National Human Services Data Consortium

2017 Spring Conference

Salt Lake City, UT

April 26-27, 2017

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase

Mary McGrail, HomeBase

Putting It All Together:
Uniting Data, Technology, and People

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Introduction

- Matt Olsson (Staff Attorney, HomeBase)
- Mary McGrail (Policy Analyst, HomeBase)

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Learning Objectives

- Understand the basic regulatory framework governing the handling of client-level data in HMIS and related human services systems, including the basic elements of privacy regulations covering:
  - Healthcare
  - Substance Abuse Treatment
  - Domestic Violence
  - Education

- Understand how these laws and regulations effect our day-to-day efforts to end homelessness

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Getting to Know You

- **Basic Information**:
  - Who are you?
  - Where are you from?
  - What's your role within your CoC?

- **Privacy Law**:
  - How has privacy law impacted your work?
  - What obstacles have you faced and how have you overcome these obstacles?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Legal Disclaimer

The information conveyed in this presentation and discussion is for **information purposes only**. It is neither legal advice nor a substitute for the advice of an attorney licensed in your state.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

The Basics

Fundamental Data Privacy Concepts

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Why Privacy Matters

- **Trust:** Our data is often self-reported information of a highly personal and sensitive nature. Trust is essential to successfully engage clients and gather accurate and complete responses.
- **Vulnerability:** Our clients are particularly susceptible to abuse and access to client information often raises legitimate safety concerns.
- **Collaboration:** Effective privacy controls can facilitate the exchange of information across mainstream systems.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining "Privacy"

"Privacy" encompasses the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

The American Institute of Certified Public Accountants

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Information Lifecycle

Legal Disclaimer: The information conveyed in this presentation is for informational purposes only. It is neither legal advice nor a substitute for the advice of an attorney licensed in your State.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining "Personal Information"

Personal information is **any** information related to an **identified or identifiable** person.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Types of Personal Information

- **General Personal Information**:
  - Name
  - Date of Birth/Age
  - Citizenship
  - Veteran Status
  - Disability Status
  - Contact Information (Address, Phone Number, Email Address, etc.)

- **Sensitive Personal Information**:
  - Social Security Number
  - Driver's License Number
  - Medical Records (including Mental Health and Substance Abuse)
  - Educational Records
  - Financial Information

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

General Principles

- Notice and Consent
- Accuracy and Completeness
- Information Security
- System Administration

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Notice and Consent

- Also referred to as **Release of Information ("ROI")**
- **Notice**:
  - Description of how personal information is collected, stored, used, and shared
- **Consent**:
  - Client's agreement to the use of his or her personal data

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Notice and Consent Drafting Tips

- **Plain English:** Client releases should minimize jargon and clearly explain both how and why personal information is collected, stored, used, and shared.
- **Demonstrate Value:** Outline the benefits of participation, as well as the consequences of non-participation.
- **Lay the Foundation for Collaboration:** Collaborate with other systems of care to develop a common framework for sharing and collaboration.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Accuracy and Completeness

- **Up to the Task:** Personal information should be relevant and timely for the purpose defined in the notice.
- **Access and Verification:** The ability for the subject to review and verify personal information, upon verification of identity.
- **Means to Update:** Policies supporting the ability of participating clients and programs to update and correct personal information where appropriate.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

System Administration Tips

- **Written Policies and Procedures:** System policies and procedures should include clearly documented and defined privacy policies and procedures, including the roles and responsibilities of personnel.
- **Maintain an Archive:** A well-organized archive of past policies, documents, and communications help maintain compliance in an evolving privacy landscape.
- **Provide Support:** Ensure that each user has access to the support and training resources necessary to understand the privacy component of their job.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Information Lifecycle

Legal Disclaimer: The information conveyed in this presentation is for informational purposes only. It is neither legal advice nor a substitute for the advice of an attorney licensed in your State.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Information Security (More Later…)

- **Confidentiality:** Access should be granted on a "need to know" basis.
- **Integrity:** Controls should be in place to ensure the accuracy of all information.
- **Availability:** Information should be available when and were it is needed.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Major Laws

An Overview of the Major Federal Privacy Laws

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

A Few Misconceptions

Generall, privacy laws…

- **"…prevent the sharing of data across systems of care":** Privacy laws establish a framework for the sharing and integration of homeless data across systems of care.
- **"…only apply to healthcare data":** Privacy law is about more than just HIPAA. HMIS and other system administrators should be mindful of privacy laws and regulations even if they only store basic client data.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

