Legal Issues Associated with Use and Release of HIV/HCV Personally Identifiable Information

Cason Schmit, J.D.
Research Assistant Professor
HIPAA Compliance Officer
Texas A&M School of Public Health

NASTAD Health Systems Data Consultation and Workshop

February 10, 2017
Disclaimer

The contents are for educational purposes only and are not intended as a substitute for professional legal advice.

Always seek the advice of an attorney or other qualified professional with any questions you may have regarding a legal matter.
Background

- HIPAA Privacy Officer
  Texas A&M University School of Public Health

- Former Public Health Analyst
  US Centers for Disease Control and Prevention,
  Office for State, Tribal, Local, and Territorial Support,
  Public Health Law Program

- Licensed Attorney (AZ)

- Certificate in Law, Science, and Technology with
  specialization in
  - Health Law
  - Intellectual Property
  - Genomics & Biotechnology Law
Overview

- Real v. perceived legal barriers to data
- Legal Framework
- Types of legal agreements relating to health data
- Tips for dealing with your legal counsel
Real v. Perceived Legal Barriers to Data
Real and Perceived Legal Barriers to Data Use and Release

- There are many “perceived” legal barriers to data use and release
  - Not all are actual legal prohibitions
- Three approaches to perceived barriers
  - Apply conservative data use policies
  - Identify legal solutions
  - Identify technological solutions

Require an understanding of underlying legal framework. Your attorney is your friend!
Example of Conservative Data Use Policies

- Conservative HIPAA policies in organizations
  - Total data lockdown
    - Assume all data is identifiable/HIPAA-protected
    - Share nothing
    - No secondary data uses permitted
    - Restricts _legal_ uses of data
Examples of Legal Solutions to Perceived Barriers

- **EHR Access difficulties during a fungal meningitis outbreak investigation**
  - Educate healthcare providers of legal protections and exceptions
  - Create data use and confidentiality agreements with healthcare providers
  - Share governance documents and policies and procedures
  - Enact new laws
    - “Access shall be given in the most efficient and expedient means possible, including remote electronic access, to facilitate investigations and inquiries while responding to an immediate threat to the public health, welfare, or general good.”
      - TENN. CODE ANN. § 63-1-117 (West)

Examples of Technological Solutions to Perceived Barriers

- **Distributed database querying**
  - Allows custodians to maintain custody of health data
  - Allows researchers to query distributed database network for aggregated results
  - No personally identifiable data is obtained

- **Differential privacy**
  - Adds random “noise” to datasets to limit re-identification of individuals
  - Maintains some aggregate query functionality
Legal Framework for Data Use and Release
State Law Variations Issues

HIV and HCV Data Protections
HIV Exceptionalism

- Stigma associated with HIV in the early years of the epidemic led to implementation of HIV specific laws in many states
  - HIV-related privacy and confidentiality laws
  - Criminalization of certain behaviors of persons with HIV
- Laws persist despite the dissipation of the motivating factors

In 2013, 43 states criminalize certain behaviors of HIV-positive individuals
http://legacy.lawatlas.org/query?dataset=hiv-criminalization-statutes
State Laws Relating to Health Department HIV PII
Dataset of Health Department Privacy Laws

- LawAtlas.org
  - Policy Surveillance Platform
  - Funded by RWJF
- Health Department (HD) privacy data set
  - Transparent legal research methods
  - Publically available data
State law includes a provision regulating the use of HIV/AIDS-related PII held by the health department (HD)
Use of HIV/AIDS-related PII held by HD: Public Health (2013)

- State law includes a provision regulating the use of HIV/AIDS-related PII held by HD
  - HD may use HIV/AIDS-related PII without patient consent for public health activities
Use of HIV/AIDS-related PII held by HD: Research (2013)

- State law includes a provision regulating the use of HIV/AIDS-related PII held by HD
  - HD may use HIV/AIDS-related PII without patient consent for research

[Map showing jurisdictions that meet criteria with a note: JURISDICTIONS FOUND: 3]
State law regulates the release of HIV/AIDS-related PII held by HD.

