security posture and history by examining their security policies, procedures, and any past incidents. This provides insight into the vendor's commitment to security and their ability to maintain compliance over time.
- **Incorporate HITRUST Requirements into Contracts.** Include specific requirements related to HITRUST compliance in contracts and agreements with vendors. This ensures that the vendor remains accountable for maintaining their certification and adhering to the HITRUST CSF throughout the partnership.

Ensuring Downstream Partners' Adherence to HITRUST

As CCHs continue to expand their network of partners and vendors, it becomes essential to ensure that all stakeholders involved maintain the same level of commitment to security and compliance. A crucial aspect of this process is making sure that downstream partners also adhere to HITRUST standards. By taking a proactive approach to monitoring and supporting downstream partners, CCHs can strengthen their security posture and reduce the risk of potential data breaches.

- **Engage a Third-Party Assessor.** Contract with a reputable third-party assessor who specializes in HITRUST assessments to monitor and evaluate downstream partners' compliance with HITRUST standards. This provides an unbiased assessment of partners' security practices and ensures they are held accountable for maintaining compliance.
- **Establish Clear Expectations.** Clearly communicate the requirement for downstream partners to adhere to HITRUST standards in contracts and agreements. This helps set expectations from the outset and emphasizes the importance of maintaining robust security practices.
- **Conduct Regular Assessments.** Schedule periodic assessments of downstream partners to verify their ongoing adherence to HITRUST standards. This helps identify any gaps or issues in their security practices and ensures that they continue to maintain compliance over time.

- **Provide Support and Resources.** Offer guidance and resources to downstream partners to help them understand and implement HITRUST requirements effectively. This may include sharing best practices, offering training sessions, or providing access to tools and templates that can facilitate compliance efforts.
- **Foster Collaboration and Communication.** Establish open lines of communication with downstream partners to encourage collaboration and address any security concerns or issues proactively. This helps create a culture of shared responsibility for maintaining compliance and protecting sensitive health information.

Older Americans Act

The Older Americans Act (OAA) is a federal law first enacted in 1965. It is designed to provide funding for a range of services and programs that support older adults and their caregivers. The OAA is administered by ACL. State units on aging receive funding from the OAA to distribute to area agencies on aging (AAAs) to administer the OAA grant programs regionally. They may also act as a single planning and service area, in which they directly administer the OAA grant programs. The goal of the OAA is to help older adults age with dignity and independence in their homes and communities.

The OAA provides funding for a variety of programs and services, including:

- **Nutrition Programs.** The OAA provides funding for programs like Meals on Wheels, which delivers nutritious meals to older adults who are homebound or have difficulty preparing meals for themselves.
- **Caregiver Support.** The OAA provides funding for programs that support family caregivers, including respite care, counseling, and training.
- **Health Promotion and Disease Prevention.** The OAA funds programs that promote healthy aging and prevent chronic disease, such as falls prevention programs and chronic disease self-management programs.
- **Elder Abuse Prevention.** The OAA funds programs that help prevent elder abuse, neglect, and exploitation.
- **Transportation Services.** The OAA provides funding for transportation services, such as senior transportation programs, which help older adults get to medical appointments, grocery stores, and other essential destinations.

Many CCHs are operated by area agencies on aging and may allocate a portion of their OAA funds to support and provide services to older adults who meet the requirements for the various programs. When this is the case, the CCH should be aware of the privacy and confidentiality provisions of the OAA. Many states require that programs and services that receive funding under the Act have procedures in place to protect the privacy and confidentiality of older adults. In general, these procedures often include the following:

- A written policy that explains how the program or service will protect the privacy and confidentiality of older adults
- A system for collecting and storing personal information in a secure manner
- A system for accessing and using personal information only for authorized purposes
- A system for responding to requests for access to personal information

- A system for reporting violations of privacy and confidentiality

The state agencies that administer the OAA often also prohibit the disclosure of personal information about an older adult without the individual's consent, except in certain limited circumstances. These circumstances include:

- When disclosure is required by law
- When disclosure is necessary to protect the health or safety of the individual or another person
- When disclosure is necessary for the administration of the OAA or another Federal program

While the OAA provides general guidance regarding privacy and confidentiality, each state unit on aging is ultimately responsible for developing policies and procedures in accordance with all provisions of the OAA to ensure that older adults' personal information is used only for authorized purposes.

Chapter 4: Technical Requirements

As CCHs continue to emerge as essential components of the healthcare system, it is critical that they have the necessary technical and IT infrastructure in place to maximize efficiency and streamline service delivery. CCHs must comply with relevant regulatory requirements, such as data privacy and security regulations, healthcare standards, technical infrastructure best practices, and other legal and regulatory mandates. IT systems used in CCHs should be designed and configured to meet these requirements. CCHs are meant to coordinate several business functions and routine tasks on behalf of CBOs that are part of the network. This structure requires a common set of administrative processes as well as appropriate IT systems to support those processes. CCHs often provide support and infrastructure necessary for smaller CBOs in their network to deliver services through health care contracts. On the other hand, larger CBOs may choose to maintain their own IT systems but integrate with the CCH's IT systems to be part of the network. Therefore, the IT systems at the CCH level play a critical role in both directly supporting CBO business functions as well as serving as an integration platform for the network.

While the previous chapter focused on the business functions to be supported by this common CCH IT system, this chapter focuses on the under-the-hood technical requirements that are often not directly visible but are equally important to ensure seamless operations. The following subsections provide an overview of the pertinent technical requirements. It is worth noting that each of these subsections represent a wide range of technical considerations and options. Therefore, this Playbook is meant to serve as a quick checklist of those considerations along with the references for further details.

Security and Data Privacy Considerations

Chapter 2 of this Playbook provided an overview of relevant security and privacy regulations that will apply to the CCH operations. Those include the HIPAA Rules as well as HITRUST security framework. This section further goes into the details of the technical requirements applicable under those regulations as well as the technical safeguards to be implemented in the IT system.

Overview of Related Regulatory Guidelines

In addition to the commonly mentioned security and privacy standards and frameworks, there are some other important policies and guidelines that are applicable in specific circumstances as described below.

Federal Information Security Management Act of 2002 (FISMA)

FISMA was passed in 2002 by the United States Congress and generally requires federal agencies to implement information security plans to protect sensitive data. FISMA compliance requires adhering to data security guidance specified by FISMA that are further specified in the detailed compliance documents developed and maintained by the National Institute of Standards and Technology (NIST). FISMA applies to federal agencies, contractors, or other sources that provide information security for the information and information systems that support the operations and assets of a federal agency.

FISMA and NIST guidance documents provide the following:

- Minimum security requirements for establishing information security solutions and protocols
- Recommendations on the types of security systems implemented by federal government agencies and approved third-party vendors
- Standardized risk assessment and auditing practices based on the severity of agencies' security risk levels.

Exhibit 11. FISMA Compliance Levels

Low Impact	Moderate Impact	High Impact
• The loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. • The compliance measures for those systems or types of data need only meet the low compliance level.	• The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. • The compliance measures for those systems or types of data need to meet the medium compliance level.	• The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. • The compliance measures for those systems or types of data need to meet the highest compliance level.

FISMA Security Controls refer to the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Determining which FISMA compliance level is applicable to a specific system or data require a good understanding of the security controls applicable at all three levels and documenting how the system adherence to those controls in the various key areas defined by the NITS guidance documents.

More details about FISMA can be obtained from the NIST FISMA background website here: https://csrc.nist.gov/Projects/risk-management/fisma-background.

Substance Use Disorder 42 CFR Part 2

42 CFR Part 2 regulations (Part 2) serve to protect patient records created by federally assisted programs for the treatment of substance use disorders. The information protected by 42 CFR Part 2 is any information disclosed by a covered program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem, or as a participant in a covered program. With limited

exceptions, 42 CFR Part 2 requires patient consent for disclosures of protected health information even for the purposes of treatment, payment, or healthcare operations (TPO) that are generally exempted under the HIPAA Rules. Part 2 generally requires a patient's written consent before making a disclosure of protected records. Patient consent must always be written and include specific information about the recipient of the records and the records to be shared.

42 CFR Part 2 may be relevant for CCHs and participating CBOs if they are directly providing substance use disorder services under federally assisted programs or may be receiving recovery support services referrals from other organizations providing substance use disorder treatment services. This may include referrals to recovery-oriented settings for outpatient services, clinically managed low-intensity residential facilities, transitional/supportive housing, or other community-based treatment and recovery service providers. When a CCH has participation of such organizations within their network, it will be important to keep 42 CFR Part 2 under consideration, assess the applicability of the rule, and make appropriate decisions about integration and data exchange that could be impacted under this rule.

More details can be obtained from the SAMHSA regulations site here: https://www.samhsa.gov/about-us/who-we-are/laws-regulations/confidentiality-regulations-faqs.

Medicaid Information Technical Architecture (MITA)

MITA is an initiative of the CMS Center for Medicaid & State Operations (CMSO). MITA is intended to foster integrated business and IT transformation across the Medicaid enterprise to improve the administration of the Medicaid program. MITA framework focuses on the three different aspects of the system architecture: business, information, and technical. MITA's vision for state Medicaid organizations emphasizes the following characteristics:

- A patient-centric view not constrained by organizational barriers
- Common standards with, but not limited to, Medicare
- Interoperability between state Medicaid organizations within and across states
- Web-based access and integration
- Software reusability
- Use of COTS software
- Integration of public health data

MITA has evolved over several years. MITA 3.0 is the latest major release that updates MITA 2.0 published in 2006. The latest version incorporates the availability of new technologies, such as cloud computing service-based architecture, and reflects new and recently updated legislation, including HIPAA, HITECH, Affordable Care Act (ACA), and Children's Health Insurance Program Reauthorization Act (CHIPRA). MITA 3.0 also adds a new section to the framework to assist states in the preparation of the State Self-Assessment (SSA) and Advanced Planning Documents (APD) which are used by states to obtain federal financial participation for the costs of IT systems.

Although MITA may not appear to be directly relevant to CCH operations, it comes into play when CCH system components need to be integrated with the state Medicaid enterprise systems and may be leveraging any federal funding made available to states under the APD process.

More details about MITA framework can be obtained from the CMS MITA 3.0 website here: https://www.medicaid.gov/medicaid/data-systems/medicaid-information-technology-architecture/medicaid-information-technology-architecture-framework/index.html.

HIPAA Rules Safeguards

Under HIPAA Rules, individually identifiable health information should be protected with reasonable safeguards to ensure its confidentiality, integrity, and availability and to protect against reasonably anticipated, impermissible, intentional, or unintentional use or disclosures. These safeguards emphasize that trust in electronic health information exchange can only be achieved if reasonable safeguards are in place. The HIPAA Privacy Rule supports the safeguards by requiring covered entities and their business associates to implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. The HIPAA Security Rule requires covered entities and their business associates to implement appropriate administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of ePHI. These three types of safeguards are depicted in Exhibit 12 below.

Administrative Safeguards are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information. These requirements cover training and procedures for employees regardless of whether the employee has access to PHI or not. These standards include:

- **Security Management Process.** A covered entity and their business associates must implement security measures that will help to reduce vulnerabilities in ePHI security. A key part of this standard is conducting a thorough HIPAA risk assessment.
- **Security Personnel.** The rule requires that a security official is designated who is responsible for developing and implementing security policies and procedures.
- **Information Access Management.** This standard focuses on restricting unnecessary access to ePHI meaning that only the appropriate personnel have access to that data only when it is appropriate.
- **Workforce Training and Security Awareness.** This standard requires that employees complete an annual HIPAA training and be educated on the organization's specific security procedures. The organization must also have and apply sanctions against any employee who violates these security procedures.
- **Evaluation.** HIPAA Security Rule requires covered entities and their business associates to perform recurring risk assessments as part of their security management processes. The HIPAA Risk Assessment, also called a Security Risk Assessment, will help to determine which security measures are reasonable and appropriate for a particular covered entity or business associate.

Exhibit 12. Safeguards Under HIPAA Security Rule

Physical Safeguards are the physical measures, policies, and procedures for protecting ePHI within electronic information systems, equipment, and the buildings they are housed in from natural and environmental hazards and unauthorized intrusion. Common examples of physical safeguards include:

- **Access Control.** These are procedures that limit access to the facilities that contain information systems like computers and servers.
- **Workstation and Device Security**. These pertain to the usage of workstations, which can be any computers or devices as well as the information contained within it.

Technical safeguards are the technology and policies and procedures for its use that protects ePHI as well as control access to that data. This can often be the most challenging regulation to understand and implement.

- **Access Control.** A covered entity must put in place policies and procedures that allow only authorized individuals to access ePHI.
- **Audit Control.** Covered entities must implement procedures through hardware or software that record and monitor access to systems that contain ePHI.
- **Integrity Controls.** Organizations must have procedures in place to maintain that ePHI is not altered, destroyed, or tampered with.
- **Transmission Security.** A covered entity must implement security measures that protect against unauthorized access to ePHI that is being transmitted over an electronic network.

More details about HIPAA Security Rule can be obtained from the HHS HIPAA Security Rule summary website here: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

Security and Privacy Contract Checklist

Since there are several rules, regulations, and industry best practices applicable for the security and privacy of information systems, it is important to embed these requirements more explicitly in the IT system's related contract. Many of these security requirements are based on ensuring the HIPAA Rules safeguards described in the previous sections. This subsection provides an overview of what terms should be expected in contract or expected IT security plan deliverables.

Baseline Context

- **Primary Contract Data.** Primary contract data includes all data collected or generated under contract including, but not limited to PHI, PII, and other confidential data

- **Personnel.** All employees and any other persons who have access to the network subcontractor's facilities, systems, or primary contract data
- **Applicability.** Access (physical or logical) to contract data or operating a system containing contract data that need to be protected
- **Information Security Laws, Regulations, Policies.** Federal policies such as HIPAA, HITECH, FISMA, etc. as well as other state and local policies

General IT Security Terms

- **Security Program Requirements.** Establish and maintain a comprehensive security program that has the physical, administrative, and technical safeguards
- **Program Updates.** Security program to be updated as necessary to comply with changes in federal, state, and local laws and regulations pertaining to the privacy and protection of primary contract data
- **Policy and Procedure Updates.** Review and update security policies and procedures annually and provide a copy when requested
- **Designated Account Security Representative.** Provide a designated focal point (i.e., Security Officer) with responsibility for day-to-day security management
- **Termination Due to Security Breach.** Contract may be terminated without further liability if there is a material security breach
- **Return and Destruction of Data.** Provide all contract data and permanently delete data in their environment within specified period after termination
- **Security Incident Response and Reporting.** Notify and report any security breach including unauthorized access to data and violation of security/privacy laws
- **Security Assessments.** Perform a security assessment to determine the compliance of overall security policies and standards
- **Subcontractor Security Requirements.** Contractor's security program must meet certain minimum requirements and provide evidence documentation
- **Training of Personnel.** Contractor's security program must include minimum security and privacy training to each person involved

Minimum Security Requirements

- **Password Requirements.** Minimum password length; combination of letters in upper and lower case, numbers, and special characters; password change frequency (days), disallow reuse of the last few passwords, etc.
- **Access Control.** Employ physical and logical access control mechanisms to prevent unauthorized access to facilities and systems
- **Unique Accounts.** Each individual requiring unique user account and not share with other users
- **Multi-factor Authentication (MFA).** Use of MFA (also referred as Two-Factor Authentication) to authenticate user through another device and method
- **Authorization Roles.** Access to facility and/or system must be limited to personnel on need-to-know basis as categorized under various authorization roles

- **Timely Revocation/Termination of Access.** Access to the facility and/or system must be terminated immediately after the personnel leaves or access no longer needed
- **Data Transmission and Storage.** Data will be secured and encrypted during transmission and at rest, and data access through personal devices will not be allowed
- **Security Patch Management.** Maintain and patch/remediate all systems, devices, firmware, operating systems, applications, and other software
- **Network Security.** Deploy appropriate firewall, intrusion detection/prevention, and network security technology in the operation of the systems and facilities
- **Malicious Code Protection.** All workstations and servers must have anti-virus software current with the latest definitions and configured to run real-time scanning

More details about the details of these security and privacy contract terms can be found in Appendix F Sample IT Security Contract Terms.

System Infrastructure

CCHs leverage economies of scale to streamline administrative functions and operational infrastructure for the entire network of participating CBOs. That means that the CCH's systems must be able to handle the large number of users and transactions expected for all CBOs combined. This section describes various technical considerations regarding architecture and infrastructure of the CCH systems.

A robust system infrastructure and security measures are critical for smooth and secured operations of the systems. The system infrastructure includes the deployment environment, physical or virtual servers, storage, network, scaling mechanisms, load balancing, firewalls, intrusion detection and prevention, encryption, regular security audits, and other measures to protect against unauthorized access, data breaches, and other security protocols. Overall environment set up with the necessary infrastructure for deploying the systems is commonly referred to as the hosting environment.

System Hosting Environment

While the architecture considerations described in the Chapter 6 provide tools for the system design, many of those are also directly or indirectly influencing the system hosting environment decisions. The CCH will need to consider those along with various hosting options to determine what will be appropriate infrastructure to meet their specific needs. If the infrastructure resources are not allocated adequately, the users as well as backend data processing will likely experience performance issues. If the infrastructure resources allocated are more than necessary to support future demand, then that will likely cost a lot more for initial deployment. The infrastructure will have to be 'right sized' initially, but with flexibility to scale up/expand quickly when needed.

There are several key decision factors regarding hosting infrastructure and configuration:

- Who operates the physical facilities ("datacenters") that house the IT infrastructure, providing power, cooling, physical security, network connectivity, etc.
- Whether the infrastructure itself is dedicated to a specific system ("single-tenant"), or part of a pool of shared resources, available on-demand to multiple clients ("multi-tenant"), or in large public/private cloud ("cloud hosting").

Based on above considerations and decision factors, following are the most commonly chosen hosting options.

Exhibit 13. Hosting Environment Options

Co-located Data Center	The shared datacenter provider offers space, power, physical security, and network connectivity, but the organization (e.g., CCH) renting that capacity manages the environment on their own in a "single tenant" configuration
Managed Hosting by the Data Center	The datacenter provider operates and manages the IT infrastructure as well as the physical facility where it resides in a "single tenant" configuration designed for and dedicated to the organization
Managed Hosted by a Third Party	The shared datacenter provider offers space, power, physical security, and network connectivity, but another third-party organization (e.g., vendor contracted with CCH) is managing the environment in a "single tenant" configuration
Private Cloud	In the private cloud environment, the provider manages all facilities and IT infrastructure but uses modern "virtualization" technologies to pool this infrastructure and make it available on a flexible, pay-by-usage basis to specific organization or related organizations
Public Cloud	The public cloud extends the cloud computing similar to the private cloud environment but shared across many organizations

Irrespective of hosting environment, there needs to be a contractual Service Level Agreement (SLA) to ensure that the services provided by the hosting provider meet the minimum expectations. The first objective of all SLAs should be to motivate appropriate behavior, be easily collectible, and set reasonable expectations for performance. The SLA should include a description of the services to be provided, expected service levels, metrics and how they will be measured including frequency, the duties and responsibilities of each party, the remedies or penalties for not meeting expected standards, and a protocol for reviewing and updating metrics. Defined and implemented correctly, SLAs provide a mechanism for productive improvement in performance and prioritization of business needs instead of punitive actions. Key metrics include system availability, service desk responses, service availability, service levels, and resolution/response times based on criticality.

Cloud Hosting

Although datacenters and private cloud hosting are still in practice, public cloud environment are getting more momentum since those require minimal up-front effort to acquire and setup the environment and provide better scalability and flexibility. Since CCHs are a centralized hub that many participating organizations can use, it is often difficult to estimate the number of users and transactional volume upfront. Therefore, more dynamic and cost-effective public cloud environments serve as a good platform for hosting CCH systems. The following subsections are more focused on the cloud hosting requirements to support CCH systems.

Cloud Architecture Requirements

The architecture considerations described earlier are applicable to cloud hosted systems, but there are some variations of how the same architecture considerations can be supported in cloud. Below is the list of requirements that should be supported:

- Cloud-based application should be designed and deployed as modular with separation of concerns between various components of the application.

- Cloud infrastructure must provide the front-end graphical user interface for accessing the application via commonly used web browsers such as Chrome, Edge, Firefox, and Safari.
- Cloud infrastructure must support back-end components of the application such as application server, services, data storage, security, cache, connectivity, and management.
- Cloud services must primarily provide computing services (e.g., Elastic Computing or EC2 in AWS) and storage services (e.g., Relational Data Storage in AWS).
- Cloud services must be sized as per the base estimates for number of users and transactions but be burstable to handle short-term increase in load.
- Cloud confirmation must be scalable to be able to dynamically add more memory, CPU, or storage to meet the increased demand over the longer period.
- Cloud infrastructure may support serverless deployment (cloud native) to allow running code, managing data, and integration without managing servers to provide best scalable solution.
- Cloud hosting must provide the dynamic pricing model to charge either based on resources utilized with server-based deployment or event-driven usage in serverless deployment.
- Cloud infrastructure must provide support for built-in licensing for tools and technologies available within the cloud environment but also allow deployment of externally licensed tools.
- Cloud infrastructure must allow designated authorized users to manage all cloud services, resources, user access control, application access keys, monitoring, and billing/payment.

More details about cloud architecture principles and examples can be obtained from the cloud specific websites and resources such as AWS Architecture Center: https://aws.amazon.com/architecture/ or Azure Architecture Center: https://learn.microsoft.com/en-us/azure/architecture/.