HMIS Data

HMIS-Specific Privacy Guidance and Regulation

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

HMIS-Specific Privacy Guidance

- **HMIS Proposed Rule:** The HMIS Proposed Rule sets forth basic requirements around the privacy and security of client-level data and HMIS.
- **HMIS Privacy and Security Notice:** HUD is in the process of finalizing a draft of the HMIS Privacy and Security Notice that should be released later this year for public comment.
- **2004 Data and Technical Standards Notice:** In the meantime, communities are expected to continue using the 2004 Data and Technical Standards Notice to implement their HMIS.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

2004 Data and Technical Standards Notice

- **Purpose:** Seeks to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited use and disclosure of data.
- **Basis:** Based on the principles of fair information practices and security standards recognized by information privacy and security communities.
- **HIPAA Influence:** Developed after careful review of the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

HUD's Standard: Protected Personal Info

Definition: Any information that is maintained by an organization contributing data to HMIS about a living person that:

- Identifies, either directly or indirectly, a specific person; or,
- Can be manipulated to identify a specific person; or,
- Can be linked together with other available information to identify a specific person.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

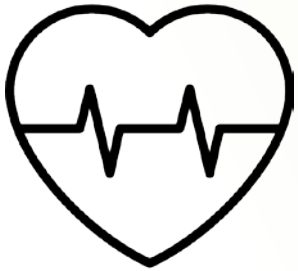
Healthcare Data

The Health Insurance Portability and Accountability Act

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

HIPAA-Covered Entities



- Healthcare Providers
- Insurers
- Healthcare Information Clearinghouses
- Business Associates

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining “Health Information”

“Any information” that (1) “is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school, university, or healthcare clearinghouse” and (2) relates to the physical or mental health condition of a client or the provision of care to that client.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining "Protected Health Information"

- **Protected Health Information (PHI):** Any health information that is explicitly linked to an individual or which can reasonably identify a person when combined with other data elements.

- **Electronic Protected Health Information (ePHI):** Protected health information that is stored or transmitted electronically.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Privacy Rule

- **Notice:** Must provide the client with a detailed privacy notice at the time of first service delivery.

- **Consent/Authorization:** Client requirements depend on how the protected health information is utilized:
  - **Treatment, Payment, Operations, and Compliance:** Authorized by HIPAA.
  - **Other Uses:** Opt-in authorization required.

- **Minimal Use:** Outside of treatment, a reasonable effort must be made to limit the use and disclosure of protected health information to the minimum amount necessary.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

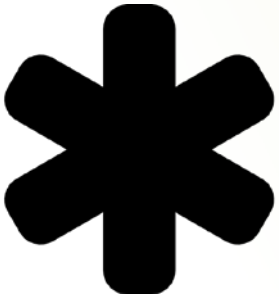
Privacy Rule (Continued)

- **Access/Disclosure:** Clients have the right to access a copy of protected health information and receive an accounting of certain disclosures.
- **Reasonable Safeguards:** Administrative, physical, and technical safeguards to reasonably protect the confidentiality and integrity of protected health information.
- **Accountability:** Covered entities must designate a Privacy Officer responsible for developing and implementing compliant privacy policies and procedures.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Exceptions to the Privacy Rule



- De-identification
- Research
- Required by law

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

De-Identification

There are two methods to de-identify protected health information:

- **Safe Harbor:** PHI is considered de facto de-identified if 17 specific data elements are removed from the client record, including: (a) names; (b) geographic subdivisions smaller than a state; (c) dates; (d) telephone numbers; (e) fax numbers; (f) email addresses; (g) social security numbers; (h) medical record numbers; (i) full-face photographs; (j) biometric identifiers; (k) health plan beneficiary numbers; (l) vehicle identifiers; (m) device identifiers; (n) URLs; (o) IP addresses, account numbers; (p) certificate/license numbers; or, (q) any other unique identifying number, characteristic, or code.

- **Expert Determination:** Certification by an expert that the "risk is very small that information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information."

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Research

Research using protected health information is acceptable provided that:

- The data used is **de-identified** using one of the processes outlined on the previous slide; or,
- Clients to whom the protected health information is related give their **consent**; or,
- The research is approved by an **Institutional Review Board**.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Security Rule

- **Requirements**:
  - Maintain the confidentiality, integrity, and availability of all protected health information.
  - Protect against reasonably anticipated threats.
  - Protect against reasonably anticipated uses and disclosures.
  - Ensure staff compliance.