- State law regulates the release of HIV/AIDS-related PII held by HD
- HD may release HIV/AIDS-related PII without patient consent for public health activities
Release of HIV/AIDS-related PII held by HD: Research (2013)

- State law regulates the release of HIV/AIDS-related PII held by HD
- HD may release HIV/AIDS-related PII without patient consent for research
State Laws Relating to Health Department HCV PII
Laws regulating use of HCV-related PII held by HD (2013)

- State law includes a provision regulating the use of HCV-related PII held by HD
Laws regulating use of HCV-related PII held by HD: Public Health (2013)

- State law includes a provision regulating the use of HCV-related PII held by HD
  - HD may use HCV-related PII without patient consent for public health activities
Laws regulating use of HCV-related PII held by HD: Research (2013)

- State law includes a provision regulating the use of HCV-related PII held by HD
  - HD may use HCV-related PII without patient consent for research
State law includes a provision regulating the release of HCV-related PII held by HD.
State law includes a provision regulating the release of HCV-related PII held by HD. HD may release HCV-related PII without patient consent for public health activities.
State law includes a provision regulating the release of HCV-related PII held by HD.

- HD may release HCV-related PII without patient consent for research.
HIE Data Protections
CDC Assessment of State HIE Laws (2017)

- Governance
  - Oversight
  - Data ownership
  - Transparency

- Permitted uses of HIE
  - Payers
  - Public health
  - Research
  - More!

- Data protections
  - Privacy
  - Confidentiality
  - Security
  - Authorization

- Funding

- Interjurisdictional exchange

- Liability and immunity

More than 80 legal attributes
Statewide HIE Laws (2016)

- Laws authorizing implementation of a statewide HIE
  - Yes (30)
• State laws with express duties for providers or other HIE users to protect patient data from unauthorized accesses/disclosures

• Law provides heightened protections for sensitive health information

• Yes (8)
## HIE Laws with Protections for Sensitive Health Information

<table>
<thead>
<tr>
<th>State</th>
<th>Type of Sensitive Information</th>
<th>Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delaware</td>
<td>Newborn screening (metabolic, hematologic, endocrinologic, immunologic, structural disorders)</td>
<td>DE ST TI 16 § 1201; DE ST TI 16 § 806C</td>
</tr>
<tr>
<td>Illinois</td>
<td>HIV/AIDS; Genetic information</td>
<td>IL ST CH 410 § 305/2; IL ST CH 410 § 305/9.4, 9.4a, 9.6; IL ST CH 410 § 513/31.4 et seq.</td>
</tr>
<tr>
<td>Maine</td>
<td>HIV/AIDS; Psychotherapy notes</td>
<td>ME ST T. 34-B § 1207; ME ST T. 5 §§ 19203,19203-D</td>
</tr>
<tr>
<td>Maryland</td>
<td>Sensitive health information (e.g., mental and behavioral health)</td>
<td>MD ADC 10.25.18.03(A)(2)(b), 10.25.18.04</td>
</tr>
<tr>
<td>Nevada</td>
<td>Minors’ healthcare without parental consent.</td>
<td>NV ST 439.589(1)(b); NV ST 439.590</td>
</tr>
<tr>
<td>New York</td>
<td>Minor consent patient information (e.g., HIV tests, sexual assault, mental health).</td>
<td>10 NY ADC 300.5</td>
</tr>
<tr>
<td>Texas</td>
<td>Mental health and specific disease status information for which specific laws apply</td>
<td>TX HEALTH &amp; S § 182.104</td>
</tr>
<tr>
<td>West Virginia</td>
<td>HIV/AIDS; Substance abuse; Mental health; Out-of-pocket goods and services; Patient-restricted information; Other legally protected information</td>
<td>WV ST § 16-3C-3(a)(10), (b); WV ADC § 64-64-8; WV ADC § 65-28-2.45; WV ADC § 65-28-6.7; WV ADC § 65-28-7</td>
</tr>
</tbody>
</table>
• State laws specifying users and uses of HIE
  • Law authorizes state and local health authorities to access the HIE
    • Yes (31)
    • Ambiguous (1)
State laws specifying users and uses of HIE

Law authorizes research institutions to access HIE data through portal or user interface (excluding express consent requirements)

Yes (5)
No (1)
Ambiguous (2)
Federal Law Overview
Federal Law Overview

- **HIPAA**
  - Privacy (confidentiality) and security protections for identifiable health information

- **Privacy Act**
  - Protections for data held by federal agencies (CDC, CMS)

- **Common Rule (revised 1/18/2017)**
  - Protections for Human Subjects Research

- **42 CFR part 2 (revised 1/18/2017)**
  - Confidentiality of Substance Use Disorder Patient Records
Quick HIPAA Overview
HIPAA Diagram
A covered entity can only use or disclose protected health information for limited purposes unless the individual authorizes the use or disclosure:

- 45 C.F.R. § 164.502 et al.