Cloud Security Requirements

Cloud security requirements include who can access the applications and data as well as the cloud services hosting them. The application and infrastructure level security requirements described in earlier sections apply in the cloud environment as well. However, there are some additional requirements that are specifically more relevant in the cloud-environment as follows:

- To meet corporate and regulatory standards, cloud infrastructure must provide detailed logs of who has access to application and cloud resources and verify that it is adequately encrypted.
- As per the organization compliance needs and regulations, it is important to document admin and security responsibility between internal staff, contractors, and the cloud provider.
- Cloud provider and/or supporting contractor must work with the organization staff to assess the situation and requirements of hosting the systems and conduct risk assessment.
- The risk assessment must document identification of sensitive data, user access to that data, sharing of that data with other systems/applications, cloud security settings, encryption, etc.
- Cloud environment must apply authorization policies with the access control rules for all users accessing the data in the cloud storage (at-rest) as well as transmission.
- Cloud environment must support encryption of sensitive data with irreversible one-way hash or Public Key Infrastructure (PKI) key-based encryption and description.

- Cloud environment must allow use of either native cloud-based identity management services or an organization's externally hosted identify management or other third-party identity providers.
- When there is a need for back-end applications to connect with the systems and data, cloud security must support long-term access keys (or API keys) to connect programmatically.
- Cloud infrastructure must allow setting access control restrictions on computing and data services for various users and user groups as well as access keys.
- Cloud infrastructure must support built-in advanced anti-malware and anti-virus technologies that can be used for the virtual servers/services and network traffic.

More details about cloud security can be obtained from the cloud specific websites and resources such as AWS Cloud Security Guidelines: https://aws.amazon.com/security/ or Azure Security Guidelines: https://azure.microsoft.com/en-us/explore/security.

Cloud Monitoring and Metrics Requirements

The monitoring and metrics requirements for cloud-based infrastructure is no different than other deployment mechanisms. However, the tools and best practices somewhat differ. Each cloud environment provides built-in monitoring capabilities for the deployed servers/services and resources. Typically, the organization and cloud service provider will have assigned responsibilities for monitoring when some systems and applications are deployed in a cloud environment. Cloud distribution adds complexity to tracking in complex environments. Below are general requirements that cloud service providers should be responsible for:

- Cloud service providers are responsible for monitoring the infrastructure and services provided to the client organization.
- Cloud service providers will need to provide tracking information to the client regarding the use of the services (usually through the management dashboard and automated reports).
- Cloud infrastructure must provide the tools for the client organization to monitor the systems and applications that are deployed by the organization.
- Cloud infrastructure must include the alert mechanisms to notify cloud infrastructure admin or client organization admin personnel based on the alert criteria.
- The monitoring metrics must include the standard cloud infrastructure monitoring as well as application resources active and peak measures.

Although metrics for cloud monitoring may include a lot of different aspects, following are the key ones to be supported for monitoring and alerts:

- Services actively running
- Resources used by the services including current and peak memory/CPU
- Storage usage and performance
- Cost measurement based on the usage
- Active users and peak users during specific period
- Active connections and peak connections during specific period

- Unauthorized or suspicious user access
- Failed/rejected connection attempts
- Active and peak number of service requests
- Average response time
- Autoscaling and burst events

Tracking data provided by cloud service providers may differ from data collected in on-premises tracking. Therefore, it is important to know how to use new data to effectively monitor the cloud-based environment. Understanding the nature of data provided by cloud service providers, deciding what is normal or baseline, and detecting anomalies will be part of monitoring and improvement.

More details about cloud monitoring and tracing can be obtained from the cloud specific websites and resources such as AWS Cloudwatch: https://aws.amazon.com/cloudwatch/ or Azure Monitor: https://azure.microsoft.com/en-us/products/monitor.

Continuity of Operations

A Continuity of Operations Plan (COOP) is a plan to document how an organization will carry out the essential operations during an emergency, disaster, or long-term disruption of the service. The plan will need to identify the process and protocol to be followed in case of an emergency event, including primary/secondary point of contacts that will be responsible to carry out the operations. A COOP will need to identify mission-critical functions that must be continued to operate; organization communication methods; interactions with partners, customers, and vendors; alternate or backup personnel; IT system operations and recovery; and locations for the continued operations. A COOP is often designed to provide different response mechanisms for different types of events (e.g., natural disaster or widespread power/network outage).

In reference to IT systems, COOPs need to document the system availability needs for continued operations, steps to recover from the outage (if any), recovery requirements, and testing frequency. A Disaster Recovery (DR) Plan is often a subset or part of an overall COOP for the disaster recovery of the operations. However, COOP and DR Plans are often used interchangeably, though COOP will typically have a wider scope than a DR Plan. The recovery plan for the IT systems must include the restoration of organizational production data facility. The plan is often documented with the assumption of total system hosting facility loss requiring recovery/restoration of all mission critical functions related to the daily business operations. The recovery requirements for the system will also often include two key measures:

- Recovery Time Objective (RTO)—time to bring up the system after an outage, and
- Recovery Point Objective (RPO)—point in time to which data loss may be acceptable

It is important to specify the expectations of RTO and RPO in the SLAs and ensure that the COOP or DR Plan has a plan to meet those objectives. For a non-critical system, RTO and RPO may be in terms of days (e.g., RTO as 3 days and RPO as 1 day). For more critical systems, when the expected interruption is minimum, RTO and RPO may need to be lot shorter (e.g., RTO as 2 hours and RPO as 30 mins). For a mission-critical system, it is often expected that the system instantaneously switches over to the DR instance that is kept live all the time with the most up to date data synced in real time (i.e., no data loss). The SLAs and DR Plan should document agreed upon expectations regarding the systems under considerations. **Exhibit 14** provides key elements that should be documented in COOP/DR plan.

Exhibit 14. Key Elements of COOP/DR Plan

Essential Functions	The critical activities performed by organizations, especially after a disruption of normal activities.
Orders of Succession	Provisions for the assumption of senior agency officials during an emergency in the event that any of those officials are unavailable to execute their legal duties.
Delegation of Authority	Identification, by position, of the authorities for making policy determinations and decisions at all organizational levels and locations.
Continuity Facilities	Locations, other than the primary facility, used to carry out essential functions, particularly in a continuity event.
Continuity Communications	Communications that provide the capability to perform essential functions, in conjunction with other agencies, under all conditions.
Vital Records Management	The identification, protection and ready availability of electronic and hard copy documents, references, records, systems, software, and equipment needed.
Tests, Training, and Exercises	Measures to ensure that an agency's continuity plan is capable of supporting the continued execution of the agency's essential functions throughout the event.
Devolution of Control and Direction	Capability to transfer statutory authority and responsibility for essential functions from an agency's primary staff and facilities to designated secondary.
Reconstitution	The process by which surviving and/or replacement agency personnel resume normal agency operations from the original or replacement primary facility.

More details about COOP can be obtained from Federal Emergency Management Administration (FEMA)'s general guidance on continuity plan for community-based organizations: https://www.fema.gov/sites/default/files/2020-07/non-federal-continuity-plan-template_083118.pdf, as well as Department of Homeland Security (DHS) Ready.gov website guidance on IT DR Plan: https://www.ready.gov/it-disaster-recovery-plan.

Chapter 5: Data Requirements

A CCH is a community-focused entity that organizes and supports a network of CBOs providing services to address health-related social needs that help improve overall health outcomes. The CCH model effectively supplements healthcare services with social services needed to overcome barriers for those most at risk of poor health outcomes. In order to support this coordination model, CCH systems must include various data collections for the CCH/CBO specific functions, as well as any other data acquired from external sources such as EHR and HIE. It is important that the CBOs and community service providers have easy access to the client's health and social data together. In addition, CCHs must support several other administrative functions such as contracting with health systems, referrals within and outside of the CCH network, service delivery coordination, compliance with rules and regulations, billing and payment, analytics and reporting, and so on.

Because of the wider scope of the CCH, it is important to ensure that data architecture and structure are defined in CCH systems. In addition, it is also very important to leverage applicable data standards that are specifically for social/human services data but also the standards used in health systems to support meaningful interoperability with those systems. The following subsections elaborate on specific requirements related to data architecture, structure, and standards.

Data Architecture

The primary considerations of CCH system data architecture are:

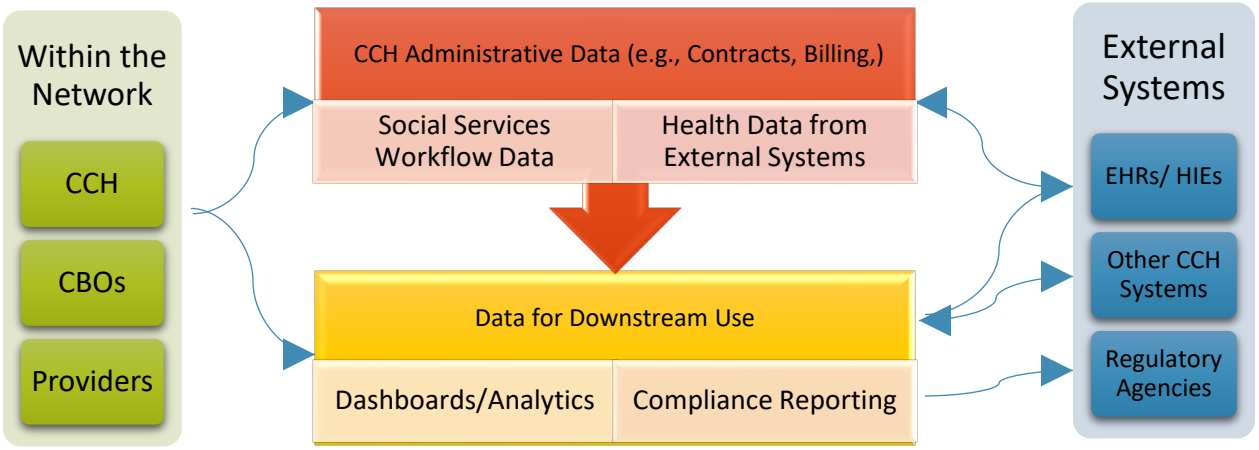
- Incorporate data for health and social services and integrate as needed for CCH activities
- Manage and track individual level data collected/updated for the services provided
- Support all CCH administrative functions that provide coordination amongst organizations
- Integrate dashboards, decision support, and any downstream use, e.g., compliance reporting

The data architecture of the CCH system will need to be defined based on these considerations. A CCH model will require keeping track of the social services at the individual level including the health data acquired from the external systems (generally as part of referral), as well as new data generated in the CCH/CBO process. All that data will collectively support better outcomes for the individual. CBOs should be able to effectively utilize EHR data acquired from health systems for their community-based health interventions.

CCH information systems should have data architecture to support data collection and integration in the above referenced operational aspects. But it is also important to have data structure to support better business decision making via business intelligence and reporting tools, dashboards, etc. Finally, the architecture should also be laid out to support any compliance reporting related to any governmental rules and regulations. In order to minimize the complexity of the data architecture, various aspects of data may be stored in a separate set of entities. However, those should remain as separate silos of data. The data architecture should provide appropriate linkages between the data entities from these various sources and continue to maintain the linkage through the workflow steps for human/social services.

The above-mentioned data architecture principle provides more streamlined data management, data quality monitoring as well as Extract, Transform, and Load (ETL) processes for data integration and reporting. This approach also allows data governance rules to be applied more effectively. For example, data sourced from EHRs will likely to be read only, so it will have different data governance rules compared to the data generated by users within CCH systems. **Exhibit 15** provides a high-level schematic representation of how the data architecture can be designed.

Exhibit 15. High-level Schematic for the Data Architecture



Below is summary of various data architecture requirements that should be supported in a CCH system:

- CCH system data architecture should organize data for various external data sources, individual level data generated within the CCH network, administrative data, and data for downstream use
- The individual-level data generated in the CCH network should be properly linked with the individual data from other external sources such as EHRs and HIEs
- All the individual-level data should be available to the care coordinators to be able to make the right decisions about the care services needed for each individual
- The individual-level data entered during the social care services workflow should be utilized for any subsequent referrals and billing
- Administrative data should be appropriately linked with the individual data (e.g., referrals and billing) as well as other organizational data (e.g., contracts, referrals, and billing)
- The CCH data system keeps the health data up to date with reasonable latency (say within a day) by utilizing interoperable connectivity with EHRs and HIEs
- Data analytics and other downstream processes should use data from all sources (externally acquired as well as generated within the CCH network)
- All data stores must be secured as per the security requirements specified in the regulations and best practices guidance
- It is important to define the data ownership clearly regarding data acquired from the external systems (source system owns) versus data generated by CCH/CBOs (CCH owns)
- All data acquired form the external sources must be kept up to date with reasonable latency period
- Data architecture should ensure that the data is normalized, integrity is enforced, constraints are in place to ensure quality, and duplication of data is avoided

The data architecture approach described above supports the key data management principles, encourages ease of access, and enhances quality, reliability, and timeliness of the data.

More details about data architecture can be obtained from the data architecture guiding principles of the Agency for Healthcare Research and Quality (AHRQ) Pathways HUB program which is a type of CCH model: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4747120/pdf/egems1182.pdf.

Data Structure

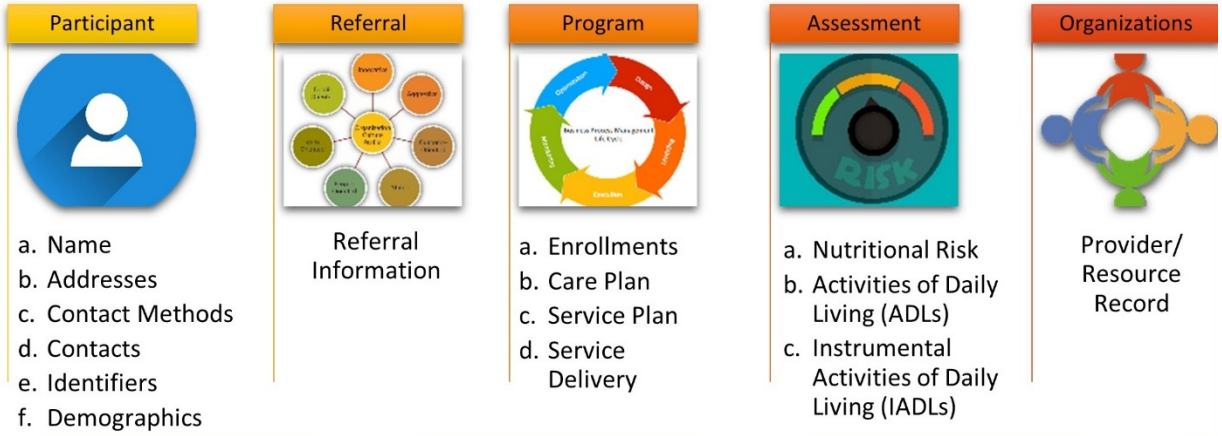
While the previous section focused on overall data architecture, this second describes specific data that needs to be collected and structured to satisfy the CCH functions. The focus of this section is more on the individual-level and organization-level administrative data collected by a CCH. At a high level, this includes an individual's demographic data, agency/organization (CCH/CBO/social care provider), referral data, social care workflow data, assessment/screening, and billing data. The following diagram shows the minimum data requirements specified by Partners in Care Foundation, a CCH in California, for inclusion by their CCH subcontractors (some of the items are formatted and/or consolidated).

Exhibit 16. CCH Subcontracts Minimum Data Requirements Specified by Partner in Care Foundation

Another example source for the data needed for social care services is developed by the Missouri Aging Services Data Collaborative (MASDC) under the ACL Social Care Referral Challenge. This dataset specification, referred to as the Aging Services Dataset and Interoperability Standards (ASDIS), is meant to provide an essential step forward for interoperability across health and social care providers.

Exhibit 17 provides list of high-level entities specified in ASDIS.

Exhibit 17. Data Entities Defined under Aging Services Dataset and Interoperability Standards



ASDIS provides several data elements under each of the entities listed above. While above data requirements serve as a good reference for minimum data requirements to be included in the CCH system, there will be several more data entities and elements needed for a fully functional system to support entire social care workflow, business operations, compliance, and interoperability.

More details about data requirements can be obtained from the Aging Services Dataset and Interoperability Standards: https://agingservicesdataset.org/ and Gravity Project Social Risk Data Set specification: https://confluence.hl7.org/display/GRAV/Initial+Social+Risk+Data+Set+Specification.

Data Standards

As described above, CCHs are responsible for coordinating with several CBOs as well as health systems. Hence the CCH systems require exchanging data with external health systems as well as CBOs that may be using their own systems for data collection. To enable this coordination and effective data exchanges, it is very important to employ standardized data exchanges as much as possible. Use of relevant data standards will result in streamlined processes, more reliable data exchanges, better quality and integrity of the data, and reduced cost of operations. At the same time, the system implementation should also allow for flexibility to be able to integrate with the community systems that may not be prepared to adopt and implement standards. However, such exceptions should be minimized as much as possible.

The U.S. healthcare sector has been going through a major shift during the last decade with government initiatives and regulations requiring the use of healthcare standards for any data exchanges. Government agencies have been working closely with the Standards Development Organizations (SDO) such as Health Level 7 (HL7) to ensure that the right standards are in place and specified in regulations as mandatory requirements. These efforts have led to significant increase in healthcare standards adoption by the organizations supporting physical health. The HHS Office of National Coordinator (ONC) facilitates development or modifications of many of the standards and specifies those standards in rulemaking in support of the regulations released by CMS. ONC maintains an excellent repository called Interoperability Standards Advisory (ISA) that provides lists and details of relevant standards.

More details about applicable data standards can be obtained from the CMS Interoperability Standards Advisory (ISA): https://www.healthit.gov/isa/; especially the ISA section on Human and Social Services standards: https://www.healthit.gov/isa/section/human-and-social-services, ISA section on Social Determinants of Health (SDOH): https://www.healthit.gov/isa/uscdi-data-class/social-determinants-health, and ISA section on vocabulary/terminology representing Social, Psychological and Behavioral data: https://www.healthit.gov/isa/section/social-psychological-and-behavioral-data.

Data Standards Adoption and Implementation

It is important to note that the healthcare data standards are not always adequate or appropriate for human or social care services. There has been increasing effort to make healthcare standards more relevant to human and social care services, and introduce more standards as needed to fill the gap. Several of those standards are already developed or are being developed to cater to social care services, and hence should be adopted by CCHs. It is important to determine what standards should be adopted to enable the interoperability with the external CBO systems and health systems. **Exhibit 18** provides high-level implementation guidance for various purposes.

Exhibit 18. Standards Adoption and Implementation

Purpose	Implementation
Clinical Data Exchange	▪ Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) and clinical document standards such as Consolidated Clinical Document Architecture (C-CDA) or Continuity of Care Document (CCD) are predominantly used for clinical data exchange. The vast majority of the EHR systems support these standards. ▪ While clinical document standards were required by regulations and more commonly used in the past for the clinical data exchange, FHIR standards implemented as Application Programming Interface (API) are more aligned with the changing technology and required by the latest CMS and ONC rules. ▪ Although originally designed and developed for clinical data, FHIR is also becoming the foundational standard for other health domains such as behavioral health, long-term support services, as well as social care services. ▪ If a new clinical data exchange is to be implemented by CCH systems to integrate with EHR or HIE systems, then it is recommended to implement the FHIR standard as it is relatively easier to implement and leverages more modern technology.
Social care data Exchange	▪ In order to facilitate seamless social are data across the partnering systems, CCH systems must be designed to support this type of data exchange. ▪ While there are non-standardized methods to support such exchange, it is recommended to implement new industry recognized standards defined by the Gravity Project. The implementation guides defined under this project are based on the HL7 FHIR standard mentioned above. ▪ In addition, the FHIR Implementation Guide for Human Services Directory is a newly developed standard to query organizations, locations, and services from a social care directory in a standardized manner. This specification is based on the Human Services Data Specifications (HSDS) that is developed and maintained by Open Referral initiative.

Purpose	Implementation
Admin and Billing Data Exchange	▪ For administrative and billing data, HIPAA X12 standards are de facto standards used in the U.S. The X12 transactions are used within healthcare industry to exchange health insurance claims and payments. ▪ Some of the most commonly used X12 transactions are 834 (enrollment), 270/271 (eligibility inquiry/response), 278 (services review), 837 (claims), 835 (payments), and 276/277 (claims status inquiry/response). ▪ Although these standards primarily focus on healthcare services, it is important to adopt and implement these standards due to increasing support for non-healthcare services as well. It is especially important for CCH systems that need to integrate with health systems to exchange some of these data. ▪ The commonly used procedure codes and diagnosis codes used as part of the HIPAA X12 transactions include provision to bill for non-healthcare services such as social care services.
Terminology and Taxonomy	▪ There are several terminology coding systems used as part of above-mentioned content standards to define and exchange specific types of concepts. Below is the list of some of the most commonly used terminology systems in healthcare: ✓ Systematized Nomenclature of Medicine Clinical Terms (SNOMED-CT) is the most comprehensive, multilingual clinical terminology in the world, along with terms and definitions for human and non-human concepts. ✓ International Classification of Diseases (ICD) is a globally used diagnostic tool for epidemiology, health management, and clinical purposes. ✓ Current Procedural Terminology (CPT) for procedures and services rendered by the healthcare providers. ✓ Healthcare Common Procedure Coding System (HCPCS) for procedure codes that includes CPT codes as Level I while non-physician services under Level II and other local and payor specific codes under Level III. ✓ Logical Observation Identifiers, Names, and Codes (LOINC) is an international standard for identifying health measurements, observations (e.g., labs and radiology), and documents. ✓ RxNorm is a consolidated names and codes of drugs from various drug vocabularies including SNOMED-CT and National Drug Codes (NDC). ▪ While the terminology systems are primarily used in healthcare, they don't provide exhaustive collection of concepts and services for social care data exchange. Below is the list of some of the taxonomy/value sets for social care services: ✓ 211 LA County taxonomy defines standard for defining wide variety of human services available in communities across North America. ✓ Open Eligibility taxonomy is a simple way to categorize human services and situations for social care providers and navigators to find services. ✓ Gravity SDOH Value Sets developed by the Gravity Project for each SDOH activity (screening, diagnosis, goal setting, and interventions)
Access Control	▪ The following access control standards are important to be adopted as they play a key role in interoperability using FHIR API as well as support federated identity management: ✓ Open Authorization 2 (OAuth2) for access authorization roles ✓ Open ID Connect (a profile on OAuth2) for identify management

The following subsections provide more details about some of the key standards mentioned above.