- **Considerations**:
  - Size, complexity, and capability of the covered entity.
  - Cost and difficulty.
  - Probability and severity of potential harm.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining “Business Associates”

Any individual or organization that performs services or activities involving the use or disclosure of protected health information for a HIPAA-covered entity.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Applicability to Business Associates

- **HIPAA Applies:** HIPAA privacy and security rules apply directly to Business Associates through the Health Information Technology for Economic and Clinical Health (HITECH) Act.

- **Business Associate Agreements:** Covered entities must sign a written agreement with any Business Associates passing privacy and security requirements down to the contracting party.

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Enforcement

- **Serious Consequences:** Some HIPAA infractions carry criminal penalties.
- **Civil Enforcement:** The US Department of Health and Human Services enforces HIPAA regulations directly. State Attorneys General are also granted enforcement powers through the HITECH Act.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Drug and Alcohol Abuse Treatment and Prevention Records

42 CFR Part 2

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

42 CFR Part 2

- **Description:** The primary federal regulations governing the confidentiality of drug and alcohol abuse treatment and prevention records.

- **Purpose:** Sets forth the limited circumstances in which substance abuse patient information may be used or disclosed, and no uses or disclosures other than those detailed in the regulations are permitted.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Covered Entities

42 CFR Part 2 is only applicable to federally-assisted programs that hold themselves out as providing – and actually do provide – drug or alcohol abuse treatment, diagnosis, or referral for treatment.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Federal Assistance

Only federally-assisted programs are subject to Part 2, though the definition is broad and includes programs that are:

- Authorized, certified, licensed, or registered by the Federal government;
- Receiving Federal funding in any form, including sources that do not directly subsidize substance abuse services;
- Granted tax-exempt status by the IRS;
- Allowed tax reductions by the IRS for contributions;
- Authorized to conduct business by the Federal government, including programs:
  - Certified as a Medicare provider;
  - Authorized to conduct methadone maintenance treatment; or,
  - Registered with the Drug Enforcement Administration;
- Conducted directly by the Federal government.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining "Providing Substance Abuse Services"

The program must do both of the following in order to be covered by Part 2:

- **Hold Themselves Out:** The program must hold itself out as a provider of drug or alcohol abuse treatment or prevention services; and,
- **Actual Provision:** Actually provide drug or alcohol abuse treatment or prevention services.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Disclosure (Generally)

Generally, **written patient consent** is required to disclose the patient's records. The consent must contain:

- Name/general description of the program/person making the disclosure;
- Name/title of the individual/organization to whom the disclosure will be made;
- Intended purpose of the disclosure;
- Patient's name;
- How much and what kind of information is to be disclosed;
- Statement that consent may be revoked at any time (except to the extent that it has already been relied upon);
- The date the consent is signed;
- The patient's signature; and,
- The date, event, or condition when the consent will expire if not previously revoked (consent may last no longer than necessary).

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Allowable Disclosures (Exceptions)

Programs may disclose or use drug or alcohol abuse patient information without written consent:

- In the course of internal program communications;
- In a communication with a Qualified Service Organization (an outside organization that provides services to the program);
- In medical emergencies;
- In response to a crime against program staff or on program premises (or threats);
- For research activities;
- For audit and evaluation purposes;
- To report suspected child abuse or neglect;
- In circumstances involving certain minors or incompetent parents; or,
- In response to a valid court order.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

A Note of Caution

The first major revision of Part 2 since 1987 is currently underway. Public comment closed in April of 2016 and a new final rule is expected. The **Proposed Rule** includes changes touching upon:

- Consent requirements for Health Information Exchanges;
- Inclusion of population health activities among the scope of activities that can be conducted by Qualified Service Organizations;
- Clarification that Part 2 does not apply to general medical practices; and,
- Prohibition of re-disclosure only applies to information that would identify (directly or indirectly) an individual as having been diagnosed, treated, or referred for treatment for a substance abuse disorder.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Education Data

Major Privacy Laws Governing Education Data

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Two Key Laws

- **Family Educational Rights and Privacy Act of 1974 (FERPA):**
  - Sometimes called the "Buckley Amendment".
  - Protects the privacy of student educational records.
  - Applies to educational institutions that receive funding under US Department of Education programs.

- **Pupil Rights Amendment of the General Educational Provisions Act (PPRA):**
  - Sometimes called the "Hatch Amendment".
  - Governs the administration of certain types of surveys given to students.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Defining "Education Records" Under FERPA

- **Definition:** Records that directly relate to a student and that are maintained by an educational agency or institution, or by a party acting on behalf of an educational agency or institution.

- **Identifiable Information:** Any record that contains personally identifiable information that is directly related to the student is an educational record under FERPA.