What limited purposes?
- Disclosure to the individual
- Disclosures for treatment, payment, or health care operations
Basic HIPAA Privacy Rule Flow Chart

Covered Entity?  • HIPAA only applies to covered entities

Protected Health Information?  • HIPAA only protects identifiable information

Exceptions?  • Exceptions might still permit disclosure

Yes

No

HIPAA doesn’t apply

Yes  No

No  Yes
Who does HIPAA apply to?

- **Covered Entities**
  - Health care providers
  - Health plans
  - **Health care clearinghouse**
  - **Business associates**

- **Hybrid Entities**
  - Business activities include “covered” and “non-covered” functions
    - HIPAA only applies to the part that performs covered functions
## State Health Department HIPAA Status (2005)

<table>
<thead>
<tr>
<th>State</th>
<th>HIPAA Status</th>
<th>State</th>
<th>HIPAA Status</th>
<th>State</th>
<th>HIPAA Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>Hybrid</td>
<td>Louisiana</td>
<td>Covered</td>
<td>Ohio</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Alaska</td>
<td>Covered</td>
<td>Maine</td>
<td>Other</td>
<td>Oklahoma</td>
<td>Covered</td>
</tr>
<tr>
<td>Arizona</td>
<td>Hybrid</td>
<td>Maryland</td>
<td>Hybrid</td>
<td>Oregon</td>
<td>Covered</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Covered</td>
<td>Massachusetts</td>
<td>Hybrid</td>
<td>Pennsylvania</td>
<td>Hybrid</td>
</tr>
<tr>
<td>California</td>
<td>Covered</td>
<td>Michigan</td>
<td>Hybrid</td>
<td>Rhode Island</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Colorado</td>
<td>Other</td>
<td>Minnesota</td>
<td>Other</td>
<td>South Carolina</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Hybrid</td>
<td>Mississippi</td>
<td>Covered</td>
<td>South Dakota</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Delaware</td>
<td>Hybrid</td>
<td>Missouri</td>
<td>Hybrid</td>
<td>Tennessee</td>
<td>Covered</td>
</tr>
<tr>
<td>Florida</td>
<td>Hybrid</td>
<td>Montana</td>
<td>Covered</td>
<td>Texas</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Georgia</td>
<td>Covered</td>
<td>Nebraska</td>
<td>Covered</td>
<td>Utah</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Hawaii</td>
<td>Hybrid</td>
<td>Nevada</td>
<td>Hybrid</td>
<td>Vermont</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Idaho</td>
<td>Hybrid</td>
<td>New Hampshire</td>
<td>Covered</td>
<td>Virginia</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Illinois</td>
<td>Hybrid</td>
<td>New Jersey</td>
<td>Hybrid</td>
<td>Washington</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Indiana</td>
<td>Hybrid</td>
<td>New Mexico</td>
<td>Covered</td>
<td>Wisconsin</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Iowa</td>
<td>Other</td>
<td>New York</td>
<td>Hybrid</td>
<td>West Virginia</td>
<td>Hybrid</td>
</tr>
<tr>
<td>Kansas</td>
<td>Hybrid</td>
<td>North Carolina</td>
<td>Hybrid</td>
<td>Wyoming</td>
<td>Covered</td>
</tr>
<tr>
<td>Kentucky</td>
<td>Hybrid</td>
<td>North Dakota</td>
<td>Hybrid</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Basic HIPAA Privacy Rule Flow Chart

Covered Entity?
- HIPAA only applies to covered entities

Protected Health Information?
- HIPAA only protects identifiable information

Exceptions?
- Exceptions might still permit disclosure

Yes

No

Yes

No

HIPAA doesn’t apply
What does HIPAA protect?

- Individually identifiable health information
  - Is created or received by a covered entity; and
  - Relates to the health of an individual; and
    - Identifies the individual; or
    - Reasonable to believe information can be used to identify the individual.