HL7 Fast Healthcare Interoperability Resources

FHIR is a healthcare data exchange standard that was developed by HL7. It is a lightweight, modern approach to exchanging healthcare information that is designed to be more efficient, flexible, and interoperable than previous standards.

Exhibit 19. Benefits of HL7 FHIR for CCHs

Benefit	Description
Improved Interoperability	FHIR is designed to be interoperable with a wide range of healthcare systems and applications. This makes it easy to exchange data with other organizations.
Reduced Costs	FHIR can help to reduce the costs of healthcare by making it easier to exchange data between organizations. This can lead to reduced duplication of services and improved efficiency.
Improved Patient Care	FHIR can help to improve patient care by making it easier to access and share patient data. This can lead to better diagnoses, more informed treatment decisions, and improved outcomes.
Increased Patient Engagement	By making it easier for patients to access and share their health information, FHIR can help to increase patient engagement in their care. This can lead to better outcomes and a more positive patient experience.
Improved Decision Making	By making it easier for healthcare providers to access and share patient data, FHIR can help to improve decision-making. This can lead to better diagnoses, more effective treatment plans, and improved outcomes.
Reduced Administrative Burden	By making it easier to exchange data between healthcare organizations, FHIR can help to reduce administrative burden. This can free up time and resources that can be better spent on patient care.

FHIR is a valuable tool for CCHs that want to improve the interoperability of their IT systems. By using FHIR, CCHs and CBOs can exchange data more easily and efficiently with healthcare organizations. This can lead to improved patient care, reduced costs, and increased efficiency. Some of the benefits of adopting FHIR include:

- FHIR data elements are the building blocks of FHIR resources. There are hundreds of individual pieces of data that are used to represent a patient's health information.
- FHIR data elements are defined in a standard way, which makes it possible for different systems to exchange health information. While there are many different FHIR data elements, each of which represents a different type of health information to illustrate the value of FHIR, the following data elements from various FHIR resources are part of a patient record.[11]

Exhibit 20. Example FHIR Resources and Data Elements

Data Element	Description	Value
Patient demographics		
Name	Patient's full name	John Doe
Date of birth	Patient's date of birth	01/01/1980
Gender	Patient's gender	Male
Address	Patient's home address	123 Main St
Contact information	Patient's contact details	(555) 555-5555

[11] Health Level Seven International. (2023). HL7 FHIR Implementation Guide: Electronic Case Reporting. Accessed at: https://bit.ly/3W8HPK8

Data Element	Description	Value
Medical history		
Allergies	Patient's known allergies	Penicillin
Medications	Current medications patient is taking	Lisinopril
Diagnoses	Patient's medical diagnoses	Hypertension
Procedures	Medical procedures patient has undergone	Appendectomy
Laboratory results		
Blood pressure	Patient's blood pressure reading	140/90 mmHg
Cholesterol	Patient's cholesterol level	220 mg/dL
Glucose	Patient's glucose level	100 mg/dL
Other lab values	Other laboratory test results	Hemoglobin: 14 g/dL
Medications		
Prescription and over-the-counter medications	Medications prescribed to the patient and over-the-counter medications the patient is taking	Aspirin
Discharge disposition	Where the patient is going after discharge from the hospital	Home
Discharge medications	Medications that the patient is taking when they are discharged from the hospital	Metoprolol
Discharge instructions	Instructions that the patient has been given by the hospital staff	Follow up with PCP
Discharge plan	Outlines the plan of care for the patient after they are discharged from the hospital	Home care
Functional status	Indicates the patient's ability to perform activities of daily living and instrumental activities of daily living	Independent
Social support	Indicates the patient's social support network	Family
Financial resources	Indicates the patient's financial resources	Private insurance
Language	Indicates the patient's preferred language	English
Cultural beliefs	Indicates the patient's cultural beliefs	Christianity
Advance directives	Indicates the patient's wishes for end-of-life care	DNR

As CCHs and CBOs consider adopting FHIR, it is important to assess how vendor software can support FHIR functionality. FHIR standard provides capability called profiling to develop specification related to specific domain or use cases and there are several profiles or Implementation Guides (IGs) developed in reference to human and social services. The right software vendor is crucial for organizations that want to improve their interoperability with healthcare systems and applications. Evaluating software vendors for FHIR compatibility is an essential step to achieve these goals. The following section discusses key criteria that CCHs and CBOs should consider when evaluating software vendors for FHIR compatibility. By following these guidelines, CCHs and CBOs can ensure that they choose a vendor that can support their interoperability goals and help them to provide better patient care. The following criteria can be useful to CCHs and CBOs as they assess vendor software systems for FHIR functionality and support.

Exhibit 21. Vendor Criteria for HL7 FHIR Related Experience

Criteria	Description
Commitment to FHIR	The vendor's history of involvement in FHIR, their investment in FHIR development, and their commitment to FHIR standards.
Comprehensive FHIR offering	The ability to support a wide range of FHIR resources, the ability to exchange data with a wide range of healthcare organizations, and the ability to integrate with existing systems and applications.
Support FHIR profiles relevant for human and social services	The vendor should have the ability to implement such FHIR specifications developed for human and social services.
Strong track record of success	The vendor's customer base, their references, and their case studies.
Good reputation	Online reviews, industry publications, and analyst reports.
Easy to use	The vendor's user interface, documentation, and training materials.
Security	The vendor's security features, their security practices, and their security certifications.
Reliability	The vendor's uptime record, their disaster recovery plan, and their customer support.
Affordability	The vendor's pricing structure, their payment terms, and their discounts.
Responsive and helpful support	The vendor's support hours, their support channels, and their support documentation.
Willing to customize software to meet needs	The vendor's customization options, their pricing for customization, and their turnaround time for customization.
Willing to integrate software with existing systems	The vendor's integration capabilities, their pricing for integration, and their turnaround time for integration.
Willing to train staff on software	The vendor's training options, their pricing for training, and their availability of training.
Willing to provide ongoing support for software	The vendor's support options, their pricing for support, and their availability of support.
Commitment to continuous improvement	The vendor's roadmap for new features and enhancements, their commitment to security, and their commitment to customer satisfaction.
Good fit for organization	The vendor's culture, their values, and their goals.

More details about the FHIR standard can be obtained from the HL7 website for the specification: https://www.hl7.org/fhir/.

The Gravity Project

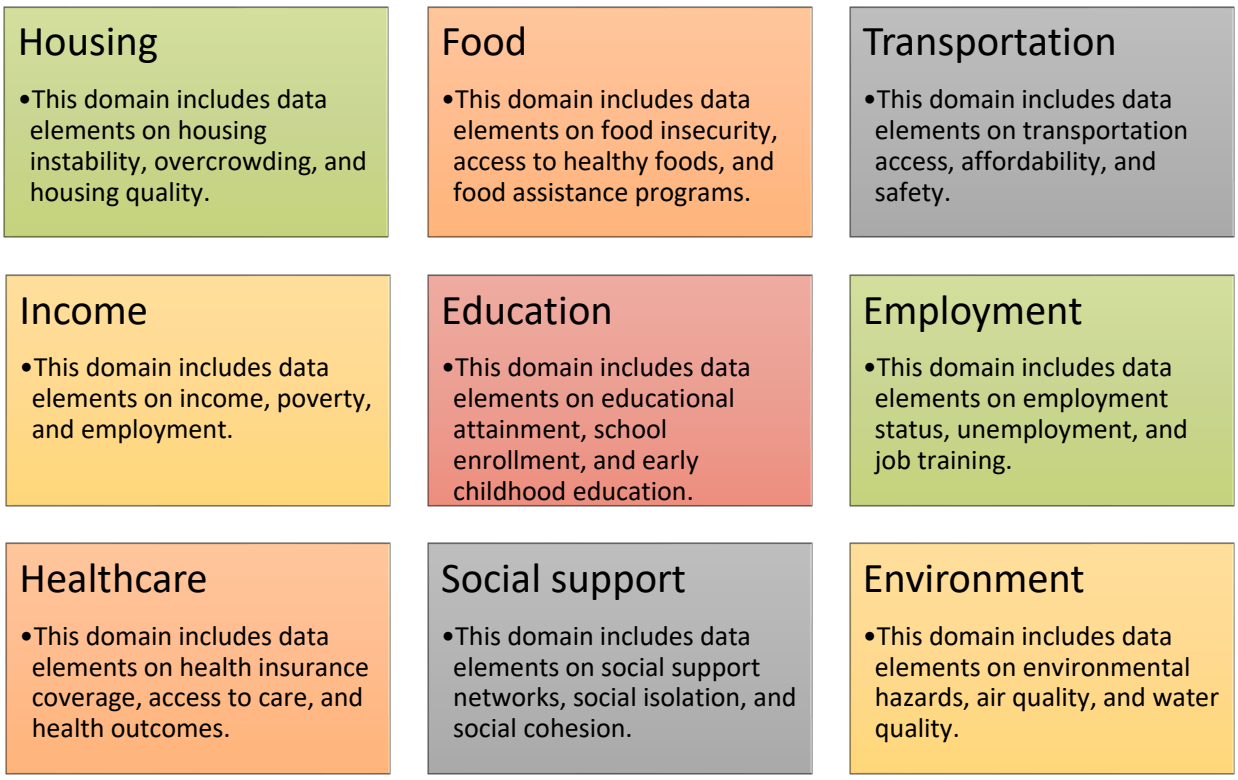
The Gravity Project is a multi-stakeholder initiative aimed at standardizing the documentation and exchange of SDOH data. By addressing gaps in the consistent and interoperable capture of SDOH information, the project seeks to enable better integration of this information into healthcare delivery and decision-making processes. The initiative brings together healthcare providers, payers, policy experts, researchers, and other stakeholders to develop consensus-driven data standards for SDOH.

Gravity Project Data Use Principles for Equitable Health and Social Care are as follows:

- Improving Personal Health Outcomes
- Improving Population Health Equity
- Ensuring Personal Control
- Designing Appropriate Solutions
- Ensuring Accountability
- Preventing, Reducing, and Remediating Harm

The Gravity Project aims to improve the sharing and integration of SDOH data across different health information systems, promoting better coordination and collaboration among healthcare providers, CCHs and CBOs, and other partners. By developing standardized SDOH data elements, terminologies, and data exchange formats, the Gravity Project hopes to enhance the interoperability of SDOH data across different health information systems, improve the consistency and quality of SDOH data collection and documentation processes, and enable better integration of SDOH data into clinical decision-making and care planning processes.

Exhibit 22. Social Risk Domains under the Gravity Project



The Gravity Project has identified 20 SDOH-related domains that are essential for documenting social risk and protective factors data for screening, diagnosis, treatment, and population health management activities.[12] These data elements are organized into various domains shown in **Exhibit 22**.

For CCHs, it is important to adopt data standards that facilitate effective communication and collaboration with health systems and other partners. The Gravity Project's data standards may one day provide a comprehensive and standardized framework for capturing, documenting, and sharing SDOH information. By adopting these standards, CCHs may be able to exchange data more seamlessly, promote interoperability, and ultimately enhance the quality of care provided to clients.

Adopting the Gravity Project data standards can be a complex process, but it can be a valuable investment for organizations that want to improve the interoperability of their data. It is crucial for CCHs to ensure that the software vendors they partner with have the capability to support the Gravity Project data standards effectively to improve their SDOH data sharing and collaboration with health systems and other partners, ultimately enhancing the quality and impact of their services. To assess software vendors' compliance and functionality with the Gravity Project Data Standards, CCHs should consider the factors in the **Exhibit 23**.

Exhibit 23. Vendor Criteria for Gravity Project and SDOH Related Experience

Plans to support the Gravity Project Data Standards in the future	The software vendor should be committed to supporting the latest version of the data standards.
Experience with other SDOH data standards	The software vendor should have experience working with SDOH data standards in general.
Support for other SDOH data collection and sharing tools	The software vendor should be able to integrate with the other tools that you are using.
Compliance with standardized SDOH data elements and terminologies	The vendor's solution should be able to accurately capture, store, and manage the standardized SDOH data elements and terminologies as defined by the Gravity Project.
Support for data collection and documentation processes	The vendor's solution should provide the necessary tools and features to enable consistent data collection and documentation processes in line with the Gravity Project's guidelines.
Interoperability and data exchange capabilities	The vendor's solution should be compatible with recommended data exchange formats and protocols, such as FHIR.
Affordability	This is an important consideration for organizations that are on a budget.
User-friendliness	The vendor's solution should be easy to use and navigate for staff members who will be responsible for entering and managing SDOH data.
Data security and privacy	The vendor should be able to provide assurances that their solution is compliant with relevant data security and privacy regulations, such as the HIPAA Rules.
Customer support and training	The vendor should provide adequate customer support and training to help ensure that staff members are able to effectively use their solution.

[12] Arons, A., DeSilvey, S., Fichtenberg, D., and Gottlieb, L. (2019). Documenting social determinants of health-related clinical activities using standardized medical vocabularies. *JAMIA Open*. 2018;2(1):81-88. DOI: 10.1093/jamiaopen/ooy051.

Plans to support the Gravity Project Data Standards in the future	The software vendor should be committed to supporting the latest version of the data standards.
Integration with existing systems	The vendor's solution should be able to integrate with any existing systems or software that CCHs are currently using.
Scalability	The vendor's solution should be able to grow and adapt as CCHs' needs and workflows evolve over time.
Reporting and analytics	The vendor's solution should provide reporting and analytics capabilities that can help CCHs to identify trends and patterns in their SDOH data, which can inform their decision-making processes.
Customization	The vendor's solution should allow for some level of customization, so that CCHs can tailor the solution to meet their specific needs and workflows.

By carefully evaluating software vendors based on these criteria, CCHs are more likely to select a partner that can effectively support their efforts to adopt the Gravity Project's data standards. This, in turn, will help CCHs improve their SDOH/HRSN data sharing and collaboration, leading to better outcomes for the vulnerable populations they serve.

More details about the Gravity Project can be obtained from the public website for this initiative: https://thegravityproject.net/ as well as the H7 confluence portal for project-specific documentation and artifacts: https://confluence.hl7.org/display/GRAV/. Similarly, more details about SDOH can be obtained from ONC's SDOH website: https://www.healthit.gov/health-equity/social-determinants-health and HHS Office of Assistance Secretary of Health (OASH) website: https://health.gov/healthypeople/priority-areas/social-determinants-health.

Human Services Data Specifications

The Human Services Data Specification (HSDS) is a standardized data format designed to facilitate the sharing of information across various human services providers, including CCHs. HSDS was developed by the Open Referral Initiative in response to the growing need for a standardized data format that would enable human services providers to share information efficiently. The primary use case served by HSDS is the provision of human service directory information as "open data," to be consumed by any third-party information system.

HSDS defines a minimal set of data for publishing machine-readable directory information about health, human, and social services; their locations and accessibility details; and the organizations that provide them. HSDS is taxonomy agnostic so the implementer can use the taxonomy that they prefer to use. Exhibit 24 provides several key elements that are part of HSDS.

Exhibit 24. Key Entities of HSDS

Organization	Location	Program	Service
Contact	Phone	Address	Language
Service Attribute	Service at Location	Service Taxonomy	Service Area
Schedule	Funding	Accessibility	Other Information

HSDS has the potential to enhance the interoperability of data across different health information systems and social services organizations, promote better collaboration, and ultimately improve the quality of care provided to vulnerable populations.

Adopting HSDS may prove to be a valuable investment for CCHs. By adopting HSDS, you may be able to improve the quality, consistency, interoperability, and cost-effectiveness of your referral data collection, storage, and exchange. This can lead to more efficient coordination and delivery of services that address health-related social needs.

Many software vendors have already adopted or provide support for the HSDS. CCHs should ensure that the software vendors they partner with can support the HSDS effectively to improve their data sharing and collaboration with health systems and other partners, ultimately enhancing the quality and impact of their services.

More details about the HSDS can be obtained from the Open Referral website for this project information: http://docs.openreferral.org/en/latest/ as well as the HSDS specification on GitHub: https://github.com/openreferral/specification.

FHIR Implementation Guide for Human Services Directory

The FHIR Implementation Guide (IG) project was initiated by ACL to support searching human and social services directories for services to help mitigate the unmet social needs of patients, consumers, and caregivers. This FHIR IG provides standardized specification for querying and exchanging social care provider directory data mapped to FHIR format. This guide consists of FHIR implementation profiles for three of the FHIR resources: Organization, Healthcare as a service, and Location.

This FHIR IG defines a FHIR interface to directories of social services information provided by community-based organizations at locations in which they operate. Publication of these data through standard FHIR-based APIs enables third parties to develop applications that can be used by healthcare providers, payers, and consumers to query directories of community-based services to help address the circumstances that make it difficult to live healthy lives and address unmet social needs.

The primary source of requirements for this FHIR IG is the HSDS specification. So, this guide essentially combines HL7 FHIR and HSDS standards mentioned above. A primary purpose for this IG is to provide implementers who are familiar with the HSDS format a map between HSDS-structure directory data to FHIR profiles, eliminating the need for implementers to have extensive experience mapping local directory data to FHIR in order to implement the standard FHIR APIs that allow FHIR-based applications to access human services directories of community-based resources.

The CMS Interoperability and Patient Access Rule (CMS-9115-F) specified FHIR technical standards and implementation guides that support development and testing of FHIR APIs to foster interoperability. CMS identified technical standards for Provider Directories and recommended the DaVinci Payor Data Exchange (PDEX) Plan Net Provider Directory Implementation Guide. In order to minimize the effort/burden required to implement FHIR-based human and social services directories into current workflow practices, this IG is developed to be based on the DaVinci PDEX Plan Net Provider Directory FHIR standard. This approach allows use of this IG by the healthcare providers, payers, and consumer applications for accessing healthcare provider directories.

Exhibit 25. Vendor Criteria for HSDS and Human Services Data Experience

Criteria	Description
Compliance with HSDS technical specifications	Does the software vendor's product meet the technical specifications of the HSDS? This includes things like the use of open standards and the ability to exchange data with other HSDS-compliant systems.
Standardized interoperability with other HSDS-compliant systems	Can the software vendor's product exchange data in standardized format with other HSDS-compliant systems? This is important for ensuring that data can be shared between different organizations.
Security and compliance	Does the software vendor's product meet the security and compliance requirements? This includes things like the ability to protect SDOH data from unauthorized access, use, or disclosure.
Documentation and training	Does the software vendor provide adequate technical support for their product? This is important for ensuring that healthcare providers are able to resolve any issues that they may encounter when using the product.
Affordability	This is an important consideration for organizations that are on a budget.
User-friendliness	The vendor's solution should be easy to use and navigate for staff members who will be responsible for entering and managing human services data.
Customer support and training	The vendor should provide adequate customer support and training to help ensure that staff members are able to effectively use their solution.
Integration with existing systems	The vendor's solution should be able to integrate with any existing systems or software that CCHs are currently using.
Scalability	The vendor's solution should be able to grow and adapt as CCHs' needs and workflows evolve over time.
Customization	The vendor's solution should allow for some level of customization, so that CCHs can tailor the solution to meet their specific needs and workflows.

More details about the FHIR IG for Human Services Directory can be obtained from the HL7 website for this draft standard: https://build.fhir.org/ig/HL7/FHIR-IG-Human-Services-Directory/index.html, and more details about this project can be found here: https://openreferral.org/hsds-is-now-interoperable-with-fhir/.

211 LA County Taxonomy

The 211 LA County taxonomy is the North American standard for indexing and accessing human services resource databases. It is a classification system used by the field of information and referral to index and access information about organizations that provide community services based on the types of organizations they are (hospital, adult school, library), the services they provide, and the people they serve.

Taxonomies are sophisticated tools that help people find the information they need. They are a type of a controlled vocabulary, a standardized set of terms and phrases that are used to index and retrieve information about a particular subject in a systematic, unambiguous way. Control is exerted in the

careful identification of concepts, selection of preferred wording for term names, and organization of the terms in a logical framework. New terms are only added when it is clear that a relevant concept has been identified for which there is no current term.

The following are some key facts and features of the 211 LA taxonomy:

- 211 LA taxonomy has been developed and enhanced for over 30 years
- It creates an infrastructure for human services directory including those maintained by 2-1-1 systems and statewide aging and ADRC systems as well as HMIS systems
- It provides a "common language" for human services organizations
- It is used internationally, and it has three different views called "locales" which represent the language in which a term and associated data elements appear and the domain of application
- It applies to all segments of the economy: nonprofit, for-profit, and government agencies
- It applies to all human services sectors and a goal is to have sufficient breadth and depth to meet the needs of both comprehensive and specialized databases
- It can be customized to meet the unique needs of communities. The filter function allows subscribers to deactivate the terms they don't want to use and to download the filtered set
- It has been widely endorsed and adopted. Most notably for our purposes, it is referenced in the Alliance of Information and Referral Systems (AIRS) standard is required for AIRS accreditation
- Implementers/users of this taxonomy requires purchasing license from 211 LA.