- **Non-Education Records:** Campus police records, medical records, or statistical data compilations that contain no mention of personally identifiable information about any specific students are not considered "education records" under FERPA. Note that they may be covered by other privacy laws, however.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Two Types of Education Records

- **<u>Directory Information</u>:**
  - Written consent is advisable, but not required.
  - Parents and adult students have the right to limit disclosure (opt-out).
  - ”Directory information” includes: name, address, phone number, email address, dates of attendance, degree(s) awarded, enrollment status, and major fields of study.

- **<u>Non-Directory Information</u>:**
  - Written consent is required (opt-in).
  - “Non-directory information” includes: social security number, student identification number, race, ethnicity, nationality, gender, transcripts, and grades.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

What Data Can Schools Share with CoCs?

- **Aggregate Information:** Schools may disclose aggregate student information that does not include personally identifiable information for research and evaluation purposes.
- **Directory Information:** Directory information, as long as the parent or eligible adult student has not opted-out.
- **Homeless Statistics:** The number of students experiencing homelessness at the time of the PIT Count, including information about grade level, primary nighttime residence, race, and gender, so long as that data does not contain personally identifiable information.
- **De-Duplication Support:** Schools may view personally identifiable information to de-duplicate their count of homeless students, but may not disclose personally identifiable information to the CoC for de-duplication.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

PPRA Requirements

- **<u>Protected Areas</u>:** Survey subjects protected under PPRA include:
  - Mental or psychological problems of the student or the student's family;
  - Sexual behaviors or attitudes; and,
  - Illegal, anti-social, self-incriminating, or demeaning behaviors.

- **<u>Notification Requirements</u>:**
  - Direct notification of parents and/or adult students.
  - Provision of an opportunity to opt-out.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Criminal Justice Data

Privacy Provisions Related to Criminal Records and Disclosures to Law Enforcement

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Disclosures to Law Enforcement

- **Court Order Required:** There is no general exemption for disclosures to law enforcement and administrators may face liability for disclosures made without a valid court order or other lawful order.

- **Limited Exceptions:** Narrowly defined exceptions exist for extraordinary circumstances.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Records Maintained by Criminal Justice Agencies

- **Generally Public:** Criminal and civil court records are generally open and public.
- **Juvenile, Financial, and Medical Records:** May be subject to additional protections and/or redaction.
- **Potential for Abuse:** Be mindful of the potential for abuse and/or discrimination.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Other Laws

Other Privacy-Specific Laws

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

A Few Highlights…

- **State-Specific Laws:** Many states have additional laws which go above and beyond the Federal regulatory framework. Be sure to consult an attorney licensed in your state for more information.

- **Credit and Financial Information:** The Fair and Accurate Credit Transaction Act (FACTA) regulates organizations that collect credit information on consumers or employees.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Information Security

How to Protect Data Privacy

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Key Considerations

- **Confidentiality:** Access to protected data should only be granted on a "need to know" basis.
- **Integrity:** Controls should be in place to ensure the timeliness, completeness, and accuracy of all data.
- **Availability:** Information should be available when and where it is needed.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Determining the Need for Information Security

- **Threat/Risk Assessment:** What are your system's threats and vulnerabilities?
- **Obligations:** What are your contractual and regulatory obligations?
- **Goals:** What are your policies and objectives?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

So, There's Been a Breach

Data Breach, Incident Management, and Notification Laws

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Incident Management 101

- **Confirm:** Determine whether there was an actual breach of information security.
- **Contain:** Prevent further damage and determine what happened (and why).
- **Communicate:** Notify impacted parties of the breach.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators
Matt Olsson, HomeBase
Mary McGrail, HomeBase

Data Breach Notification Laws

- **(Almost) Every State:** Every state has enacted notification laws except for three holdouts (as of 2014): Alabama, New Mexico, and South Dakota.
- **Fines and/or Shame:** Notification laws incentivize effective information security by attaching financial and reputational harm to public disclosure.
- **High Standards May Minimize Liability:** Many states include exemptions for data protected by encryption or similar technology.

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Questions?

Demystifying Privacy Law: An Overview of Privacy Law for HMIS and Human Service System Administrators

Matt Olsson, HomeBase
Mary McGrail, HomeBase

Thank You

Should you have any questions in the future, please don't hesitate to contact us at:

- **Matt Olsson:**
  - matt@homebaseccc.org
  - (415) 788-7961 x314
- **Mary McGrail:**
  - mary@homebaseccc.org
  - (415) 788-7961 x307