- Protected health information
  - Individually identifiable health information that is transmitted or maintained in any form or medium
    - Some exclusions apply
De-identification Methods

- Why de-identify?
  - Information that is not identifiable is not HIPAA protected

- Methods
  - Statistical De-identification (Expert Opinion)
    - Re-identification risk is "very small"
    - Might depend on anticipated recipient
  - "Safe Harbor" De-identification
    - Exclude list of 18 identifiers
    - No actual knowledge

- Aggregate data
  - Usually not individually identifiable

Basic HIPAA Privacy Rule Flow Chart

Covered Entity?
- HIPAA only applies to covered entities

Protected Health Information?
- HIPAA only protects identifiable information

Exceptions?
- Exceptions might still permit disclosure

Yes

No

HIPAA doesn’t apply

No
Yes
Important!

- Many HIPAA provisions allow the use and release of protected health information!!!
Important HIPAA Disclosure Exceptions

- No requirement for authorization or opportunity to object for:
  - Public health activities
    - PH authority authorized to collect information
      - i.e., state and local legal authorities
  - Other entities
  - Research
    - IRB or Privacy Board approval
      - IRB must follow Common Rule
  - Others
    - E.g., uses and disclosures required by law, for law enforcement activities, health oversight activities
Public Health Authorities with Covered Entity Status

- HIPAA not intended to apply to public health activities
  - So what about public health authorities that are covered entities?

- HIPAA rules are clear:
  - **If a public health authority is also a covered entity, it may use and disclose health information without patient authorization for public health activities.**
    - 45 C.F.R. § 164.512(b)(2)
Scope of HIPAA Disclosures

- Minimum Necessary
- Limited Data Set
When using or disclosing protected health information ... a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

- Some exclusions apply

- This is the standard for many HIPAA disclosures!
Limited Data Set Disclosures

- A specific type of disclosure of PHI
  - Specific data elements are excluded (i.e., partially de-identified)
    - Limited data sets are still HIPAA protected
- Permitted uses for limited data set disclosures:
  - Research
  - Public health
  - Health care operations
- Requires a Data Use Agreement
Limited Dataset v. Minimum Necessary

- **Limited Data set Disclosure**
  - A specific type of disclosure
  - Specific data elements are excluded
  - Permitted uses:
    - Research
    - Public health
    - Health care operations
  - Requires a Data Use Agreement

- **Minimum Necessary Standard**
  - Standard for many permitted HIPAA disclosures
  - Get what you need
    - Including data elements that would be excluded from a Limited Dataset disclosure
  - Reasonable effort
    - Covered entity may rely (if reasonable) on PH official’s representations
Types of Legal Agreements Relating to Health Data
Types of Legal Agreements

- Contract
- Memorandum of Understanding (MOU)
- Data Use Agreement (DUA)
  - “Standard”
  - HIPAA limited data set DUA
- Business Associate Agreement (BAA)
Contracts

- A legally binding and enforceable agreement
- Created when three elements are present
  1. Offer
  2. Acceptance
  3. Consideration
     - Promise to do something you legally do not have to do, or
     - Promise not to do something you legally can do
- The label a party assigns the agreement (DUA, MOU, BAA, etc) is not legally relevant to determinations of contract existence.
OUR LAWYER SENT OVER A SIXTY-PAGE CONTRACT RENEWAL THAT I NEED YOU TO REVIEW.

MAKE SURE YOU COMPARE IT TO THE ORIGINAL CONTRACT AND ALL SIX OR SEVEN AMENDMENTS.

ARE THERE SIX OR SEVEN?

NO ONE REALLY KNOWS.

CHECK OUT OUR OTHER NINE HUNDRED CONTRACTS TO MAKE SURE THIS ONE DOESN'T VIOLATE ANY OF THOSE.
Memorandum of Understanding (MOU)

- Intended to be less formal instrument
  - BUT still could be a binding contract if the 3 elements are present
- Purpose:
  - Reduce misunderstandings between parties
  - Outline the bounds and terms of arrangement
- Common for use among government entities
Data Use Agreements (DUA)

- Formal written agreements between two or more parties
  - Can be a binding contract if the 3 elements are present
- Tools to
  - Constrain use of data after it has been disclosed
  - Constrain additional disclosure
  - Ensure rights and obligations are maintained
    - Parties (e.g., CDC, HDs, healthcare providers)
    - Stakeholders (e.g., patients)
When should you consider a DUA?