More details about the 211 LA taxonomy can be obtained from the website: https://211taxonomy.org/.

Open Eligibility

The Open Eligibility taxonomy is a simple way to categorize human services and human situations. With these common categories, we, as service providers, navigators, and people in need, can find human services quickly and easily. The Open Eligibility taxonomy consists of two important top-level concepts: Human Services and Human Situations.

- Human Services are services offered by government or charitable organizations, and include things such as housing, food pantries, or counseling services.
- Human Situations are ways of describing attributes of a person that could help them find programs they are looking for, including examples like veterans, persons with a physical disability, or older adults.

More details about the Open Eligibility taxonomy can be obtained from the websites: http://openeligibility.org and https://company.findhelp.com/the-open-eligibility-project/.

Z-Codes

Z-codes are a group of codes in the International Statistical Classification of Diseases and Related Health Problems (ICD-10) that are used to report social and environmental circumstances that may affect a patient's health. They are not diagnostic codes, but they can be used to provide additional information about a patient's health and to help healthcare providers and CBOs/CCHs understand the social and environmental factors that may be contributing to a patient's health problems.

Healthcare providers, insurers, and CBOs may use Z-codes to track and monitor these factors, helping identify patients potentially at risk for health problems. By monitoring these factors and targeting services to address these concerns, providers, insurers, and CBOs can create targeted interventions to improve the health of affected patients.

As the importance of addressing SDOH indicators grows, an increasing number of healthcare providers are assessing these factors and entering into contracts with CCHs to make referrals based on Z-codes. CCHs, in turn, may need to refer patients to other community partners to provide direct services tailored to address their specific needs.

Z-Codes – Social and Environmental Factors
Education
Employment
Income
Housing
Food Insecurity
Transportation
Healthcare Access
Social Support
Violence
Addiction
Mental Health
Physical Health

For instance, a CCH might receive a referral from a contracted health system for a patient who was assessed and assigned a Z-code indicating homelessness or food insecurity. The CCH or a partner organization could then develop a program to provide housing or food assistance to these individuals, ultimately improving their health and well-being. This collaborative approach ensures that healthcare providers and community organizations work together to address SDOH and provide comprehensive care for vulnerable populations.

Z-codes can also be used to track the effectiveness of interventions. For instance, a healthcare provider might use Z-codes to monitor the number of patients with uncontrolled diabetes. By comparing the number of patients diagnosed with diabetes before and after implementing an intervention to improve diabetes care, the provider can assess the effectiveness of the intervention. This information may also be used to determine incentive payments for CCHs, as their success in improving patient outcomes could be directly linked to the interventions provided.

As CCHs and CBOs evaluate the need for their software systems to receive referrals from health systems based on Z-codes, it is crucial to assess how vendor software can support Z-code functionality. The following are some criteria that CCHs and CBOs might consider when evaluating software vendors to ensure they choose a partner that can support their interoperability goals, including the need to integrate with revenue cycle management software (see Exhibit 26).

Exhibit 26. Vendor Criteria for Z-Codes Related Experience

Criteria	Description
Z-code integration	The vendor's software should seamlessly integrate Z-codes into the system, ensuring accurate data capture and easy referral tracking.
Compatibility with EHR systems	The software should be compatible with various EHR systems used by healthcare providers to ensure seamless data exchange.

Criteria	Description
Support for secure data exchange	The vendor's solution should support secure data exchange protocols to protect sensitive patient information during transmission.
Automated referral processing	The software should have the capability to automate the referral process based on Z-codes, reducing manual effort and potential errors.
Customizable referral workflows	The software should allow for the customization of referral workflows to accommodate the unique needs of each CCH or CBO.
Support for multi-disciplinary collaboration	The software should facilitate collaboration between different providers, including healthcare providers and community partners, to streamline care coordination.
Reporting and analytics capabilities	The vendor's solution should provide robust reporting and analytics capabilities to track and evaluate the impact of Z-code based referrals on patient outcomes.
Revenue cycle management integration	The software should integrate with revenue cycle management systems to accurately track reimbursements and financial outcomes associated with Z-code referrals.
Scalability	The software should be able to scale up as the organization grows, accommodating increases in referral volume and complexity.
Compliance with data privacy regulations	The vendor's solution should adhere to all relevant data privacy regulations, including the HIPAA Rules and GDPR, to ensure the protection of sensitive patient information.
User-friendly interface	The software should have an intuitive interface that is easy for staff to learn and use, reducing the time required for training and onboarding.
Vendor support and training	The software vendor should provide ongoing support and training resources to help CCHs and CBOs effectively utilize the system.
Interoperability with other SDOH data standards	The software should support interoperability with other SDOH data standards to facilitate data exchange with a wide range of partners.
Customizable alerts and notifications	The software should allow for the configuration of customizable alerts and notifications to ensure that key stakeholders are informed of important referral updates and changes.
Vendor commitment to continuous improvement	The software vendor should demonstrate a commitment to ongoing product development and improvement, ensuring that their solution remains up to date with industry best practices and evolving needs.

Best Practices for Data Collection and Reporting

Effective data collection and reporting is essential for CCHs ensure the accurate collection and reporting of key data points. To achieve this, CCHs should follow best practices for data collection and reporting, including:

- **Developing standardized data collection forms and tools.** To ensure consistent data gathering across all partners, CCHs should use standardized data collection forms and tools. This will help to reduce errors and ensure that data is collected in a uniform manner.
- **Establishing clear data sharing agreements and protocols.** CCHs should establish clear data sharing agreements and protocols to ensure data privacy and security while facilitating collaboration. This will help to build trust between partners and ensure that data is shared in a secure and confidential manner.
- **Regularly reviewing and updating data collection methods and reporting requirements.** To align with federal and state regulations and program changes, CCHs should regularly review and

update data collection methods and reporting requirements. This will help to ensure that data is collected and reported accurately and in compliance with relevant regulations.

- **Providing ongoing training and support to staff members.** To ensure adherence to best practices and maintain data quality, CCHs should provide ongoing training and support to staff members involved in data collection and reporting. This will help to ensure that staff members are equipped with the necessary skills and knowledge to collect and report data accurately.

Chapter 6: Preparing for Contractual Relationships

System Architecture Considerations

The IT systems used by CCHs should be scalable and flexible to accommodate changing needs and requirements of the community and the hub. They should be able to adapt to evolving technologies, business workflows, and operational processes. In order to support such dynamic operations, the CCH IT systems should be designed and implemented with several key architectural considerations as described in Exhibit 27.

Exhibit 27. Architecture Considerations and Approach

Architecture Consideration	Recommended Approach
System Response Time	The system response for various functions should be within acceptable range for a given function/module. For example, users should not have to wait for several seconds to get to the next workflow steps while entering data or should not have to wait for minutes to get the report results. Applications designed with an appropriate caching mechanism can help reduce costs on data loading and increase reusability, allowing your users to retrieve data more quickly without hitting up your servers on multiple requests.
Overall User Experience	The system should provide an intuitive user interface that require minimal or no learning curve for the end users. A system user interface may also need to be customizable to provide different look and feel, and navigation for different types of users based on the functions they need to access. Also, the system should be able to support a large number of users without sacrificing response time and provide overall good quality of user experience.
Batch Processing Time	Batch processing generally includes daily/nightly, weekly, monthly, quarterly, or annual processing of data acquired from other sources to be ingested in the system or processing of internal data for specific purpose such as analytics and reporting. The performance expectation and time to process the data in batch are often driven by the volume of data but must be designed to complete within the available time window.
Ability to Support Increase in Workload	A scalable application needs to maintain or improve efficiency as throughput increases, so it must be designed specifically to scale to prevent bottlenecks when there is a surge in system users. Similarly, the batch processing should scale up as the number of processes and/or transactions continue to grow.
Tools and Technical Platform	Before developing a scalable application, it is important to think about using the right technology frameworks with asynchronous programming, database optimization, loose coupling, partitioning, and caching to maintain application performance as user base and data volume increase. There are several technologies available that can help expedite the system implementation at a lower cost. It is important to look at overall cost of ownership including licensing, implementation effort, maintenance, and support as opposed to just looking at license cost to acquire specific tools.

Architecture Consideration	Recommended Approach
Design Patterns and Best Practices	There are various design patterns and best practices that should be factored into the system architecture. This includes but is not limited to a layered architecture for separation of concerns, microservices for internal and external communications, containerization for distributed deployment, zone-based system security and connectivity, etc. These design practices take advantage of a decentralized modular system that allows developing and maintaining various parts of the system without affecting the entire application. It is particularly important when a specific technology component (e.g., database) need to be replaced with other alternatives.
Integration and Interoperability	While individual systems may be performing well on their own, it is important that they are able to integrate and interoperate with other related systems internally and externally. There are various integration mechanisms that can be adopted to transfer and integrate data from system to system such as batch file transfer methods, real-time or batch web services, and RESTful Application Programming Interface (API). Interoperability takes it a step further by establishing common format and codes to provide common language for systems to understand each other, including commonly known industry standards to establish interoperability at a larger scale.
Application Programming Interface (API)	As mentioned above, APIs are one of the ways to establish interoperability between two systems. APIs are typically used for more complex integrations where multiple systems need to communicate with each other. This requires at least one system expose the backend functions as an interface that can be invoked by the other interfacing system(s). APIs are more complex to implement but easier to integrate with greater flexibility and scalability. It is an important requirement that the chosen solution offers API-based connectivity for better integration.
Storage Optimization	Application storage mechanisms play an important role in designing and implementing a highly scalable and robust application. It is important to choose a storage platform that offers better speed and reliability such as use of Solid State Drives (SSD), multi-disk arrays to provide redundancy such as Redundant Array of Independent Disks (RAID) configuration, distributed storage such as Network Attached Storage (NAS), or cloud-based storage. Modern storage mechanisms allow scaling up or down storage size and performance dynamically as per the demand.
Scaling Approach	While hardware will make up the backbone of your application, it is important to consider various scaling approaches when user base and/or data volume grows. This may be achieved by upgrading hardware memory (Random Access Memory or RAM) or processing power (Central Processing Unit or CPU). This means the existing server is expanded to handle the load, which is commonly referred as Vertical Scaling. An alternative is to add more CPUs or more servers to handle the load, which is commonly referred Horizontal Scaling.
Load Balancing	In order to enhance scalability to handle large number of users, applications may be deployed on multiple servers that are ready to process user and/or batch processing requests in a distributed manner. This can be achieved by employing a load balancing mechanism to spread out the workload with optimization mechanisms. Load balancing is the method of distributing network traffic equally across a pool of resources that support an application.
Performance/ Load Testing	Before putting an application into production or releasing it to your user base, it is important to carry out performance and load testing to address any potential issues not yet uncovered through the design and development process. Load testing uses realistic simulations of user demand and data volume to see how your application reacts. If performance issues crop up as throughput increases during this test, that's a very useful discovery to address without having to risk frustration among your users.

Architecture Consideration	Recommended Approach
Identity and Access Management (IAM)	IAM is primarily a set of policies, processes, and technology solutions to manage the identity of end users as well as trusted applications that access the system. The identity of users will involve all types of users including CCH administrative users, care coordinators, social care navigators, community service providers, persons receiving services as well as users from other external systems connected with CCH. The applications that are integrated are also to be trusted under the same framework for access control. Due to the complex environment CCH systems will need to deal with, it is also important to employ federated identity management that enables authentication and authorization across multiple systems and multiple organizations that are participating in data exchanges. As mentioned under the Data Standards section in Chapter 5, OAuth2 and OpenID Connect are commonly used for the IAM implementation and should be supported by the solution.
Master Patient/Person Index (MPI)	This capability is essential to uniquely identify the patient or person within and across the systems. Although there are several national (e.g., Social Security Number, Tax ID, Medicare ID, etc.) or state level identifiers (e.g., Medicaid ID, driver's license number, etc.), these identifiers may be missing, mistyped, or somehow changed over time. The same issue may occur with the person's profile information such as name, address, date of birth, race, gender, etc. Therefore, identifying a person uniquely and correctly is a major challenge in the healthcare sector. This is particularly challenging across systems and organization boundaries. The systems need to adopt some approach and tools to build an MPI repository that serve as a primary source for resolving identity using the data available from various sources. Such MPI solutions often rely on probabilistic algorithms using available person identifiers and demographics information to match a person/patient against the master index. While a CCH can implement such MPI using third-party tools, it is better to leverage and integrate with an existing MPI solution that may be used by a CCH integrating partner such as HIE which often includes a robust standard-based MPI solution.
Vocabulary Management	CCH systems will require collecting and reporting a vast amount of structured data that is coded in a certain manner for better tracking and reporting. Vocabulary management refers to the system capabilities that allow managing these codes for the structured data. Since many systems use proprietary codes internally, those codes often need to be mapped to the standardized codes to exchange with the external systems. Vocabulary management capability should also support such mapping and transformation of codes for various purposes. It is also recommended to use a standardized taxonomy or terminology system even internally to the system to minimize the mapping. A taxonomy is a way to classify controlled vocabulary in a hierarchical grouping for application in a specific domain or subject area. Terminology is a system of standardized terms or concepts that may be used as a source for specific coding. A robust vocabulary management system will allow organizing and linking such hierarchical grouping of taxonomy and standardized terminology with an internal coding. Sometimes there is also a need to use a subset of codes from an internal system or standardized taxonomy or terminology. A vocabulary management capability can also allow creating Value Sets that represent such subset of codes/concepts. Such vocabulary management solutions could get very complex and it is recommended to leverage a common solution that may already be implemented by one of the integrating partners such as EHR or HIE.

The architecture considerations above are important for typical system design and implementation, but the importance and approach taken may vary based on specific needs and constraints. Since CCH systems are likely be central hub for many different organizations, there may be conflicting requirements as well as constraints that should be enforced. Therefore, the architecture of CCH systems will need to be determined based on much wider context than just the lead organization implementing and supporting the systems.

Selecting and Implementing Technology Solutions

Selecting and implementing technology solutions can be a complex process, but it is important to ensure that the solution meets the needs of the organization and is effective. Here are some considerations for selecting and implementing technology solutions:

Compatibility—is an important consideration when selecting a technology solution. It is important to consider the compatibility of the technology solution with existing systems, including EHRs, case management systems, and referral platforms. The solution should be able to integrate with these systems to ensure that data can be exchanged securely and efficiently. Compatibility also ensures that the solution can be used by all members of the care team, including healthcare providers, social workers, and community-based organizations.

Scalability—is another important consideration. As organizations grow and evolve, their technology solutions should be versatile enough to adapt to changing needs. This includes managing larger data volumes, supporting more users, and adjusting to altered workflows. It is recommended to select a solution that can scale up with increased needs. However, sometimes a simple solution is more feasible on a smaller scale initially with a path to migrate to a new, more robust solution when there is need to scale up to handle more complex requirements and/or larger volumes. Hence, different tools might be required at different scales of growth instead of expecting a single tool to scale universally. This consideration is crucial, especially for organizations planning service expansion or penetration into new markets.

Ease of Use—should also be considered when selecting and implementing technology solutions. The solution should be intuitive and user-friendly, with a minimal learning curve. This can help to reduce the time and resources required for training and adoption. The solution should also be customizable (to the extent possible) to meet the specific needs of the organization and its users.

Security and Privacy Security—are critical considerations for any technology solution. The solution should be designed with security and privacy in mind, including encryption, access controls, and audit trails. The solution should also comply with relevant regulations and standards, such as the HIPAA Rules, HITRUST, HITECH, etc. See Chapter 2 for a more in-depth discussion of compliance and regulations.

Support and Maintenance—are also important factors to consider when selecting and implementing technology solutions. The solution should have a reliable support system in place, including technical support, training, and documentation. It's important to consider the level of support provided, such as 24/7 availability, response time, and escalation procedures. Additionally, it's important to consider the cost of support and maintenance, including any additional fees for upgrades or enhancements.

Enhancements—are critical to the success of any technology solution. The solution should be regularly updated and enhanced to ensure that it remains effective and meets the evolving needs of the organization. It's important to consider the frequency of updates and enhancements, as well as the process for implementing them. Some solutions may offer automatic updates, while others may require manual updates. It's also important to consider the cost of updates and enhancements, as some solutions may charge additional fees for new features or functionality.

By considering these factors when selecting and implementing technology solutions, organizations can ensure that the solution meets their needs and is effective in supporting coordinated care and

improving outcomes. It's important to note that security and privacy, support and maintenance, and enhancements are critical to the success of any technology solution.

CONCLUSION

Interoperability is crucial for CCHs to improve the quality of care provided to their clients. By sharing data with healthcare providers, aging and disability network partners, and other CBOs, CCHs can promote seamless coordination of care, reduce fragmentation, and improve health outcomes for all populations served.

This Playbook highlights the importance of understanding data structure, data elements, and partner agency reporting requirements as well as the various federal rules and regulations regarding it. CCHs must engage with their partners to establish data sharing agreements and implement privacy and security protocols to protect the privacy of client data. The Playbook emphasizes the legal and regulatory requirements guiding how CCHs can share data with their partners, such as the HIPAA Rules, and the importance of developing a compliance program to ensure that the organization is meeting all regulatory requirements.

Investing in a flexible IT infrastructure is essential for CCHs to support data sharing. CCHs should use IT systems that are compatible with their partners' systems and have the resources, either internally or outsourced, that manage and maintain the IT infrastructure and provide technical support to staff. Standardized data formats and coding systems are necessary to ensure that data can be easily shared and understood by all partners. A data governance framework is also essential to ensure that data is accurate, complete, and consistent.

CCHs should adopt a collaborative approach to data sharing, working with their partners to establish data sharing agreements and implementing privacy and security protocols. By doing so, CCHs can achieve interoperability and promote the seamless coordination of care, ultimately improving the health outcomes of their clients. By using this Playbook as a tool, CCHs can successfully move one step closer to achieving interoperability and promoting data sharing with their partners to improve the quality of care provided to their clients.

APPENDICES

Appendix A: Glossary of Terms

Term	Acronym	Definition
Accountable Care Organization	ACO	Groups of healthcare providers who work together to coordinate care for a specific population of patients. ACOs are designed to improve the quality and efficiency of healthcare services by incentivizing providers to work together to achieve better health outcomes and reduce healthcare costs.
Accountable Health Communities	AHC	A model of healthcare delivery that aims to address social determinants of health by connecting patients with community-based resources and services. The AHC model is designed to improve health outcomes and reduce healthcare costs by addressing the root causes of health disparities.
Activities of Daily Living	ADL	Those basic activities and behaviors that are the most fundamental self-care activities to perform, and that indicate whether a person can care for his/her own physical needs. On the DON-R, these activities are defined as eating, bathing, grooming, and dressing, transferring, and continence.
Administration for Community Living	ACL	An agency in the U.S. Department of Health and Human Services, ACL is one of the nation's largest providers of home and community-based care for older persons, people with disabilities, and their caregivers. Its mission pursuant to the federal Older Americans Act is to develop a comprehensive, coordinated, and cost-effective system of long-term care that helps older adults maintain their independence and quality of life in their homes and communities. ACL provides oversight for OAA funded programs through the aging network.
Affordable Care Act	ACA	A federal law that was enacted in 2010 with the goal of expanding access to healthcare and reducing healthcare costs. The ACA includes provisions for expanding Medicaid, establishing health insurance marketplaces, and implementing new payment models to incentivize high-quality, cost-effective care.
Aging and Disability Resource Center	ADRC	A collaborative effort of the Administration for Community Living (ACL) and the Centers for Medicare and Medicaid Services (CMS), ADRCs serve as single points of entry into the long-term system for older adults and people with disabilities.
Alliance of Information and Referral Systems	AIRS	The professional membership association for community Information and Referral (I&R), and the sole source for standards, program accreditation, and practitioner certification for the I&R sector.
Americans with Disabilities Act	ADA	The Americans with Disabilities Act of 1990, P.L. 101-336 prohibits discrimination by covered entities and ensures equal opportunity for qualified persons with disabilities in employment, state and local government services, public accommodations, commercial facilities, and transportation.
Application Programming Interface	API	Application Programming Interfaces are standardized interfaces that allow different computer systems to communicate with each other. APIs are more complex than point-to-point connections, but they offer greater flexibility and scalability. They are typically used for more complex integrations where multiple systems need to communicate with each other.
Area Agency on Aging	AAA	The entity designated by a state unit on aging pursuant to the Older Americans Act (OAA) to provide a comprehensive array of programs and services for older and vulnerable adults within a planning and service area for OAA programs.

