HUU Database Requirements (in progress)

Context:

As the Home Unite Us team continues its planning process and preliminary development, they would like to identify requirements related to data processing and storage, including compliance and security requirements. Identifying requirements early will minimize future rework.

Objective:

- Identify requirements for data processing and storage, along the following dimensions:
    - Legal requirements - must do
    - Customer demand
    - Industry best practices
- Include the above requirements in relevant Epics and Issues
- Provide documentation and resources related to the above requirements

Compliance Frameworks:

- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- Homeless Management Information System (HMIS)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- SOC-2

Summary:

Framework	**Legally Required / Covers HUU**	**Notes**
GDPR	No	Applies if information is collected on people from the EU
CCPA	No	Does not apply to nonprofit

		organizations
HIPAA	No	CoCs are not covered entities under HIPAA
SOC-2	No	SOC-2 is a standard for an audit, it is not a legal requirement

Assumptions:

- Currently (March 2023), the Home Unite Us application is not publicly available and does not have any users
- The Home Unite Us application must meet applicable legal and compliance requirements before being made publicly available and accepting users
- Host Home programs want/need HMIS integration (to confirm)
    - Host Home programs already have their own HMIS systems (to confirm)
    - Home Unite Us should allow Host Home programs to integrate data into HMIS systems (to confirm)
    - → Home Unite Us is not a CoC but serves the same population as a CoC. Recommend that HUU follow the HMIS privacy, security, and confidentiality standards Source

Open Questions:

- What are the legal requirements that apply to Home Unite Us with respect to data processing and storage?
- What requirements do alternative products meet?
- Which epics and user stories is this relevant for?
- Do Host Home organizations use HMIS today? If yes, which service do they use and why?
- What is the difference between the various HMIS vendors?
- When is the right time to implement an HMIS integration? Is it better to start on AWS then migrate to HMIS or to start with HMIS from the beginning?

What is a Homeless Management Information System (HMIS)?

"A Homeless Management Information System (HMIS) is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless

individuals and families and persons at risk of homelessness. Each Continuum of Care (CoC) is responsible for selecting an HMIS software solution that complies with HUD's data collection, management, and reporting standards." Source

What is a Continuum of Care (CoC)?

"The Continuum of Care (CoC) Program (24 CFR part 578) is designed to promote a community-wide commitment to the goal of ending homelessness; to provide funding for efforts by nonprofit providers, states, Indian Tribes or tribally designated housing entities (as defined in section 4 of the Native American Housing Assistance and Self-Determination Act of 1996 (25 U.S.C. 4103) (TDHEs)), and local governments to quickly rehouse homeless individuals, families, persons fleeing domestic violence, dating violence, sexual assault, and stalking, and youth while minimizing the trauma and dislocation caused by homelessness; to promote access to and effective utilization of mainstream programs by homeless individuals and families, and to optimize self-sufficiency among those experiencing homelessness." Source

"A Continuum of Care (CoC) is a regional or local planning body that coordinates housing and services funding for homeless families and individuals.

HUD requires communities to submit a single application for McKinney-Vento Homeless Assistance Grants in order to streamline the funding application process, encourage coordination of housing and service providers on a local level and promote the development of Continuums of Care (CoCs). A lead agency is designated to coordinate and submit the annual application. LAHSA is the lead agency for the Los Angeles CoC.

According to HUD, a CoC is "a community plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximize self-sufficiency. It includes action steps to end homelessness and prevent a return to homelessness." HUD identifies four necessary parts of a continuum:

- Outreach, intake and assessment
- Emergency shelter
- Transitional housing with supportive services
- Permanent & permanent supportive housing with services if needed

CoC's are responsible for managing and tracking the homeless systems of care in their community. One of the most important activities entrusted to CoC's is the biannual count of the homeless population and an annual enumeration of emergency systems, transitional housing units and beds that make up the homeless assistance systems.

These counts provide an overview of the state of homelessness in a CoC and offer the information necessary to redirect services, funding and resources as necessary." Source

Which vendors provide HMIS software solutions?

- Bitfocus
- Wellsky
- Eccovia
- Bell Data Systems
- Social Solutions
- Adsystech

Source

To what extent are homeless service providers required to use HMIS?

"Service providers that receive Federal funding and some State funding [in California] are required to participate in local HMIS. Participation in HMIS is optional for other independent providers (often faith- and community-based organizations)." Source

"The HEARTH Act, enacted into law on May 20, 2009, requires that all communities have an HMIS with the capacity to collect unduplicated counts of individuals and families experiencing homelessness. Through their HMIS, a community should be able to collect information from projects serving homeless families and individuals to use as part of their needs analyses and to establish funding priorities. The Act also codifies into law certain data collection requirements integral to HMIS. With enactment of the HEARTH Act, HMIS participation became a statutory requirement for recipients and subrecipients of the Continuum of Care (CoC) Program and Emergency Solutions Grant (ESG) funds." Source

To what extent are software vendors that process sensitive data required to integrate with HMIS?

"Our [Social Solutions] software meets current HUD, Domestic Violence, HMIS, and Social Security Administration data management and security protocols, as well as the minimum required FERPA and HIPAA standards." Source

"Our [Social Solutions] software systems are certified SOC 2 Type II and HIPAA compliant. Data is automatically encrypted while in transit between your computer and our servers — and while at rest." Source

How does the HMIS work? What is an example?

Source

Source

Is it possible to upload documents to the HMIS?

Yes. For example, documents can be attached to a participant or a program. Source

What is the California Consumer Privacy Act?