- Whenever you want to disclose data, and
  - You are concerned about the future use and disclosure of your data
  - You are required by law to enter a DUA to disclose the data
    - E.g., A limited data set disclosure under HIPAA

- DUA’s are not required for every disclosure
  - E.g., Public health disclosures for outbreak response
    - Unnecessary DUA negotiations may delay necessary response
HIPAA Limited Data Set DUA

- A type of DUA required for a Covered Entity to disclose a limited data set
  - Limited data sets are protected health information under HIPAA
- HIPAA requires specific terms to be included for the disclosure to be compliant
Contents of a HIPAA Limited Data Set DUA

- Establish
  - Permitted uses and disclosures of the data
  - Who is permitted to use or receive the data

- Provide that data recipient will
  - Not use or disclose data other than permitted by DUA or required by law
  - Use appropriate safeguards
  - Report unauthorized disclosures
  - Ensure any agents to whom the recipient provides the data agree to the same restrictions and conditions
  - Not identify the information or contact the individuals

45 C.F.R. § 164.514(e)(4)(ii)
(4) Payers, Providers, Provider Organizations and Researchers shall enter into a Data Use Agreement with CHIA prior to the receipt of Data. The Data Use Agreement shall, at a minimum:

   (a) restrict the use of the Data to those uses identified in the application;
   (b) require the Data Recipient to adhere to processes and procedures aimed at preventing unauthorized disclosure or use of the Data;
   (c) require the Data Recipient to notify CHIA of any unauthorized use or disclosure of the Data; and
   (d) permit CHIA, at its discretion, to audit the Data Recipient's compliance with the provisions of the Data Use Agreement.

957 Mass. Code Regs. 5.04
Business Associate Agreements (BAA)

- Written agreements between HIPAA covered entities and other persons/organizations that provide services on behalf of covered entities requiring the disclosure of protected health information
- If a Business Associate relationship exists, a BAA is required by HIPAA
- BAAs have HIPAA required terms
Business Associates

- Includes:
  - “A Health Information Organization, E–prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.”
  - 45 C.F.R. § 160.103
BAA Considerations

- Is a Business Associate relationship necessary?
- Business Associates can be held liable for HIPAA violations
- Business Associates have obligations to the individuals whose PHI they possess
- HIPAA requires specific BAA terms
HHS guidance clearly says disclosures of limited datasets for research do not create a BA relationship and do not require a BAA.
Tips for Dealing with your Attorney
“Of all the advice in this toolkit, among the most important is to meet early and often with your agency or department’s attorney”

- Public Health Informatics Institute, Toolkit for Planning an EHR-based Surveillance Program, [http://www.phii.org/ehrtoolkit/introduction](http://www.phii.org/ehrtoolkit/introduction)
Tips for Dealing with Your Attorney

- Your agency’s attorney serves two important roles for the agency:
  - (1) supporting it in achieving the public health mission within the confines of current law; and
  - (2) protecting it against conducting embarrassing or unlawful activity or implementing poorly formulated plans

- Public Health Informatics Institute, Toolkit for Planning an EHR-based Surveillance Program, [http://www.phii.org/ehrtoolkit/introduction](http://www.phii.org/ehrtoolkit/introduction)
Prepare Your Case!

- Do your research, but respect your attorney’s role
- Connect the overall goal of the new program to an agency or leadership priority to broaden the context in which to support your program’s creation.
- Prepare to discuss all the possible uses of the data internally and externally
  - Distinguish critical uses and bonus uses
- Ask others to learn how your agency attorney or legal unit responded to similar cases in the past.

Public Health Informatics Institute, Toolkit for Planning an EHR-based Surveillance Program, [http://www.phii.org/ehrtoolkit/introduction](http://www.phii.org/ehrtoolkit/introduction)
Acknowledgements

Public Health Law Program
Office for State, Tribal, Local and Territorial Support
U.S. Centers for Disease Control and Prevention

Gregory Sunshine, J.D.
Dawn Pepin, J.D., M.P.H.
Tara Ramanathan, J.D., M.P.H.
Akshara Menon, J.D., M.P.H.
Matthew Penn, J.D., M.L.I.S.
Sarah Wetter (J.D. Candidate 2017)
Questions?

Cason D. Schmit, J.D.

Schmit@sph.tamhsc.edu
HIE and Public Health