Term	Acronym	Definition
Business Associate	BA	An individual or organization that performs certain functions or activities that involve the use or disclosure of protected health information (PHI) on behalf of a covered entity but is not a member of the covered entity's workforce. Examples of business associates include third-party billing companies, IT vendors, and attorneys.
Business Associate Agreement	BAA	A written agreement between a covered entity and a business associate that establishes the permitted uses and disclosures of protected health information (PHI) by the business associate. The BAA also requires the business associate to implement appropriate safeguards to protect the confidentiality, integrity, and availability of the PHI.
Business Continuity Plan	BCP	A concept used to create and validate a logistical plan for how the organization will recover and restore interrupted critical functions within a predetermined time after a disaster or extended disruption.
Care Coordination		The process of organizing and coordinating healthcare services for individuals with complex medical needs, with the goal of improving patient outcomes and reducing healthcare costs. Care coordination involves assessing an individual's needs, developing a care plan, and coordinating services such as medical appointments, medication management, and home health services.
Case Management		A collaborative process of assessment, planning, facilitation, care coordination, evaluation, and advocacy for options and services to meet an individual's health needs through communication and available resources to promote quality, cost-effective outcomes.
Center for Independent Living	CIL	Community-based organizations that provide services and support to individuals with disabilities to help them live independently. Centers for Independent Living offer a range of services, including advocacy, peer support, skills training, and information and referral services. The goal of Centers for Independent Living is to empower individuals with disabilities to live independently and participate fully in their communities.
Centers for Medicare & Medicaid Services	CMS	A federal agency within the U.S. Department of Health and Human Services (HHS) that administers the Medicare program and works in partnership with state governments to administer Medicaid, the Children's Health Insurance Program (CHIP), and health insurance portability standards. In addition to these programs, CMS has other responsibilities, including the administrative simplification standards from the Health Insurance Portability and Accountability Act of 1996 (HIPAA), quality standards in long-term care facilities (more commonly referred to as nursing homes) through its survey and certification process, clinical laboratory quality standards under the Clinical Laboratory Improvement Amendments, and oversight of HealthCare.gov.
Chronic Disease Self-Management Program	CDSMP	An evidence-based health and wellness program that helps individuals better manage their chronic conditions, improve their quality of life, and lower healthcare costs.
CoC Lead Agency		An organization or government department designated by a Continuum of Care (CoC) to administer and manage the CoC's Homeless Management Information System (HMIS). The CoC Lead Agency is responsible for ensuring that the HMIS is used to collect and report accurate data on the homeless population.

Term	Acronym	Definition
Common Security Framework	CSF	A set of controls and requirements developed by the Health Information Trust Alliance (HITRUST) to help healthcare organizations manage their information security and compliance with various regulations and standards. The CSF includes a comprehensive set of controls that align with various regulations and standards, including HIPAA, HITECH, and the NIST Cybersecurity Framework.
Community-Based Organization	CBO	A nonprofit organization that is rooted in and serving a specific geographic community or population. CBOs are typically run by and for members of the community they serve and may provide a wide range of services and supports. CBOs often work in partnership with government agencies, businesses, and other organizations to address community needs and promote social and economic development.
Community Care Hubs		A community care hub (CCH) is a community-focused entity that centralizes administrative functions and operational infrastructure to enable CBO/healthcare partnerships. Functions of the CCH include, but are not limited to, contracting with healthcare organizations; payment operations; management of referrals; service delivery fidelity and compliance; and technology, information security, data collection, and reporting. A CCH has trusted relationships with and understands the capacities of local community-based and healthcare organizations and fosters cross-sector collaborations that practice community governance with authentic local voices.
Community Health Needs Assessment	CHNA	A process used by healthcare organizations and public health agencies to identify the health needs and priorities of a specific community or population. The CHNA typically involves collecting and analyzing data on a range of health indicators, such as disease prevalence, health behaviors, and social determinants of health, as well as input from community members and stakeholders.
Consolidated Clinical Document Architecture	C-CDA	A standard developed by Health Level Seven International (HL7) for the exchange of clinical documents, such as discharge summaries, progress notes, and diagnostic test results. The C-CDA standard defines the structure and content of clinical documents to ensure that they can be exchanged between different healthcare systems and applications in a standardized format.
Continuous Quality Improvement		A philosophy and approach to quality improvement that emphasizes ongoing, incremental improvements to processes and systems. Continuous quality improvement involves collecting data, analyzing it, and using it to make changes to improve the quality and safety of healthcare services.
Continuum of Care	CoC	A collaboration of public, private, and nonprofit organizations that work together to prevent and end homelessness. CoCs are responsible for coordinating the delivery of housing and support services to homeless individuals and families within a specific geographic area.
Cost Accounting		The process of tracking and analyzing the costs associated with providing healthcare services. Cost accounting is used to identify areas where costs can be reduced or eliminated, and to improve the efficiency and profitability of healthcare organizations.

Term	Acronym	Definition
Covered Entities		Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, covered entities are healthcare providers who transmit any health information in electronic form in connection with a transaction for which HHS has adopted a standard, health plans, and healthcare clearinghouses. Covered entities are subject to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, which establish national standards for the protection of individuals' medical records and other personal health information.
Data Management		Activities including data entry of client and provider information, maintenance of automated information system software data information, and records management.
Department of Housing and Urban Development	HUD	A federal department responsible for administering programs that provide affordable housing and support services to low-income individuals and families. HUD is also responsible for developing policies and regulations related to housing and community development.
Electronic Health Record	EHR	Digital version of a patient's medical history maintained by healthcare providers and can be shared across different healthcare settings. EHRs contain information such as medical diagnoses, medications, allergies, immunization status, and laboratory test results.
Fast Healthcare Interoperability Resources	FHIR	A set of standards developed by Health Level Seven International (HL7) for exchanging electronic health information. FHIR is designed to be flexible, modular, and easy to implement, and is intended to improve interoperability between different healthcare systems and applications.
Federal Fiscal Year	FFY	Defines the U.S. government's budget cycle. It runs from October 1 of the budget's prior year through September 30 of the year being described.
Fee for Service	FFS	A payment model in healthcare where healthcare providers are paid for each service they provide to a patient. In a FFS model, healthcare providers are reimbursed for each individual service, such as a doctor's visit, diagnostic test, or medical procedure, based on a predetermined fee schedule. This model incentivizes healthcare providers to provide more services, which can lead to higher healthcare costs. FFS is often contrasted with value-based payment models, which incentivize healthcare providers to focus on delivering high-quality, cost-effective care rather than simply providing more services.
General Data Protection Regulation	GDPR	A regulation of the European Union that governs the collection, use, and disclosure of personal data of individuals located in the European Union. The GDPR applies to organizations located within the EU as well as organizations located outside the EU that process the personal data of EU residents. The regulation includes requirements for obtaining consent, providing access to personal data, and reporting data breaches.
Geographic Information System	GIS	A geographic information system that integrates hardware, software, and data for capturing, managing, analyzing, and displaying all forms of geographically referenced information.
Health Information Technology for Economic and Clinical Health Act	HITECH	A federal law passed in 2009 as part of the American Recovery and Reinvestment Act. The HITECH Act provides funding for the adoption and meaningful use of EHRs by healthcare providers. The law includes provisions for the development of health information technology standards, privacy and security regulations, and penalties for non-compliance. The goal of the HITECH Act is to promote the widespread adoption of EHRs to improve the quality and efficiency of healthcare services.

Term	Acronym	Definition
Health Information Trust Alliance	HITRUST	A non-profit organization that provides a common security framework (CSF) for healthcare organizations to manage their information security and compliance with various regulations and standards. The HITRUST CSF includes a set of controls and requirements that align with various regulations and standards, including HIPAA, HITECH, and the NIST Cybersecurity Framework.
Health Insurance Portability and Accountability Act of 1996	HIPAA	A federal law passed in 1996 that included Administrative Simplification provisions that required HHS to adopt national standards for electronic healthcare transactions and code sets, unique health identifiers, and security. HIPAA mandated the adoption of federal privacy protections for individually identifiable health information and establishes national standards for the protection of individuals' health information. The goal of HIPAA is to protect the privacy and security of individuals' health information while allowing for the flow of health information necessary to support high-quality healthcare. The HIPAA implementing rules include the Privacy, Security, Breach Notification, and Enforcement Rules. See the separate term for description of each rule.
Health Level Seven International	HL7	A non-profit organization that develops standards for the exchange, integration, sharing, and retrieval of electronic health information. HL7 standards are widely used in the healthcare industry to facilitate interoperability between different healthcare systems and applications.
Healthcare Effectiveness Data and Information Set	HEDIS	A set of performance measures developed by the National Committee for Quality Assurance (NCQA) to assess the quality of healthcare services. HEDIS measures are used by health plans, employers, and other organizations to evaluate and compare the quality of healthcare services provided by different healthcare providers.
Health-Related Social Need	HRSN	An individual's unmet, adverse social conditions (e.g., housing instability, homelessness, nutrition insecurity) that contribute to poor health and are a result of underlying social determinants of health (conditions in which people are born, grow, work, and age).
HMIS Lead Agency		An organization or government department designated by a Continuum of Care (CoC) to administer and manage the CoC's Homeless Management Information System (HMIS). The HMIS Lead Agency is responsible for ensuring that the HMIS is used to collect and report accurate data on the homeless population.
Home and Community Based Services	HCBS	A range of services and supports provided to individuals with disabilities and older adults in their homes and communities. HCBS programs are designed to help individuals live independently and avoid institutionalization. Services may include personal care, home healthcare, transportation, meal delivery, and in-home support services. HCBS programs are typically funded through Medicaid and administered by State agencies.
Homeless Management Information System	HMIS	A software system that collects and stores data on the homeless population. HMIS is used by Continuums of Care (CoCs) to track the number and characteristics of homeless individuals and families, and to monitor the effectiveness of housing and support services.
Information and Referral Program	I&R	A service that connects individuals and families with community resources and services to address their needs. I&R services provide information on a wide range of topics, such as healthcare, housing, employment, education, and social services. The goal of I&R services is to help individuals and families access the resources and services they need to improve their health and well-being.

Term	Acronym	Definition
Information Technology	IT	The use of computer systems, software, and telecommunications equipment to store, retrieve, transmit, and manipulate data. IT encompasses a wide range of technologies and applications, including hardware, software, networking, and cybersecurity. In healthcare, IT is used to manage EHRs, support clinical decision-making, and improve the efficiency and quality of healthcare services.
Institute for Healthcare Improvement's Model for Improvement		A quality improvement framework that involves setting specific, measurable goals, developing and testing interventions to achieve those goals, and using data to monitor progress and make adjustments as needed. The Model for Improvement is widely used in healthcare settings to improve patient outcomes and reduce costs.
Instrumental Activities of Daily Living	IADL	Activities that are necessary for independent living and community participation. IADLs are typically more complex than basic activities of daily living (ADLs) and require higher cognitive and physical functioning. Examples of IADLs include managing finances, shopping, preparing meals, using transportation, and managing medications. Assessment of IADLs is often used to evaluate an individual's ability to live independently and may be used to guide the development of care plans and support services.
Integrated Eligibility System	IES	A system that integrates multiple eligibility determination processes and systems for public assistance programs, such as Medicaid, Temporary Assistance for Needy Families (TANF), and Supplemental Nutrition Assistance Program (SNAP). An IES provides a single point of entry for applicants to apply for multiple programs, streamlines eligibility determination, and reduces administrative costs. An IES may also include decision support tools to help caseworkers make eligibility determinations and manage cases more efficiently.
Interoperability Rule		The Interoperability Rule is a set of regulations issued by the Centers for Medicare and Medicaid Services (CMS) that requires healthcare providers, health plans, and health information technology (IT) vendors to adopt standardized application programming interfaces (APIs) to improve the exchange of electronic health information (EHI). The Interoperability Rule includes provisions for patient access to their own health information, provider directory information, and payer-to-payer data exchange. The goal of the Interoperability Rule is to improve the interoperability of health IT systems and promote the seamless exchange of health information between different systems and organizations.
Long-Term Services and Supports	LTSS	A range of services and supports that help individuals with functional limitations and chronic conditions to perform daily activities and live as independently as possible. LTSS may include personal care, home healthcare, transportation, meal delivery, and in-home support services. LTSS are typically provided over an extended period of time and are designed to support individuals with ongoing care needs. LTSS may be provided in a variety of settings, including the home, community-based settings, and institutional settings.
Managed Care Organization	MCO	Managed care is a healthcare delivery system organized to manage cost, utilization, and quality. Medicaid managed care provides for the delivery of Medicaid health benefits and additional services through contracted arrangements between State Medicaid agencies and managed care organizations (MCOs) that accept a set per member per month (capitation) payment for these services.

Term	Acronym	Definition
Medicaid Managed Long-Term Services and Supports	MLTSS	Managed Long-Term Services and Supports (MLTSS) refers to the delivery of long-term services and supports through capitated Medicaid managed care programs. These services include HCBS Waiver services, skilled nursing facilities and all other services required to keep individuals in their setting of choice to receive long term care.
Medicare Hospital Value-Based Purchasing	HVBP	A payment model that links Medicare payments to the quality of care provided by hospitals. Hospitals are evaluated based on a set of quality measures, and their payments are adjusted based on their performance relative to other hospitals. The goal of the HVBP program is to incentivize hospitals to provide high-quality, cost-effective care.
Medicare Shared Savings Program	MSSP	A program that encourages the formation of accountable care organizations (ACOs) by offering financial incentives for improving the quality and efficiency of healthcare services. ACOs are groups of healthcare providers who work together to coordinate care for a specific population of patients.
Money Follows the Person	MFP	Federal grant to transition individuals living in nursing facilities into an independent community living environment.
National Committee for Quality Assurance	NCQA	A non-profit organization that develops and maintains standards for measuring and reporting on the quality of healthcare services. The NCQA's Healthcare Effectiveness Data and Information Set (HEDIS) is widely used in the healthcare industry to measure and report on healthcare quality.
No Wrong Door	NWD	No Wrong Door (NWD) is a network of state agencies and community-based organizations promoting access to LTSS through coordinated points of entry. The NWD system assists individuals navigating health and social care services through outreach, streamlined assessments, person-centered plans, information and referral to state and community-based resources, and a governance structure that ensures these functions are available and coordinated across the state.
Nursing Home	NH	Any facility who primarily provides skilled nursing care and related services to residents who require medical or nursing care; rehabilitation services to the injured, disabled, or sick; or on a regular basis, healthcare and services to individuals who because of their mental or physical condition require care and services (above the level of room and board) which is available to them only through these facilities and is not primarily for the care and treatment of mental diseases.
Older Americans Act	OAA	A federal law passed in 1965 that provides funding for a range of services and programs to support the health and well-being of older adults. The Older Americans Act (OAA) provides funding for programs such as meal delivery, caregiver support, transportation, and senior center programs. The law also includes provisions for the prevention of elder abuse, neglect, and exploitation. The OAA is administered by the Administration for Community Living (ACL) and is reauthorized every five years.
Older Americans Act Performance System	OAAPS	A performance measurement system used to evaluate programs funded by the Older Americans Act. OAAPS includes a set of standardized performance measures that are used to assess the effectiveness of programs that provide services to older adults.
Outsourcing		The practice of contracting with an outside vendor to provide a service or perform a function that is normally done in-house. Outsourcing is commonly used in the healthcare industry to manage non-core functions such as revenue cycle management, IT services, and medical transcription.

Term	Acronym	Definition
Population Health Management		An approach to healthcare delivery that focuses on improving the health outcomes of a specific population of patients. Population health management involves identifying and addressing the health needs of a population, developing and implementing interventions to improve health outcomes, and measuring the impact of those interventions.
Privacy Rule		A regulation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that sets national standards for the protection of individuals' medical records and other personal health information. The Privacy Rule applies to healthcare providers who transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard, health plans, and healthcare clearinghouses.
Program Performance Reports	PPRs	Reports required by the Administration for Community Living (ACL) for Centers for Independent Living (CILs) to provide information on their performance and compliance with federal regulations and guidelines. These reports include data on the number of individuals served, services provided, and outcomes achieved, as well as financial information and other programmatic data. PPRs are used by ACL to monitor and evaluate the effectiveness of CILs and to inform funding decisions.
Protected Health Information	PHI	Generally, any individually identifiable health information that is created, received, maintained, or transmitted by a covered entity or business associate, and that relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the payment for healthcare services provided to an individual. PHI is protected by the HIPAA Rules. Examples of protected health information include medical records, test results, and health insurance claim information.
Quality Improvement	QI	A systematic approach to improving the quality and safety of healthcare services. QI involves identifying areas for improvement, developing and implementing interventions to address those areas, and measuring the impact of those interventions.
Rapid Cycle Quality Improvement	RCQI	A quality improvement methodology that involves testing and implementing small-scale changes quickly and repeatedly to identify and address problems in real-time. RCQI is often used in healthcare settings to improve patient safety and quality of care.
Revenue Cycle Management	RCM	The process of managing the financial transactions and interactions between healthcare providers and patients throughout the entire healthcare revenue cycle, from patient registration and appointment scheduling to claims processing and payment collection. RCM includes activities such as verifying insurance eligibility, submitting claims, following up on denied claims, and collecting patient payments. The goal of RCM is to optimize revenue and cash flow while minimizing administrative costs and ensuring compliance with regulatory requirements.
Risk		The degree to which activities expose an individual or organization to the potential for financial loss, inappropriate disclosure of data, or other deficiencies that result from inadequate controls or ineffective use of human resources; the possibility that an event could adversely affect the organization; the tendency of a system or function to have problems; or the chance of injury, damage, or loss.
Risk Analysis	RA	The process of gaining an understanding of the amount of inherent risk and control risk present in the system to be examined and the use of that knowledge to correct the deficiencies creating that risk.

Term	Acronym	Definition
Security Rule		A regulation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that establishes national standards for protecting individuals' electronic personal health information (ePHI) that is created, received, used, or maintained by a covered entity or business associate.
Service Plan		A dynamic plan of action developed collaboratively between the case manager and the consumer/caregiver that is structured, action-oriented, and time-specific.
Single Entry Point	SEP	A system or process that allows individuals to access multiple publicly funded long-term services and supports (LTSS) programs through a single point of entry. SEP is designed to simplify the process of accessing LTSS programs and services, reduce duplication and fragmentation, and improve coordination and integration of care. SEP may be operated by a state agency, a managed care organization, or a community-based organization, and typically involves a comprehensive assessment of an individual's needs and preferences to determine eligibility and appropriate services.
Social Care Coordination		The process of coordinating social services for individuals who need help with activities of daily living, such as bathing, dressing, and meal preparation. Social care coordination involves assessing an individual's needs, developing a care plan, and coordinating services such as home health aides, transportation, and meal delivery.
Social Determinants of Health	SDOH	The social and economic factors that influence an individual's health, such as access to healthcare, education, employment, housing, and transportation. Social determinants of health are increasingly recognized as important factors in shaping health outcomes and healthcare utilization.
Social Health Access Referral Platforms	SHARP	Platforms that connect patients with community-based resources and services to address social determinants of health. SHARP platforms are designed to improve health outcomes and reduce healthcare costs by addressing the root causes of health disparities.
State Fiscal Year	SFY	The 12-month period used by a state government for budgeting and financial reporting purposes. The start and end dates of the SFY vary by state, but most states begin their SFY on July 1st and end on June 30th of the following year.
State Medicaid Agency		A state-level agency responsible for administering the Medicaid program, which is a joint federal-state program that provides health coverage to eligible low-income individuals and families. The SMA is responsible for implementing federal Medicaid regulations and guidelines, developing and managing the state's Medicaid plan, determining eligibility for Medicaid benefits, and overseeing the delivery of Medicaid services by healthcare providers. The SMA also works with the Centers for Medicare and Medicaid Services (CMS) to ensure compliance with federal requirements and to secure federal funding for the state's Medicaid program.
State Unit on Aging	SUA	The commonly used name for State Agencies on Aging as referred to in the federal Older Americans Act. They are agencies of state and territorial governments designated by governors and state legislatures to administer, manage, design, and advocate for benefits, programs, and services for older adults and their families and, in many states, for adults with physical disabilities.

Term	Acronym	Definition
Statewide Independent Living Council	SILC	A federally mandated council established by the Rehabilitation Act of 1973, as amended, that is responsible for developing, monitoring, and evaluating the implementation of the State Plan for Independent Living (SPIL). The SILC is composed of individuals with disabilities, representatives from centers for independent living (CILs), and other stakeholders, and is responsible for ensuring that the SPIL reflects the needs and priorities of individuals with disabilities in the state. The SILC also provides guidance and support to CILs and other organizations that provide services and supports to individuals with disabilities to promote independent living and community integration.
Total Quality Management	TQM	A management approach that focuses on continuous improvement of processes and systems to achieve customer satisfaction and improve organizational performance. Total quality management involves all employees in the organization and emphasizes the importance of data-driven decision making, customer focus, and continuous improvement.
Unit Cost Methodology	UCM	A cost accounting method that assigns costs to individual units of healthcare services, such as a patient visit or a specific medical procedure. Unit cost methodology is used to identify the cost of providing specific healthcare services, and to compare the costs of different healthcare providers.
Unit of Service		The means by which a service is quantified, reported, and in some cases, reimbursed. The unit may be stated as one hour, one contact, one visit, one trip, one session, etc.
User Acceptance Testing	UAT	User Acceptance Testing (UAT) is the trial and review process conducted by the owner or client of the object under test to confirm that the modification or addition meets requirements.
Value-Based Purchasing	VBP	A payment model that links payment to the quality and efficiency of healthcare services. In a value-based purchasing model, healthcare providers are incentivized to provide high-quality, cost-effective care, and are penalized for poor outcomes or high costs.

Appendix B: Additional Resources

Community Care Hub Spotlights

Western New York Integrated Care Collaborative

The Western New York Integrated Care Collaborative (WNYICC) is a collaborative of healthcare providers and community-based organizations that aims to provide integrated, coordinated care to individuals and communities in western New York. The collaborative was formed in 2014 in response to the need for more integrated and coordinated care for individuals with complex medical and social needs. WNYICC brings together healthcare providers (more than 30), social service organizations, and community members to provide holistic care that addresses the social determinants of health. The collaborative aims to improve health outcomes, reduce healthcare costs, and enhance the quality of life for program participants.