"The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

In November of 2020, California voters approved Proposition 24, the CPRA, which amended the CCPA and added new additional privacy protections that began on January 1, 2023. As of January 1, 2023, consumers have new rights in addition to those above, such as:

- The right to correct inaccurate personal information that a business has about them; and
- The right to limit the use and disclosure of sensitive personal information collected about them.

Businesses that are subject to the CCPA have several responsibilities, including responding to consumer requests to exercise these rights and giving consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers.

CPRA amends the CCPA; it does not create a separate, new law. As a result, our office typically refers to the law as “CCPA” or “CCPA, as amended.”” Source

What organizations does the CCPA apply to?

“The CCPA applies to for-profit businesses that do business in California and meet any of the following:

- Have a gross annual revenue of over $25 million;
- Buy, sell, or share the personal information of 100,000 or more California residents, households, or devices; or
- Derive 50% or more of their annual revenue from selling California residents’ personal information.

The CCPA generally does not apply to nonprofit organizations or government agencies.” Source

What is General Data Protection Regulation (GDPR)? What organizations does GDPR apply to?

“The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018.” Source

What is the Health Insurance Portability and Accountability Act (HIPAA)?

“The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.” Source

The Privacy Rule standards address the use and disclosure of individuals’ health information (known as *protected health information* or *PHI*) by entities subject to the Privacy Rule. These individuals and organizations are called “covered entities.”

“The Privacy Rule also contains standards for individuals’ rights to understand and control how their health information is used. A major goal of the Privacy Rule is to make sure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high-quality healthcare, and to protect the public’s health and well-being. The Privacy Rule permits important uses of information while protecting the privacy of people who seek care and healing.” Source

What organizations are considered covered entities under HIPAA?

- *“Healthcare providers*: Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include:
    - Claims
    - Benefit eligibility inquiries
    - Referral authorization requests
    - Other transactions for which HHS has established standards under the HIPAA Transactions Rule.

  Health plans:
  Health plans include:
    - Health, dental, vision, and prescription drug insurers
    - Health maintenance organizations (HMOs)
    - Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers
    - Long-term care insurers (excluding nursing home fixed-indemnity policies)
    - Employer-sponsored group health plans
    - Government- and church-sponsored health plans
    - Multi-employer health plans

Exception: A group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity.

- *Healthcare clearinghouses:* Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are

providing these processing services to a health plan or healthcare provider as a business associate.

- *Business associates: A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity.*These functions, activities, or services include:
    - Claims processing
    - Data analysis
    - Utilization review
    - Billing"

Source

Is a Continuum of Care a covered entity under HIPAA?

"A CoC is not a covered entity under HIPAA and most of the information that is in HMIS is not PHI. However, in some cases, organizations that are contributing data to an HMIS are covered entities, such as some mental health and behavioral health agencies, and they must comply with HIPAA in their participation in HMIS and any data sharing efforts. HIPAA allows for broad data sharing as long as appropriate protections are in place." Source

Is data on homeless services considered protected health information (PHI)?

"Data on homeless services, while protected, is generally not considered "protected health information" (or PHI), especially if the service provider is not also a health care provider, and therefore is not covered under HIPAA." Source

What is Service Organization Control Type 2 (SOC-2)?

"SOC 2, aka Service Organization Control Type 2, is a cybersecurity compliance framework developed by the American Institute of Certified Public Accountants (AICPA). The primary purpose of SOC 2 is to ensure that third-party service providers store and process client data in a secure manner. The framework specifies criteria to uphold high standards of data security, based on five trust service principles:

security, privacy, availability, confidentiality, and processing integrity." Source

What are the principles of SOC-2?

"Security. Broadly speaking, the security principle enforces the protection of data and systems, against unauthorized access. To that end, you may need to implement some form of access control, e.g. using access control lists or identity management systems.

You may also have to strengthen your firewalls, by introducing stricter outbound and incoming rules, introduce intrusion detection and recovery systems, and enforce multi-factor authentication.

Confidentiality. Data qualifies as confidential if only a specific group of people should access it. This may include application source code, usernames and passwords, credit card information, or business plans, etc.

To adhere to this principle, confidential data must be encrypted, both at rest and during transit. Moreover, while providing access to confidential data, adhere to the principle of leastprivilege, i.e. grant the bare-minimum permissions/rights that people need to do their jobs.

Availability. Systems should meet availability SLAs at all times. This requires building inherently fault-tolerant systems, which do not crumble under high load. It also requires organizations to invest in network monitoring systems and have disaster recovery plans in place.

Privacy. The collection, storage, processing, and disclosure of any personally identifiable information (PII) must adhere to the organization's data usage and privacy policy, along with the conditions

defined by the AICPA, in the Generally Accepted Privacy Principles (GAPP).

PII is any information that can be used to uniquely identify an individual, e.g. name, age, phone number, credit card information, or social security number etc. An organization must enforce rigorous controls to protect PII from unauthorized access.

Processing integrity. All systems must always function as per design, devoid of any delays, vulnerabilities, errors, or bugs. Quality assurance and performance monitoring applications and procedures are crucial to achieve adherence to this principle." Source

Is SOC-2 a legal requirement?

"One of the compliance standards that has emerged in an effort to ensure data is being protected are Service Organization Control 2, or SOC 2 reports. While SOC 2 standards aren't part of a law or regulation, they are equally as important to your business if you're handling customer data." Source

"While SOC 2 isn't monitored by a government agency and doesn't incur hefty fines for violations, achieving compliance is still a vital process for SaaS companies and cloud vendors. There may not be the danger of fines for violations, but there's definitely the danger of losing business if you can't prove you're on the path towards compliance with SOC 2." Source