WNYICC also works to promote the use of technology and data analytics to improve the delivery of care. The collaborative uses a shared data platform to track program outcomes and identify opportunities for improvement. The platform allows healthcare providers and social service organizations to share information and coordinate care more effectively.

WNYICC is an innovative and collaborative approach to improving the delivery of care in western New York. By bringing together healthcare providers, social service organizations, and community members, the collaborative aims to provide integrated, coordinated care that improves health outcomes and enhances the quality of life for individuals and communities.

WNYICC works with Medicare Advantage plans, Medicaid managed care organizations (MCOs), and entities participating in the Global and Professional Direct Contracting Model to help connect beneficiaries with health-related social needs with social care providers participating in the Collaborative. One member of the Collaborative, LifeSpan, received healthcare referrals for more than 1,200 older adults between 2016 and 2019 and connected them with an average of four community-based services, which was associated with a 29 percent reduction in inpatient hospitalizations and a 28 percent reduction in emergency department visits.[13]

Alameda County Care Connect Initiative

The Alameda County Care Connect Initiative (CC) is a collaborative effort between the Alameda County Health Care Services Agency and community-based organizations to provide integrated care to individuals with complex medical and social needs in Alameda County, California. The initiative was launched in 2013 in response to the need for more coordinated and effective care for individuals with complex needs.

The CC initiative aims to provide integrated, patient-centered care that addresses the social determinants of health.

One key aspect of the CC initiative is the development and implementation of Community Care Teams (CCTs). These CCTs bring together healthcare providers, social service organizations, and community

[13] Chappel, A., Cronin, K., Kulinski, K., Whitman, A., DeLew, N., Hacker, K., Bierman, A. S., Wallack, S., Meklir, S. C., Monarez, S., Johnson, K. A., Whelan, E.-M., Jacobs, D., & Sommers, B. D. (2022, November 29). Improving Health and Well-being through Community Care Hubs. Accessed at: https://bit.ly/3On3Kdl

members to provide integrated, coordinated care to individuals with complex needs. The CCTs aim to improve health outcomes, reduce healthcare costs, and enhance the quality of life for program participants.

The CC initiative also works to promote the use of technology and data analytics to improve the delivery of care. The initiative uses a shared data platform to track program outcomes and identify opportunities for improvement. The platform allows healthcare providers and social service organizations to share information and coordinate care more effectively.

SARCOA / Community Care Solutions

SARCOA, an ADRC in Alabama's NWD system and one of 13 AAAs in Alabama, created Community Care Solutions (CCS) CCH, which facilitates contracts between health plans and providers and provides access to information and assistance with other ADRCs across the state. CCS primarily focuses on providing care transitions and addressing health-related social needs. In addition to their work through CCS, SARCOA also provides a centralized case management solution through a shared services agreement to all 13 AAAs statewide. This case management solution is one component of a multi-layered information technology (IT) statewide system designed to support the ADRCs, SDOH focused programs, and case management delivery systems.

Region IV Area Agency on Aging

Region IV Area Agency on Aging (AAA) partnered with Corewell Health South (a Primary Care First practice) to address health-related social needs (HRSNs), withthe goal of improving health and driving care in the primary care setting while reducing healthcare costs. To resolve barriers faced by community members, including older adults with multiple chronic conditions, Corewell Health and the Region IV AAA tapped into a network of CBOs. An Interagency Care Team (ICT) model was developed including an in-home assessment, health benefits counseling, and a health coach to connect patients to home and community-based services and training on chronic disease self-management. The Region IV AAA serves as the hub for access to the network of CBOs to meet identified HRSNs. An added value is support for caregivers, blending what patients need within the context of the families and communities that support them. The ICT model goes beyond coordination to action aimed at improving population health and reducing costs. Through the ICT) model, Region IV AAA and Corewell Health have successfully resolved 91% of patient barriers while reducing the cost of care by 55%.

Initiatives Promoting Use of HIEs

The following are examples of states that have successfully implemented initiatives to promote the use of Health Information Exchanges (HIEs) for exchanging referral information between community-based organizations (CBOs) and healthcare providers. These examples demonstrate the various approaches and programs that states have implemented to improve care coordination and address social determinants of health.

These examples highlight the potential of HIEs to improve care coordination and address social determinants of health. However, there are still challenges to overcome, such as data standardization, privacy and security, resource constraints, legal and regulatory barriers, and cultural barriers. Addressing these challenges will require a coordinated effort among stakeholders across the healthcare system, including CBOs, healthcare providers, policymakers, and technology vendors.

Here are examples of states that have implemented initiatives to promote the use of Health Information Exchanges (HIEs) for exchanging referral information between community-based organizations (CBOs) and healthcare providers:

- California: The California Health Care Foundation (CHCF) launched the "Community Information Exchange" program in 2019 to facilitate the exchange of health and social service information between CBOs and healthcare providers through HIEs. The program has awarded grants to HIEs and CBOs to support the development of data-sharing platforms and the implementation of interoperability standards. (Reference: https://www.chcf.org/project/community-information-exchange/)
- New York: The state of New York has implemented a statewide HIE called the Statewide Health Information Network for New York (SHIN-NY), which includes a "Community Provider Data Exchange" (CPDE) module. The CPDE allows CBOs to access and share patient health information with healthcare providers, with the goal of improving care coordination and addressing social determinants of health. (Reference: https://www.health.ny.gov/technology/statewide_planning/shin-ny/)
- Maryland: The state of Maryland has implemented a pilot program called the "Maryland Total Cost of Care Model" that includes a data-sharing platform for CBOs and healthcare providers. The platform, called the "Community Information Exchange", allows CBOs to share social determinants of health data with healthcare providers through HIEs, with the aim of reducing healthcare costs and improving patient outcomes. (Reference: https://www.healthit.gov/techlab/ipg/node/4/submission/56)
- It's worth noting that these are just a few examples of the many initiatives that are underway across the United States to promote the use of HIEs for exchanging referral information between CBOs and healthcare providers. The specific approaches and programs may vary depending on the state and local context.
- Colorado: In 2018, the Colorado General Assembly passed Senate Bill 18-022, which directed the state's Department of Healthcare Policy and Financing to develop a plan for integrating social determinants of health data into the state's HIE network. The resulting "Colorado All Payer Claims Database" includes data on social determinants of health, such as housing, transportation, and food security, which can be accessed by healthcare providers and CBOs to support care coordination and population health management. (Reference: https://www.colorado.gov/pacific/hcpf/colorado-all-payer-claims-database)
- Michigan: The state of Michigan has implemented a program called the "Michigan Health Information Network Shared Services" (MiHIN) that includes a "Community Care Connect" (CCC) module. The CCC module allows CBOs to share information about patients' social needs with healthcare providers through the MiHIN HIE network, with the goal of improving care coordination and addressing social determinants of health. (Reference: https://mihin.org/what-we-do/community-care-connect/)
- Oregon: In 2017, the Oregon Health Authority launched a pilot program called the "Oregon Community Information Exchange" (OCIE) that aimed to facilitate the exchange of health and social service information between healthcare providers and CBOs through HIEs. The program was initially focused on addressing the opioid epidemic by improving care coordination and referral processes for patients with substance use disorders. (Reference: https://www.oregon.gov/oha/HSD/OHPB/HIX-OCIE/Pages/index.aspx)

- Texas: In 2019, the Texas Health and Human Services Commission launched the "Texas Health Information Exchange" (THIE) program, which includes a "Community Information Exchange" (CIE) module. The CIE module allows healthcare providers and CBOs to exchange information about patients' health and social needs through the THIE network, with the goal of improving care coordination and addressing social determinants of health. (Reference: https://hhs.texas.gov/doing-business-hhs/provider-portals/health-information-exchange-texas)
- Rhode Island: In 2017, the Rhode Island Executive Office of Health and Human Services launched the "Health Information Exchange for Social Services" (HIE-SS) program, which enables the exchange of health and social service information between healthcare providers and CBOs through the state's HIE network. The program includes a "Community Resource Directory" that provides information on social services and resources available to patients in the state. (Reference: https://health.ri.gov/programs/detail.php?pgm_id=1497)
- Minnesota: The state of Minnesota has implemented a program called the "Minnesota Statewide Health Improvement Partnership" (SHIP), which includes a data-sharing platform for healthcare providers and CBOs called the "Community Health Information Exchange" (CHIE). The CHIE allows CBOs to share information about patients' social determinants of health with healthcare providers through the State's HIE network, with the goal of improving care coordination and population health. (Reference: https://www.health.state.mn.us/communities/ship/index.html)
- Indiana: In 2018, the state of Indiana launched the "Indiana Network for Patient Care" (INPC), a statewide HIE that includes a "Community Access to Data" module. The module allows CBOs to access patient data through the INPC HIE network, with the goal of improving care coordination and addressing social determinants of health. (Reference: https://www.in.gov/fssa/hip/2635.htm)

Software Platforms for Data Management and Reporting

There are several software platforms and data management tools available that can help to streamline reporting processes and improve data analysis. This appendix provides an overview of some of the software platforms that CCHs can use to manage different types of reporting, including program operations tracking, client outcomes tracking, and funder reporting. The platforms discussed in this appendix include ETO Software, Penelope Case Management Software, Salesforce Nonprofit Cloud, and Apricot by Social Solutions. These platforms are cloud-based and customizable to meet the specific needs of each organization, providing real-time data analytics and reporting to support effective decision-making and program improvement.

Social Solutions Apricot platform is a cloud-based software solution that can be used to track program operations, client outcomes, and funder reporting requirements, while the Salesforce Nonprofit Cloud platform provides data management and analytics tools that can be used to measure program impact and improve service delivery. (Reference: https://www.socialsolutions.com/software/apricot/)

- **CharityTracker.** A cloud-based data management platform designed for non-profit organizations, including CBOs. The platform includes modules for case management, program operations tracking, client outcomes tracking, and funder reporting. (Reference https://www.charitytracker.com/)
- **ClientTrack**. A cloud-based data management platform designed for non-profit organizations, including CBOs. The platform includes modules for case management, program operations

tracking, client outcomes tracking, and funder reporting. (Reference: https://eccovia.com/clienttrack/)

Program Operations Software

- **ETO Software**. ETO Software is a cloud-based data management and reporting platform designed for non-profit organizations, including CBOs. The platform includes modules for case management, program operations tracking, funder reporting, and performance measurement. ETO Software is customizable to meet the specific needs of each organization and provides real-time data analytics and reporting. (Reference: https://www.socialsolutions.com)
- **Penelope Case Management Software**. Penelope Case Management Software is a cloud-based data management platform designed for human services organizations, including CBOs. The platform includes modules for case management, program operations tracking, client outcomes tracking, and funder reporting. Penelope is customizable to meet the specific needs of each organization and provides real-time data analytics and reporting. (Reference: https://www.athenasoftware.net/penelope/)
- **Salesforce Nonprofit Cloud**. Salesforce Nonprofit Cloud is a cloud-based data management platform designed for non-profit organizations, including CBOs. The platform includes modules for fundraising, program operations tracking, client outcomes tracking, and funder reporting. Salesforce Nonprofit Cloud provides real-time data analytics and reporting, as well as tools for donor management and marketing. (Reference: https://www.salesforce.org/nonprofit/nonprofit-cloud/)
- **Apricot by Social Solutions**. Apricot by Social Solutions is a cloud-based data management and reporting platform designed for non-profit organizations, including CBOs. The platform includes modules for case management, program operations tracking, client outcomes tracking, and funder reporting. Apricot is customizable to meet the specific needs of each organization and provides real-time data analytics and reporting. (Reference: https://www.socialsolutions.com/software/apricot/)

Sample HIPAA Privacy Rule Compliance Checklist

HIPAA Privacy Rule Compliance Checklist for Software Systems:

In addition to the requirements associated with the HIPAA Security Rule, the following checklist should be used to guide compliance with the HIPAA Privacy Rule:

Data Masking and De-identification:

☐ Data masking features for displaying PHI with obfuscated or anonymized data

☐ De-identification functionality to remove or replace identifying information from PHI

Consent Management:

☐ Integration with the Notice of Privacy Practices (NPP)

☐ Ability to track and enforce client restrictions on PHI use or disclosure

Data Minimization:

☐ Features to ensure data collection and sharing adheres to the minimum necessary standard

☐ Mechanisms for limiting access to PHI based on context and purpose

Privacy by Design:

☐ Privacy principles integrated into software design and architecture

☐ Privacy impact assessments (PIAs) conducted during development and updates

☐ Regular privacy reviews and updates to ensure ongoing compliance

Policy and Procedure Management:

☐ Functionality for managing and maintaining privacy policies and procedures

☐ Integration with other systems to enforce policies and procedures

** This checklist has not been developed by HHS and is provided as an example of public private sources available. Resources used to inform checklist: [14, 15]

HIPAA Security Rule Toolkit

The NIST HIPAA Security Rule Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from large nationwide health plans with vast information technology (IT) resources to small healthcare providers with limited access to IT expertise.

The HIPAA Security Rule Toolkit User Guide explains how to use the toolkit.

The install guide addresses how to install the toolkit for each supported operating system.

Toolkit installers for Windows, Red Hat Enterprise Linux, and MAC OS operating systems can be found below.

Questions about the NIST HIPAA Security Rule Toolkit can be submitted to hsr-toolkit@nist.gov.

Microsoft Windows Version

Released: 11/21/2011

Download: Setup_HSR_Toolkit.zip (Download 22.4 MB)

SHA-256: 5822FF2B093361CF7BC13EE536E27E196B4142EE10FCEFFF8C5F04484E03F030

[14] The HIPAA Journal. (2023). HIPAA Compliance Checklist. Accessed at: https://bit.ly/3Qh8pQq.

[15] Inspired eLearning. (2023). HIPAA Security Rule and Compliance Checklist. Accessed at: https://bit.ly/44JshjC.

Red Hat Enterprise Linux Version

Released: 11/21/2011

Download: HSRToolkit-1.0-1.noarch.zip (Download 8.56 MB)

SHA-256: 057C8F782B4E290239A3BBC83A784D26BC2A28F4AC7BB2491242CB2C32BEF37B

Apple Mac OS Version

Released: 11/21/2011

Download: HSRToolkit.zip (Download 8.85 MB)

SHA-256: AC6684DA25BF8C5FF9A5B850429133DADECCF7731A542FC87D1DA7036C7B5609

Security Risk Assessment Tool (SRA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule requires that covered entities and their business associates conduct a risk assessment of their healthcare organization. A risk assessment involves the identification of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. To learn more about the assessment process and how it benefits your organization, visit the Office for Civil Rights' official guidance.

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights, developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the risk assessment process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) EHR Incentive Program. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's computer. HHS does not collect, view, store, or transmit any information entered into the SRA Tool.

Download Version 3.3 of the SRA Tool for Windows [.msi - 70.3 MB]

SRA Tool Excel Workbook

This version of the SRA Tool takes the same content from the Windows desktop application and presents it in a familiar spreadsheet format. The Excel workbook contains conditional formatting and formulas to calculate and help identify risk in a similar fashion to the SRA Tool application. This version of the SRA Tool is intended to replace the legacy "Paper Version" and may be a good option for users who do not have access to Microsoft Windows or otherwise need more flexibility than is provided by the

SRA Tool for Windows. This workbook can be used on any computer using Microsoft Excel or another program capable of handling .xlsx files. Some features and formatting may only work in Excel.

Download Version 3.3 of the SRA Tool Excel Workbook [.xlsx - 128 KB]

SRA Tool User Guide

Download the SRA Tool User Guide for FAQs and details on how to install and use the SRA Tool application and SRA Tool Excel Workbook.

Download SRA Tool User Guide [.pdf - 6.4 MB].

Sample HIPAA Security Rule Compliance Checklist

Access Control:

[ ] Unique user identification for each user

[ ] Role-based access control (RBAC) for limiting access to ePHI based on user roles

[ ] Emergency access procedure for obtaining necessary ePHI during a crisis

[ ] Automatic logoff or timeout feature after a period of inactivity

[ ] Encryption of ePHI

Audit Controls:

[ ] Activity logging, including access, modification, and deletion of ePHI

[ ] Audit log review and reporting capabilities

[ ] Tamper-proof audit logs

[ ] Timestamps for audit log entries

[ ] Alerts for potential security incidents

Integrity Controls:

[ ] Mechanisms to ensure ePHI is not improperly altered or destroyed

[ ] 'Checksums' or other data integrity verification methods

[ ] Version control and change tracking

[ ] Secure backups of ePHI with integrity checks

[ ] Alerts for unauthorized alterations or deletions of ePHI

Transmission Security:

[ ] Secure data transmission protocols (e.g., SSL/TLS, VPN)

[ ] End-to-end encryption for ePHI transmission

[ ] Secure email and messaging systems for sharing ePHI

[ ] Secure file transfer capabilities

Authentication:

[ ] Multi-factor authentication (MFA) support

[ ] Password complexity and expiration policies

[ ] Mechanisms to verify the identity of entities requesting access to ePHI

Data Storage:

[ ] Encryption of ePHI at rest

[ ] Secure and compliant cloud storage support, if applicable

[ ] Data backup and recovery mechanisms

Patch Management:

[ ] Regular software updates and security patches

[ ] Vulnerability scanning and remediation

Integration and APIs:

[ ] Secure integration with third-party applications and services

[ ] Secure API management and access control

Incident Response:

[ ] Incident response and reporting capabilities

[ ] Integration with security information and event management (SIEM) tools

Training and Support:

[ ] Documentation and training materials for secure software use

[ ] Technical support for security-related issues

** This checklist has not been developed by HHS and are provided as an example of public and private resources available. Resources used to inform checklist: [16, 17, 18]

Value-based Purchasing, Incentives, and the Need for Data Sharing

CCHs are committed to providing high-quality, cost-effective care to individuals and beneficiaries. One approach to achieving this goal is through Value-based Purchasing (VBP), a healthcare payment model that rewards healthcare providers for the quality of care they provide, rather than the quantity of services they deliver. In a VBP system, healthcare providers are incentivized to focus on improving patient outcomes and experiences, as well as reducing healthcare costs. This model aligns financial incentives with improved healthcare outcomes, leading to better care, better health outcomes, and lower costs. VBP programs typically involve a shift away from traditional fee-for-service payments,

[16] U.S. Department of Health and Human Services. Health Information Privacy: Summary of the HIPAA Security Rule. (2023). Accessed at: https://bit.ly/44OTUaX

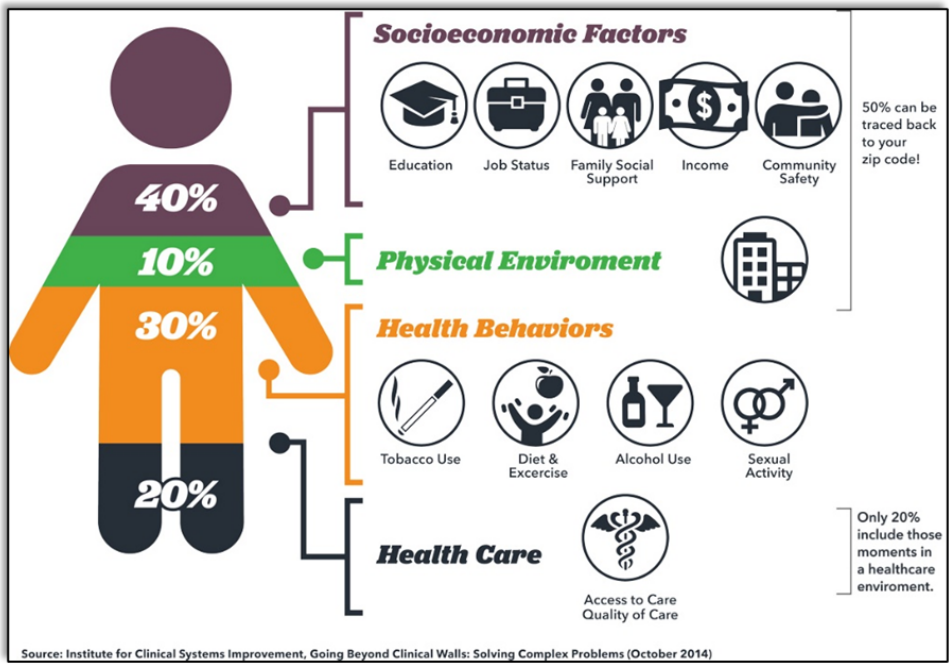
[17] The HIPAA Journal. (2023). HIPAA Compliance Checklist. Accessed at: https://bit.ly/3Qh8pQq

[18] Centers for Medicare & Medicaid Services. (2007). Accessed at: https://bit.ly/3OwH6Ad

which pay healthcare providers based on the volume of services they provide, regardless of quality. VBP is a powerful payment model that incentivizes healthcare providers to focus on providing high-quality, cost-effective care. CCHs can benefit from participating in VBP programs by being able to demonstrate the improvement in the quality of care they provide, reducing healthcare costs, and increasing patient satisfaction.

By focusing on quality metrics and cost savings targets, CCHs can improve care coordination, reduce hospital readmissions, and avoid unnecessary tests or procedures.

Exhibit 28. Representation of Factors Affecting Patient Health Outcomes



VBP programs incentivize healthcare providers to achieve specific quality metrics or cost savings targets, encouraging them to become more efficient in their care delivery. Additionally, VBP provides financial incentives for healthcare providers to focus on preventing illnesses and promoting health, rather than just treating illnesses after they occur. The growth of VBP initiatives creates significant opportunities for CCHs to help healthcare providers achieve better health and quality of life, especially given the research that illustrates that 80 percent of what makes up someone's health is determined by what happens outside of the hospital and health clinic. The largest segment is made up of the SDOH or socioeconomic factors, as shown in Exhibit 28.[1] These are the areas in which CCHs and their CBO partners excel.

VBP initiatives have the potential to improve patient outcomes, reduce healthcare costs, and promote greater efficiency and coordination within the healthcare system. By incentivizing healthcare providers to focus on improving the quality of care, VBP can lead to better patient experiences and outcomes.

Exhibit 29. Ways That VBPs Work in Healthcare

Specific Ways that VBPs Work in Healthcare	Description
Payment Tied to Performance	In VBP programs, payment is tied to performance. Providers may be incentivized to improve patient outcomes, reduce hospital readmissions, and improve clinical outcomes such as reduced mortality rates. Payment may also be tied to measures of patient experience, such as patient satisfaction surveys.
Quality Metrics	VBP programs typically use quality metrics to assess the performance of healthcare providers. These may include clinical measures, such as the percentage of patients who receive recommended preventive screenings, or patient experience measures, such as patient satisfaction scores. Providers may be rewarded financially for meeting or exceeding these metrics.
Financial Incentives	VBP programs typically provide financial incentives to healthcare providers who meet or exceed performance targets. These incentives may be in the form of bonuses or increased reimbursement rates. In some cases, providers may face financial penalties for failing to meet performance targets.
Risk Sharing	Some VBP programs involve risk sharing between payers and providers. For example, in Accountable Care Organizations (ACOs), providers are responsible for managing the health of a defined patient population. If the ACO is able to improve patient outcomes and reduce healthcare costs, the providers may share in the savings generated.
Data Sharing	VBP programs often require providers to share data with payers and other stakeholders. This data can be used to monitor provider performance, identify areas for improvement, and evaluate the effectiveness of VBP programs. Sharing data is a crucial component of many VBP programs. To assess provider performance and determine payment amounts, payers require access to clinical and claims data that allow them to evaluate the quality and cost-effectiveness of care. Sharing data enables providers to identify areas for improvement, monitor progress, and make data-driven decisions to optimize patient outcomes. However, sharing data raises concerns about patient privacy and the security of sensitive health information.

Sharing data is essential to evaluate provider performance and determine payment amounts in VBP programs. It allows payers to assess care quality and cost-effectiveness data, while enabling providers to identify areas for improvement and make data-driven decisions. Concerns about privacy and data security are addressed through data sharing agreements governed by legal requirements, such as HIPAA regulations. Some examples of how CBOs are asked to enter VBP arrangements can be found in Appendix B of this document.

The National Committee for Quality Assurance (NCQA) has played a significant role in advancing VBP in healthcare. NCQA is a non-profit organization that develops and maintains accreditation standards and performance measures for healthcare organizations, including health plans and provider organizations. One of NCQA's key initiatives in this area is the development of the Healthcare Effectiveness Data and Information Set (HEDIS), which is a widely used set of performance measures that assesses the quality of care provided by health plans. HEDIS measures cover a range of clinical areas, such as preventive care, chronic disease management, and behavioral health.

In recent years, NCQA has also been involved in efforts to develop and implement value-based payment models for healthcare providers. For example, NCQA collaborated with the Centers for Medicare & Medicaid Services (CMS) to develop the Patient-Centered Medical Home (PCMH) recognition program,

which incentivizes primary care practices to provide coordinated, patient-centered care. Additionally, NCQA developed a set of standards and measures for ACOs, which are groups of healthcare providers that work together to coordinate care and reduce costs. NCQA's ACO accreditation program evaluates ACOs on a range of measures related to care coordination, quality, and patient experience. In 2023, NCQA added a new measure to HEDIS called Social Need Screening and Interventions (SNS-E) that aims to tackle unmet social needs of health plans members (not provider level). The measure addresses food, housing, and transportation screening for both a need for and the occurrence of an intervention.

In a recent rule, CMS announced that Merit-based Incentive Payment System (MIPS) eligible clinicians, groups, or third-party intermediaries are required to report a Screening for Social Drivers of Health (MIPS 487) measure. The measure requires the patient to have a standardized health-related social needs (HRSN) for food insecurity, housing instability, transportation needs, utility difficulties, and personal safety screening done once per performance period. The implementation of a new HEDIS and MIPS 487 measures for HRSNs provides an opportunity for CCHs to directly participate in value-based payment models. One area of growth in VBP contracting includes payment incentives for providers to screen and address HRSNs and report the outcomes in alignment with these measures.

In addition to VBP, Medicare fee-for-service reimbursement is now available to Medicare Part B providers working with CBOs to provide Community Health Integration services, including assessment, planning, and coordinating home and community-based services that address HRSNs.

Examples of Value-Based Payment Arrangements and Reporting Requirements

VBP arrangements are becoming increasingly common in the healthcare industry, as payers and providers seek to improve health outcomes, reduce costs, and promote more efficient and effective use of healthcare resources. The following are some examples of how CCHs are being asked to enter VBP arrangements with healthcare providers and payers, including those that address social determinants of health, chronic disease management, care coordination, and population health management.

- Social determinants of health interventions: These arrangements may involve payment for successful outcomes, such as improved health outcomes or reduced healthcare costs, which result from CCH interventions. Another example of VBP arrangement with a community-based organization addressing social determinants of health is the Accountable Health Communities Model, which was launched by the Centers for Medicare & Medicaid Services (CMS) in 2017. Under this model, participating hospitals and health systems screen patients for health-related social needs, such as food insecurity and housing instability, and refer them to community-based organizations for assistance. (Reference: https://www.cms.gov/priorities/innovation/innovation-models/ahcm)
- Chronic disease management: CCHs that provide chronic disease management services, such as diabetes self-management education, may be asked to enter VBP arrangements with healthcare providers and payers. These arrangements may involve payment for successful outcomes, such as improved glycemic control or reduced hospital readmissions, which result from CCH interventions.
- Care coordination: CCHs that provide care coordination services, such as care transitions or medication management, may be asked to enter VBP arrangements with healthcare providers and payers. These arrangements may involve payment for successful outcomes, such as reduced hospital readmissions or improved patient satisfaction, which result from CBO interventions. Another example of a VBP arrangement with a community-based organization providing care coordination services is the Community Care Transitions Program, which was launched by CMS

in 2011. Under this program, participating hospitals partnered with community-based organizations to provide care coordination services to Medicare beneficiaries transitioning from hospital to home. The community-based organizations were reimbursed for their services based on the outcomes achieved, such as reduced hospital readmissions and improved patient satisfaction. (https://innovation.cms.gov/innovation-models/cctp/archived)

- Population health management: CCHs that engage in population health management, such as health promotion and disease prevention activities, may be asked to enter VBP arrangements with healthcare providers and payers. These arrangements may involve payment for successful outcomes, such as improved population health outcomes or reduced healthcare costs, which result from CCH interventions.
- VBP arrangements with CCHs are designed to encourage collaboration between healthcare providers and community-based organizations to improve health outcomes, reduce healthcare costs, and promote more efficient and effective use of healthcare resources. These arrangements can be a powerful tool for addressing social determinants of health and improving the health of vulnerable populations.
- Childhood immunization rates: CCHs that provide pediatric services may be required to report on childhood immunization rates, such as the percentage of children who receive recommended vaccines by age 2. (https://www.healthypeople.gov/2020/topics-objectives/topic/immunization-and-infectious-diseases/objectives)
- Patient satisfaction: CCHs that provide healthcare services may be required to report on patient satisfaction with the care received. This may be measured using a standardized survey tool, such as the Consumer Assessment of Healthcare Providers and Systems (CAHPS) survey. (Reference: https://www.cms.gov/Research-Statistics-Data-and-Systems/Research/CAHPS)
- Health outcomes: CCHs may be required to report on health outcomes achieved as a result of their services. For example, a CCH that provides chronic disease management services may be required to report on the percentage of participants who achieve improved glycemic control or blood pressure control. (https://www.ncbi.nlm.nih.gov/books/NBK220670/)
- Process measures: CCHs may be required to report on specific processes of care that are associated with improved health outcomes. For example, a CCH that provides diabetes education may be required to report on the percentage of participants who receive an annual foot exam or eye exam, which are recommended for individuals with diabetes. (https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/QualityMeasures)
- Cost of care: CCHs may be required to report on the cost of care for the services they provide. This may include the cost of medications, medical supplies, and other resources used in the delivery of care. (https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData)
- Avoidable hospital readmissions: CBOs that provide post-acute care services may be required to report on the percentage of patients who are readmitted to the hospital within 30 days of discharge. (https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/AcuteInpatientPPS/Readmissions-Reduction-Program)
- Chronic disease management: One example of a VBP arrangement with a community-based organization providing chronic disease management services is the Diabetes Prevention

Program (DPP), which was developed by the National Institutes of Health and the Centers for Disease Control and Prevention. The DPP is a lifestyle intervention program that helps participants with prediabetes make sustainable lifestyle changes to prevent or delay the onset of type 2 diabetes. Healthcare providers and payers may contract with community-based organizations to deliver the DPP and pay them based on the outcomes achieved, such as improved glycemic control and reduced healthcare costs. (https://www.cdc.gov/diabetes/prevention/about.htm)

Examples of state-specific quality reporting requirements for community-based organizations participating in value-based purchasing programs include:

- Maryland Total Cost of Care Model: CCHs that provide services to patients enrolled in Maryland's Medicaid program are required to report on the percentage of patients who receive an annual wellness visit, the percentage of patients who receive follow-up care within seven days of discharge from the hospital, and the percentage of patients who have a care plan that addresses their medical, behavioral, and social needs. (https://www.health.maryland.gov/mha/Documents/TCOC_CBO%20FAQ.pdf)
- New York State Value-Based Payment (VBP) Arrangements: CCHs that participate in New York's VBP program are required to report on quality measures related to care coordination, behavioral health, and medication management. For example, CBOs that provide care coordination services are required to report on the percentage of patients who have a care plan that addresses their medical, behavioral, and social needs. (https://www.health.ny.gov/health_care/medicaid/redesign/dsrip/docs/vbp_quality_metrics.pdf)
- However, many payers and regulatory agencies provide detailed guidance on the quality metrics that CCHs are required to report, along with instructions for how to report the data. CCHs may be required to report the data using a specific reporting tool or data submission portal. For example, the Centers for Medicare & Medicaid Services (CMS) provides detailed guidance on the quality measures that are used in various value-based purchasing programs, along with instructions for how to report the data. CMS also provides access to a data submission portal for participating providers and organizations. State-specific Medicaid agencies and other payers may also provide guidance and reporting tools for quality reporting. CBOs that are participating in value-based purchasing programs should consult the guidance provided by the payer or regulatory agency to ensure that they are reporting the required metrics correctly.
- "Value-Based Purchasing in Home- and Community-Based Services: A Primer for States" (National Academy for State Health Policy): This resource provides an overview of value-based purchasing in home- and community-based services and includes examples of quality metrics that CBOs may be required to report, as well as templates for data collection and reporting. https://www.nashp.org/wp-content/uploads/2018/06/Value-Based-Purchasing-in-Home-and-Community-Based-Services_A-Primer-for-States.pdf
- "Quality Measures for Community-Based Programs: A Guide to Selection and Use" (Centers for Medicare & Medicaid Services): This guide provides information on quality measures for community-based programs, including examples of metrics that CBOs may be required to report, and includes sample templates for data collection and reporting. https://www.cms.gov/files/document/quality-measures-community-based-programs-guide-selection-and-use.pdf

- "New York State Value-Based Payment (VBP) Resource Library" (New York State Department of Health): This resource library provides guidance and resources for providers and CCHs participating in New York's value-based payment program, including sample reports and templates for quality metric reporting. Link: https://www.health.ny.gov/health_care/medicaid/redesign/dsrip/vbp_library.htm

[1] Adopted from the Institute for Clinical Systems Improvement's Going Beyond Clinical Walls: Solving Complex Problems (October 2014).

Additional Resources:

- **ONC SDOH Toolkit**
  https://www.healthit.gov/sites/default/files/2023-02/Social%20Determinants%20of%20Health%20Information%20Exchange%20Toolkit%202023_508.pdf

The Social Determinants of Health Information Exchange Toolkit (Toolkit), produced by the Office of the National Coordinator for Health Information Exchange (ONC), can support communities working toward achieving health equity through SDOH information exchange and the use of interoperable, standardized data to represent SDOH. Stakeholders are increasingly planning and implementing information exchange initiatives to better coordinate and address SDOH service delivery challenges.

- **ONC Health IT Alignment Policy**
  https://www.healthit.gov/topic/hhs-health-it-alignment-policy

CCHs need to comply with federal policies when making procurement decisions and some policy may apply to shared services approaches. This may include standard health IT language in applicable grants, cooperative agreements, and contracts to ensure alignment of health IT investments, to the extent legally permissible.

Additional References

Centers for Medicare & Medicaid Services. (n.d.). Hospital Value-Based Purchasing. Retrieved April 24, 2023, from https://qualitynet.cms.gov/inpatient/hvbp/resources

Burwell, S. M. (2015). Setting value-based payment goals -- HHS efforts to improve U.S. health care. New England Journal of Medicine, 372(10), 897-899.

McWilliams, J. M., Gilstrap, L. G., Stevenson, D. G., Chernew, M. E., Huskamp, H. A., & Grabowski, D. C. (2017). Changes in post-acute care in the Medicare Shared Savings Program. JAMA Internal Medicine, 177(4), 518-526.

Miller, H. D. (2009). From volume to value: better ways to pay for health care. Health Affairs (Millwood), 28(5), 1418-1428.

Centers for Medicare & Medicaid Services. (n.d.). Quality Payment Program. Retrieved April 24, 2023, from https://qpp.cms.gov/

Bardach, N. S., Cabral, H. J., & Sanghavi, D. M. (2012). What can we learn from pay-for-performance for quality of care? Expert Review of Pharmacoeconomics & Outcomes Research, 12(6), 779-787.

Abrams, M. K., & Moulds, D. (2016, July 5). Integrating medical and social services: A pressing priority for health systems and payers. Health Affairs Blog. https://www.healthaffairs.org/do/10.1377/hblog20160705.055707/full/

Appendix C: IT System Functionality Checklist for Community Care Hubs

This checklist serves as a tool for CCHs looking to enhance their IT systems and related infrastructure.

General Functionality

1. Full lifecycle case and financial management support, including information and referral, intake, assessment and reassessment, care planning and service authorization, service delivery and payment, case closure, and reporting.
2. Secure, real-time access to data across stakeholders, including families and consumers, for collaboration purposes, ensuring compliance with all applicable laws and regulations.
3. User-defined view of end-user activities and responsibilities, such as upcoming activities, assessments due, care plan expirations and renewals, assigned consumers, and other client listings.
4. Automatic alerts for overdue, upcoming, and incoming tasks, referrals, activities, and events.
5. Predefined and user-defined assessment forms, including custom indicators to calculate need and enrollment eligibility status.
6. Comprehensive case management support, including tracking consumer, caregiver, and contact information, assessment and reassessment, detailed service planning and budgeting, electronic authorizations to providers, and real-time monitoring of service deliveries and outcomes.
7. Care planning support, including tracking needs, goals, and associated diagnoses.
8. Service authorization support, with the ability to identify services, frequencies, durations, and schedules of delivery.
9. Service rate definition options at the system, provider, and/or consumer level.
10. Service delivery support, including recording service deliveries, dates, times, durations, units, and service delivery notes.
11. Support for individual or bulk entry of services by agency and provider users in central and remote locations.
12. Tracking and sharing of referrals and other case management activities, such as program and agency referrals, follow-ups, consumer visits, and other activities.
13. Support for agencies with multiple programs and funding sources, including variations in eligibility criteria, business rules, funding rules, reimbursement rates, and data collection requirements.
14. Communication and collaboration support among programs, providers, and stakeholders through unified global consumer records and security permissions.
15. Web-based access for caregivers and consumers to service plans, schedules, and electronic communication with staff via standard web pages, ensuring compliance with all applicable laws and regulations.
16. HIPAA- and 5010-compliant electronic billing to third-party organizations, including Medicaid/State MMIS.
17. Inline/real-time data validation during invoice creation and end-user editing capabilities.

18. Provider management support, including provider contract and service information management, service and program contract management, automated billing and remittance tracking, and automatic audit trail creation.
19. A library of standard reports supporting all aspects of community care management and delivery.
20. Custom report-generation for enterprise management and ad-hoc reporting.
21. Automated file/report generation from system data for mandated reports, including state and local reports.
22. Tracking of modification history to all data and provision of event logs by record and worker.
23. User login/logout history tracking.
24. Standard user activity and history reports accessible by authorized users without server log examination.
25. Full control of user provisioning without vendor assistance.
26. Full control of assessment forms without vendor assistance.
27. Full control of assessment indicators and calculations for eligibility determination without vendor assistance.
28. Access to all applications, user documentation, and vendor news within a single site.
29. Bulk data entry tools for quick service recording to multiple people simultaneously, including the ability to confirm planned units as delivered.
30. Commercial-Off-the-Shelf (COTS) system with existing deployment in at least one other state for managing large populations of consumers with complex needs.
31. Ability to integrate with other systems, such as EHRs and electronic medical records.
32. Ability to meet all applicable Federal, State, and local regulations.

Referral Management

1. The ability to create a call record during or after contact with consumers or others seeking information or service referrals, ensuring compliance with all applicable laws and regulations.
2. The ability to track anonymous calls and calls for named consumers.
3. The ability to differentiate between consumers and callers within a call record.
4. The ability to search the database to determine whether a consumer record exists, automatically populating corresponding fields in the call record.
5. The ability to offer resource searching tools to quickly find providers and make appropriate referrals.
6. The ability to automatically create a consumer record from the information in the call record.
7. The ability to search for providers by geographic areas served, provider attributes such as languages and hours of operation, and services offered.
8. The ability to publish a resource directory to a standard public-facing website.

9. The ability to track information required for reporting, such as date and time of the call, source of the referral, date referral was received, call type, disability type, and call priority.
10. The ability to allow users to select call topics from an agency-defined list and perform a search for available services by keyword.
11. The ability to track the organizations to which the caller is referred, as well as information about the services they provide and their available capacity.
12. The ability to track call activities and outcomes in agency-defined drop-down menus.
13. The ability to track the time of the call or referral.
14. The ability to support assessment at the time of initial contact, allowing staff to conduct initial eligibility or screening assessments for services, and link the assessment to the call record and consumer record.
15. The ability to track applications for services throughout the application process, allowing users to update and add documents and notes to the application.
16. The ability to track documentation for applications, managing due dates and follow-up reminders to complete the application process.
17. The ability to schedule appointments for assessment and follow-up.
18. The ability to generate electronic referrals at the time of the call to internal departments and providers with access to the system.
19. The ability to identify the internal person for the referral and required action and set the date for completion.
20. The ability to include essential information about consumers, including risk levels, to assist with triage and prioritization.
21. The ability to automatically alert staff and providers to new referrals and consumers through a real-time dashboard.
22. The ability to integrate with the case management system, allowing the creation of consumer records from calls and linking between calls and consumers.
23. The ability to integrate with the provider management system, allowing referral to specific providers from calls and linking between calls and providers.

Public Facing Features and Consumer-Directed Care Features

1. The ability to publish data in a read-only manner to a public-facing website.
2. A public-facing website that is easy to use and does not require any web design expertise.
3. A public-facing website that allows consumers to search for resources and services, including providers, programs, and benefits.
4. A public-facing website that is integrated with the case management resource database, so that consumers can see a comprehensive list of available resources.
5. A public-facing website that allows consumers to request accounts on the site, so that they can access their personal information and participate in care planning.
6. A public-facing website that is secure and compliant with all applicable laws and regulations.

7. The ability for consumers to participate in care planning, including the selection of providers and the management of services.
8. The ability for consumers to communicate securely with their case manager.
9. The ability for administrators to modify the look and feel of the site.

Assessments and Reassessments

1. Support for assessment and reassessment throughout the life cycle of consumer contact, including clinical and financial eligibility assessments, as well as assessments for other purposes.
2. Standard assessment forms as well as facility for creating agency-defined assessments by non-technical users without vendor assistance.
3. Real-time calculations to assist in eligibility determinations and/or scoring.
4. The ability for assessors to enter not only a response for each question, but an individualized note attached to each response.
5. The ability to conduct reassessments as needed and at prescribed intervals, with automated reminders to users.
6. An assessment form builder usable by non-technical users without vendor assistance
7. Role-based authorization to create assessment forms
8. Central management of assessment forms
9. The ability to specify certain questions as required based on the response to a particular question
10. The ability to print assessment forms
11. The ability to share assessment forms with other service providers
12. The ability to conduct remote assessments by deploying assessment forms on non-networked devices for consumer assessments, with network synchronization later.
13. The ability to support multiple assessments per consumer, with security-controlled access by users.
14. The ability to provide reassessment feature using any prior assessment wherein the system will prefill responses to the assessment using previous answers, allowing users to edit, add, or delete responses.
15. The ability for assessment items to allow user-configured response types including selection from a single response from several options (i.e., multiple choice, Likert scales, yes/no, etc.), multiple responses from a list, text fields, and numeric values.
16. The ability for authorized users to configure assessments such that questions may be shown or hidden based on the responses to other questions, e.g., questions about pregnancies may be hidden unless a consumer answers affirmatively to “Have you ever been pregnant?”
17. The ability for assessment item response options, scores, and weights to be user-configured (i.e., agency may define acceptable responses for assessment items).
18. The ability to score assessment responses through a variety of user-configured methods and for scores to be calculated using mathematical and logical operations.

19. The ability for assessment questions to be saved in a catalog of questions, allowing questions to be used in multiple assessment instruments.
20. The ability for catalog questions to allow users to view history of previous responses on that question across any other assessment performed on the same consumer that uses the question.
21. The ability for assessments containing catalog questions to be automatically pre-populated by previous answers by the consumer to the same questions.
22. The ability for assessments to be able to be completed online or be "checked out" to mobile devices for completion in a disconnected state, and the finished assessment "checked in" and accessible from the consumer record.
23. The ability to publish read-only assessment information to consumers and other authorized stakeholders.
24. The ability to integrate with other systems, such as EHRs and case management systems.
25. The ability to provide data analytics and reporting on assessment data.
26. The ability to meet all applicable federal, state, and local regulations.

Appendix D: Sample Templates and Checklists

HIPAA Compliance Checklist

I. Administrative Safeguards

1. Have you conducted the following six required periodic Audits/Assessments?
   [ ] Security Risk Assessment
2. Have you documented all deficiencies?
   [ ] Documenting Risks and Gaps
3. Have you created remediation plans to address deficiencies found in all six Audits?
   [ ] Remediation Plans
4. Are these remediation plans fully documented in writing?
   [ ] Written Documentation
5. Do you update and review these remediation plans annually?
   [ ] Annual Updates
6. Are annually documented remediation plans retained in your records for six years?
   [ ] Record Retention
7. Have all staff members undergone annual HIPAA training?
   [ ] Staff Training
8. Do you have documentation of their training?
   [ ] Training Documentation
9. Is there a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer?
   [ ] Designated Officer
10. Have all staff members read and legally attested to the Policies and Procedures?
    [ ] Policies and Procedures

II. Vendors and Business Associates

1. Have you identified all your vendors and business associates?
   [ ] Vendor Identification
2. Do you have Business Associate Agreements in place with all business associates?
   [ ] BA Agreements
3. Do you have policies and procedures relevant to the HIPAA Privacy, Security, and Breach Notification Rules?
   [ ] Relevant Policies and Procedures
4. Do you have documentation for annual reviews of your policies and procedures?
   [ ] Annual Review Documentation
5. Do you have documentation of their legal attestation?
   [ ] Legal Attestation Documentation
6. Have you performed due diligence on your business associates to assess their HIPAA compliance?
   [ ] Due Diligence

7. Are you tracking and reviewing your Business Associate Agreements annually?
   [ ] Annual BA Agreement Review
8. Do you have Confidentiality Agreements with non-business associate vendors?
   [ ] Confidentiality Agreements

III. Incident and Breach Management

1. Do you have a defined process for incidents or breaches?
   [ ] Defined Process
2. Do you have the ability to track and manage the investigations of all incidents?
   [ ] Incident Tracking
3. Are you able to provide the required reporting of minor or meaningful breaches or incidents?
   [ ] Reporting Capabilities
4. Do your staff members have the ability to anonymously report an incident?
   [ ] Anonymous Reporting

IV. Additional Considerations for 2023

1. Ensure compliance with Privacy and Security rules, especially for online healthcare services.
2. Create policies to manage digital health interactions, including staff members browsing social media in the workplace.
3. Implement data encryption for portable drives, laptops, mobile devices, and transmitted data.
4. Plan ahead for future reviews, maintaining complete and systematic documentation.
5. Understand the difference between required and addressable specifications.
6. Take a systematic approach to addressable specifications and risk assessments.
7. If needed, seek help from expert consultancies or network security providers.

Remember, if audited, you must provide all documentation for the past six years to auditors. This checklist has not been developed by HHS and is provided as an example of public and private sources available. This checklist serves as a guide to help you self-evaluate your organization's HIPAA compliance. Regularly update and review your policies, procedures, and documentation to ensure continued compliance.
https://www.hipaajournal.com/wp-content/uploads/2018/08/HIPAA-Journal-HIPAA-Compliance-Checklist.pdf

Sample Screening Tools

AAFP Short-Form Social Needs Screening Tool

American Academy of Family Physicians
Eleven-question Provider Short-Form Social Needs Screening Tool. Questions 1-10 are reprinted with permission from the National Academy of Sciences, courtesy of the National Academies Press, Washington, D.C. Published as part of the American Academy of Family Physician's EveryONE Project.
https://www.aafp.org/dam/AAFP/documents/patient_care/everyone_project/provider-short-print.pdf

Access Health Spartanburg Screening Tool

AHS specializes in helping uninsured, low-income individuals coordinate their health care and connect to community resources. It accomplishes this through a network of 10 community partners, including two local hospital systems (Spartanburg Regional Health Care System and the smaller, private, Mary Black Hospital System); the county's drug and alcohol commission, as well as its Department of Mental Health; and Welvista, a statewide prescription assistance program. AHS also has relationships with numerous local nonprofits, including food banks, farmers' markets, shelters, and more. Physicians volunteer their time and provide AHS clients with free medical care at area clinics and hospital-affiliated practices.
https://www.chcs.org/media/AccessHealth-Social-Determinant-Screening_102517.pdf

The Accountable Health Communities Health-Related Social Needs Screening Tool Centers for Medicare & Medicaid Services

This tool was developed for use in the Center for Medicare & Medicaid Innovation's Accountable Health Communities (AHC) Model. The original version, published in May 2017, included 10 questions covering five domains: housing instability, food insecurity, transportation difficulties, utility assistance needs, and interpersonal safety. An updated and expanded version was released in January 2018 that modified the original questions slightly and added eight supplemental domains: financial strain, employment, education, family and community support, physical activity, substance use, mental health, and disabilities.
https://innovation.cms.gov/Files/worksheets/ahcm-screeningtool.pdf

https://nam.edu/wp-content/uploads/2017/05/Standardized-Screening-for-Health-Related-Social-Needs-in-Clinical-Settings.pdf

Arlington Screening Tool

https://sirenetwork.ucsf.edu/sites/default/files/2021-02/Arlington%2520Screening%2520Tool-%2520Final%2520version.pdf

Boston Medical Center-Thrive Screening Tool

Boston Medical Center (BMC) has implemented a social determinants of health screener for primary care patients in order to better identify and address patients' unmet social needs. Clinician researchers developed the EHR model, THRIVE, which facilitates an automatic print out of referral information for resources based at the hospital and in the community when the patient asks for help with a need they have identified in the screener. The hospital's work, published in *Medical Care*, demonstrates an innovative systematic model that can help clinicians better address the social needs of patients to improve their overall health.
https://sirenetwork.ucsf.edu/sites/default/files/2021-02/BMC-THRIVE.pdf

Relevant Templates and Guidelines

Health Information Technology Implementation Advanced Planning Document Template

https://www.cms.gov/regulations-and-guidance/legislation/ehrincentiveprograms/downloads/medicaid_hit_iapd_template.pdf

Estimating the Total Cost of Partnership

https://nff.org/file/934/download?token=8-D8hvto

Value Proposition Tool: Articulating Value

https://hudsonvalleyfundersnetwork.org/wp-content/uploads/2020/10/Value-Proposition-Tool.pdf

How to Partner with Hospitals for Community-Based Services

Sample MOU: How to Partner with Hospitals for Community-Based Services (ncoa.org)

Practice Management and Medical Billing

https://ng.nextgen.com/LP_20_A_Simple_Guide_Practice_Management_and_Medical_Billing_Medaxiom

PRAPARE Screening Tool

https://prapare.org/the-prapare-screening-tool/

Partnership Assessment Tool for Health

https://nff.org/fundamental/partnership-assessmenFt-tool-health

Interoperability in Healthcare

https://www.himss.org/resources/interoperability-healthcare

Value Based Payment (VBP) Guide

https://www.hca.wa.gov/assets/program/purchaser-toolkit.pdf

https://www.cms.gov/Medicare/Quality-Initiatives-Patient-Assessment-Instruments/Value-Based-Programs/HVBP/Hospital-Value-Based-Purchasing

SHARP Function Checklist

Decision Points for CBOs Considering Working with Social Health Access Referral Platforms
https://www.aginganddisabilitybusinessinstitute.org/wp-content/uploads/2022/02/SHARP-Function-Checklist-from-Aging-and-Disability-Business-Institute-at-USAging.pdf

Sample Data-Sharing and Usage Agreement

This agreement establishes the terms and conditions under which the *Data Owner Organization Name* and *Data User Organization Name* can acquire and use data from the other party. Either party may be a provider of data to the other, or a recipient of data from the other.

1. The confidentiality of data pertaining to individuals will be protected as follows:
    a. The data recipient will not release the names of individuals, or information that could be linked to an individual, nor will the recipient present the results of data analysis (including maps) in any manner that would reveal the identity of individuals.
    b. The data recipient will not release individual addresses, nor will the recipient present the results of data analysis (including maps) in any manner that would reveal individual addresses.
    c. Both parties shall comply with all Federal and State laws and regulations governing the confidentiality of the information that is the subject of this Agreement.

2. The data recipient will not release data to a third party without prior approval from the data provider.
3. The data recipient will not share, publish, or otherwise release any findings or conclusions derived from analysis of data obtained from the data provider without prior approval from the data provider.
4. Data transferred pursuant to the terms of this Agreement shall be utilized solely for the purposes set forth in the "Partnership Agreement".
5. All data transferred to *User Org* by *Owner Org* shall remain the property of *Owner Org* and shall be returned to *Owner Org* upon termination of the Agreements.
6. Any third party granted access to data, as permitted under condition #2, above, shall be subject to the terms and conditions of this agreement. Acceptance of these terms must be provided in writing by the third party before data will be released.

IN WITNESS WHEREOF, both the *Owner Org,* through its duly authorized representative, and *User Org*, through its duly authorized representative, have hereunto executed this Data Sharing Agreement as of the last date below.

Data Owner Organization	**Data User Organization**
Name	Name
Title	Title
Date:	Date:

Appendix E: Sample IT Security Contract Terms

Definition of Primary Contract Data – Primary Contract Data includes all data provided by or generated for Primary Contract including, but not limited to Protected Health Information (PHI), Personal Card Data (PCI), Personal Identity Information (PII), and other regulated and confidential information.

Survival - This clause should survive termination of the contract for as long as the Network Subcontractor has Primary Contract Data in its possession.

Definition of Personnel shall include Network Subcontractor's employees and any other persons who have access to Network Subcontractor's facilities, systems, or Primary Contract Data.

IT Security Language to be incorporated:

1. IT Security

1.1.1 **Security Program Requirements** – Network Subcontractor shall establish and maintain a comprehensive "Security Program" that has the physical, administrative, and technical safeguards to: (i) ensure the security and confidentiality Primary Contract Data; (ii) protect against threats/hazards to the security of Primary Contract Data, (iii) protect against any unauthorized use of or access to Primary Contract Data, and (iv) protect the integrity of Primary Contract Data. All of the foregoing shall be consistent with the Primary Contract IT Security Policies and Standards; shall be no less rigorous than those maintained by Network Subcontractor for its own data and information of a similar nature; and shall ensure compliance with the provisions of the applicable regulations such as Sarbanes-Oxley (SOX), the Health Information Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Payment Card Industry Data Security Standards (PCI DSS).

1.1.2 **Program Updates** - Network Subcontractor shall update its Security Program as necessary to comply with changes in Federal, State, and local laws and regulations pertaining to the privacy and protection of Primary Contract Data. Network Subcontractor shall ensure its Security Program stay's current with industry best practices with respect to new security standards and threats. If Network Subcontractor is unable to comply with such new laws, regulations, or security standards and threats, Partners shall have the right to immediately terminate the Agreement without liability.

1.1.3 **Policy and Procedure Updates** -Network Subcontractor shall review and update its security policies and procedures annually and upon request shall provide Partners a copy of the updated policies and procedures along with a report outlining material changes to Network Subcontractor's systems, applications, and security program.

1.1.4 Designated Account Security Representative - Network Subcontractor shall provide a designated focal point with responsibility for day-to-day security management to work with Partners' IT Security organization. This individual shall be at an appropriate level and with the authority to initiate corrective actions on behalf of Network Subcontractor as necessary to respond to and correct any Incident involving Primary Contract Data. If software development is involved, Network Subcontractor shall also identify the person who will be responsible for overall security of the application development, management, and update process.

1.1.5 **Termination Due To Security Breach** - Should Partners find that Network Subcontractor had a material security breach that resulted in disclosure of Primary Contract Data or that represents a material security risk in Primary Contract's reasonable discretion, Primary Contract shall have the right, in addition to all other rights and remedies under the Agreement, to immediately terminate the Agreement without further liability.

1.1.6 Return and Destruction of Data – Within ten (10) days of termination of the Agreement or if requested by Partners, Network Subcontractor shall provide a copy of all Primary Contract Data in a format specified by Primary Contract at no cost. Network Subcontractor shall permanently delete all Primary Contract Data from its systems and destroy all physical copies of Primary Contract Data stored at its facilities as requested by Partners. Upon request, Vendor shall provide a certification signed by an officer of the corporation that all Primary Contract Data has been permanently deleted from Network Subcontractor's systems and all physical files and have been destroyed. The certification shall specify the method and/or tools used to delete the files.

1.1.7 Security Incident Response and Reporting. A security "Incident" is any event that impairs the security of Primary Contract Data including any (i) unauthorized access, use, disclosure, modification, or destruction of Primary Contract Data; (ii) act that violates any law or any Primary Contract or Network Subcontractor security policy; (iii) unplanned service disruption that prevents the normal operation of the Services; or (iv) unauthorized access or attempt to access Network Subcontractors or Primary Contract applications, systems or Primary Contract Data. If Network Subcontractor detects or suspects an Incident, Network Subcontractor shall:

a) Notify Partners' IT Security Representative immediately and no later than within one (1) hour after Network Subcontractor becomes aware of a security Incident involving regulated data (PHI, PCI, SOX, etc.) or Primary Contract confidential data; business-critical environments, systems, services and/or applications; law enforcement or regulatory related; Internet systems/applications; likely to reflect negatively on Primary Contract or impact consumer confidence; and/or other material incidents. For other Incidents, notify Partners' IT Security within 24 hours.

b) Immediately perform Incident Management actions, and actions requested by Partners, including, but not limited to: responding and investigating; collecting, analyzing and preserving evidence; containing, remediating and mitigating adverse impacts; remediating, recovering, etc. related to the Incidents

c) If requested by Partners, prepare and deliver to Partners within five (5) business days of the Incident a root cause report that describes in detail (i) a description of the nature and extent of the Incident; (ii) the Primary Contract data disclosed, destroyed, or otherwise compromised or altered; (iii) all supporting evidence, including system, network, and application logs related to the incident; (iv) all investigative, corrective and remedial actions completed, and planned actions and the dates by which such actions will be completed; (v) all efforts taken to mitigate the risks of further Incidents; and (vi) an assessment of the security impact to Primary Contract. Upon Partners' request, Network Subcontractor shall provide Partners with immediate and ongoing access to all meetings, reports, copies of all logs and data, and other information that has a nexus to security Incidents impacting Primary Contract.

1.1.8 **Security Assessments.** Partners has the right to perform a security assessment on the Network Subcontractor (a "Security Assessment"). Upon Partners' request, Network

Subcontractor shall submit an IT Security Questionnaire and provide information and documentation on the security of their service, and any Services hereunder, to allow Partners to perform such a Security Assessment, and to determine the overall security of the Network Subcontractor and ability to comply with Primary Contract's IT Security Policies and Standards. In the event that Partners determines that such Initial Security Assessment indicates security concerns or issues which require mitigation, in Primary Contract's sole but reasonable opinion, Partners shall so notify Network Subcontractor in writing of any such concerns and/or issues with a request to provide an action plan for mitigation and/or correction of such concerns and/or issues. Network Subcontractor shall acknowledge receipt of such concerns within five (5) business days and shall provide an action plan for commercially reasonable correction of such issues and/or concerns within thirty (30) calendar days of receipt of such concerns. Primary Contract, Partners and Network Subcontractor shall work together in good faith to address and implement reasonable corrective actions. However, notwithstanding anything contained herein to the contrary, Partners shall have the right to terminate this Agreement in the event that Network Subcontractor cannot or does not, in Partners' sole by reasonable discretion, address and correct such concerns.

1.1.9 **Network Subcontractor Security Requirements.** Network Subcontractor's Security Program must meet the following requirements at a minimum. Network Subcontractor shall provide Partners appropriate documentation evidencing compliance with these requirements upon request.

(a) Password Requirements – At a minimum, passwords must be unique and exclusive, at least 8 characters in length, changed at least every ninety (90) days, and must include at least three of the following character types: numeric, upper- and lower-case letters, and special characters (! @#$%, etc.). Passwords associated with privileged user ids (such as those with administrator/root access privileges) and service accounts (used for machine to machine communications with no humans involved in providing the authentication at time of log in or job submission) must expire within 365 days. The minimum password length for privileged user IDs is 12 characters and 16 characters for service accounts.

(b) Access and Authorization - Network Subcontractor will employ physical and logical access control mechanisms to prevent unauthorized access to Network Subcontractor's facilities and systems associated with Primary Contract Data, applications, and systems and shall limit access to Personnel with a business need to know. Such mechanisms will have the capability of detecting, logging, and reporting access to the system or network or attempts to breach the security of the facility, compartment, system, network, application, and/or data.

a. Each person must have an individual account that authenticates the individual's access to Primary Contract Data. Network Subcontractor will not allow sharing of accounts.

b. Network Subcontractor will maintain a process to review access controls quarterly for all Network Subcontractor Personnel who have access to Primary Contract Data, applications, or systems, including any system that, via any form of communication interface, can connect to the system on which Primary Contract Data is stored. Network Subcontractor shall revoke access for any Personnel who no longer have a need for such access. Network Subcontractor will maintain the same processes of review and validation for any third party hosted systems it uses that contain Primary Contract Data.

c. Network Subcontractor will utilize two-factor authentication for network access/VPN

d. Network Subcontractor will revoke Personnel's access to physical locations, systems, and applications that contain or process Primary Contract Data within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s) or immediately if warranted or requested by Primary Contract.

(c) Data Transmission and Storage – Network Subcontractor shall not transmit or store Primary Contract Data outside the United States, or allow its employees or agents to download, extract, store, or transmit Primary Contract Data through personally owned computers, laptops, personal digital assistants, tablet computers, cell phones, or similar personal electronic devices.

(d) Security Patch Management – Network Subcontractor shall maintain and patch/remediate all systems, devices, firmware, operating systems, applications, and other software related to Primary Contract which are capable of receiving an update, patch, release, or modification.

i. Patching/remediation time frames must minimally meet the Primary Contract Security Patching Standards:

ii. Critical – as soon as practical and no later than 7 days

iii. High – within 30 days

iv. Medium – within 90 days

v. Low – within 180 days

(e) *Network Security* - Network Subcontractor will deploy appropriate firewall, intrusion detection/prevention, and network security technology in the operation of the Network Subcontractor's systems and facilities. Traffic between Partners and Network Subcontractor will be protected and authenticated and encrypted. Specifically, firewall(s) must be able to effectively perform stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing. Network Subcontractor will review firewall rule sets annually at a minimum to ensure that legacy rules are removed, and active rules are configured correctly. Network Subcontractor will deploy intrusion detection or preferably prevention systems (NIDS/NIPS) in order to monitor the network for inappropriate activity. Network Subcontractor shall deploy a log management solution and retain logs produced by firewalls and intrusion detection systems for a minimum period of one 1 year unless specified otherwise in this Agreement.

(f) *Malicious Code Protection* - All workstations and servers must run anti-virus software. Virus definitions must be updated within 24 hours. Network Subcontractor will have current anti-virus software configured to run real-time scanning of machines at regularly scheduled interval not to exceed seven (7) calendar days.

Network Subcontractor will scan incoming content for malicious code on all gateways to public networks including email and proxy servers.

(g) Data Encryption **-** Network Subcontractor will minimally utilize the following encryption algorithms and key strengths to encrypt Primary Contract Data when in transit, at rest in any application or system, or transported/stored via any physical media (e.g., tapes, disks, etc.):

i. Symmetric encryption: 3DES (≥ 168-bit, CBC mode); RC4 (≥ 128-bit, CBC mode); AES (≥ 128-bit, CBC mode);

ii. Asymmetric encryption: RSA (≥ 2048-bit); ECC (≥ 160-bit); El Gamel (≥ 1024-bit);

iii. Hashing: SHA2 with "salt" shall be added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings.

If personal computers or mobile devices (e.g., desktops, laptops, mobile phones, tablets) are used to perform any part of the Services, Network Subcontractor will encrypt all Primary Contract Data on such mobile devices.

Where encryption is utilized, Network Subcontractor will maintain a key management process that includes appropriate access controls to limit access to private keys (both synchronous and asynchronous) and a key revocation process. Private keys must not be stored on the same media as the data they protect.

(h) Physical Data - Network Subcontractor shall not keep any Primary Contract Data in physical form unless required as part of providing the Services and is authorized by Primary Contract.

1.1.10 **Designated IT Security Representatives** - The following individuals are Partners' and Network Subcontractor's IT Security Representatives. All notifications required under the IT Security clause of the Agreement shall be made to these individuals.

Partners:

Name:

Phone:

E-mail:

Network Subcontractor:

Name:

Phone:

E-mail:

2. Primary Contract Data:

Background Checks, Drug Screening and Training - Prior to assigning any Personnel to positions in which they are reasonably expected to have access to Primary Contract Data, Network Subcontractor and its subcontractors, agents, etc. will conduct background checks, drug screening and ensure all individuals are trained with respect to Network Subcontractor's security policy and procedures.