Key Legal Agreements for Data Sharing

Jennifer Bernstein, JD, MPH
Deputy Director, Network for Public Health Law
Mid-States Region

Public Health Law Summit, October 2, 2019
Overview

• Background
  • The role of an attorney in data sharing
  • Systematically analyzing a data sharing issue
  • Variations in law between jurisdictions

• Key documents for data sharing:
  • Memorandum of Understanding (MOU)
  • Data Use Agreement (DUA)
  • Business Associate Agreement (BAA)
  • User agreements and consent forms
  • Service Level Agreement (SLA)
So much data ....
Screening
» Childhood lead screening
» Newborn screening for metabolic diseases
» Early hearing detection & intervention
» Vision & hearing screening of school children

Health Plans
» Medicaid
» State Children’s Health Plan
» County Health Plans

WIC

Regulatory
» Restaurant inspection reports
» Septic, wells, other permits
» Clean indoor air act
» Burning ordinances
» Asbestos contractors
» Lead abatement contractors
» Health facilities
Vital Records
- Birth records
- Death records
- Marriage records

Registries
- Cancer
- Birth defects
- Traumatic injuries
- Immunizations

Disease Surveillance
- Infectious disease reports
- Syndromic surveillance
- Hospital acquired infections

Clinical Services
- Child & maternal health
- Immunization
- Dental clinics
- School-based clinics
- FQHCs or CHCs

Emergency Preparedness
- Health alert networks
- Volunteer registries
- Vulnerable people registries
And growing ....

- Amount of data
- Sources of data
- Data sharing partners
- Ways to transfer and exchange
- Linkages with other information
- Creation integrated databases
- Retention, reuse, and further sharing of the information
- Creation of public datasets
So many laws ....
# Data Protection and Disclosure Laws

+ frequent condition for receiving funds

<table>
<thead>
<tr>
<th>Federal</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HIPAA</td>
<td>• Health information</td>
</tr>
<tr>
<td>• FERPA</td>
<td>• Disease surveillance</td>
</tr>
<tr>
<td>• WIC</td>
<td>• Registries</td>
</tr>
<tr>
<td>• Title X family planning</td>
<td>• Vital records</td>
</tr>
<tr>
<td>• Cancer registries</td>
<td>• Screening</td>
</tr>
<tr>
<td>• Substance abuse treatment</td>
<td>• Drug monitoring</td>
</tr>
<tr>
<td>• Federally supported research</td>
<td>• Medicaid</td>
</tr>
<tr>
<td>• Social Security Act</td>
<td>• Clinical services</td>
</tr>
<tr>
<td></td>
<td>• Social security #</td>
</tr>
<tr>
<td></td>
<td>• Open records</td>
</tr>
</tbody>
</table>
Law governs every aspect of data.
When do you bring in the lawyers?

“If you want to squelch a good idea, have it reviewed by your attorney.”

Quote from presentation by a public health practitioner
How us lawyers think

» Duty: protect client

» Risk averse

» Law: fact-based and nuanced

» Requires interpretation

» Judgment calls
When should lawyers engage? 

DAY ONE
Benefits to starting on day one?

» Proactively build relationships

» Expanding our horizons

» Part of the team

» Effort justified by value
Cooperation: Getting to Yes!

» This is what we want to do . . .

» How do we best do it?
  - Pathways to yes
  - Detour when needed
  - Minimizing risk

» Judgment calls (lawyer should expect discomfort)
What do you need to know before you get started?
Getting to Yes!

» Start with factual information

» Network Tool: Checklist of Information Needed to Address Proposed Data Collection, Access and Sharing
How do you analyze a data sharing issue?

One bite at a time
Analyzing a data sharing issue

1. Establish facts
2. Identify law
3. Apply law
4. Establish & document terms for sharing
Establish facts: The **WHAT**

» **What public health threat?**

- What do you want to address
- Models and tools to assess community needs and resources, define priorities, develop plans

  e.g. Accountable Communities for Health Data-sharing Toolkit (Berkley Center for Healthcare Organizational Innovation Research)
Establish facts: The **WHAT**

» **What data?**
- Type; Data elements
  - Minimum necessary?
- From whom was it obtained (source of data)?
- For what purpose was it obtained?
- To whom is it to be disclosed?
- For what purpose is it to be disclosed?
  - Secondary use ≠ second class
- How will it be disclosed?
Map it!
Every transfer point for data is a decision point with regard to law

State Cancer Registry Data
- Patient
  - Health care provider

State Central Cancer Registry
  - Identifiable employment data
  - De-identified combined data

Occupational exposure data
- Employer
  - Employment and environmental records

Researcher

Linking tool
Establish facts: The WHO

» **Public health leaders**
  
  • Public health special legal status - broad authority to collect data to prevent and control disease, protect public health, and promote wellness

» **Multiple sector public and private partners**

» **Health and non-health sectors**

» **Partners that explicitly address ”upstream” social determinants of health**
Establish Facts: The WHO

Documenting relationships

» Establish general terms of the relationship, secure commitment, e.g. partnership agreement, charter, or master data sharing agreement

» Enter a data sharing/use agreement for a specific project

» Reflect on-going initiative with master data sharing agreement – appendices to cover specific projects
Establish facts: The WHY

» Why are you sharing these data with these partners?
» Be specific
» Permissible and prohibited disclosures often depend on purpose
Analyzing a data sharing issue

Identify laws that apply to each

» Data type

» Data source

May include general and/or specific laws:

- Health information
- Public health data and reporting
- Medical records
- Data Practices
- Privacy
- Security
- Breach notification
- Open records

- Identity theft protection acts
- Patient rights
- Health professional or facility licensing, certification
- Insurance laws
- Consumer protection laws
- Health information exchange
- Social Security No. protection
Determining exchange authority

1. Establish facts
   -- Data
   -- Participants
   -- Flow

2. Identify law

3. Apply law

4. Establish & document terms for sharing
Apply law

» What does law allow?

» What prerequisites, conditions, limitations apply

Balance: Maximize benefits, minimize risks

» Data management and statistical controls to provide the most meaningful data possible while protecting privacy
General barriers to exchange

- State law applies – variation among states
- General vs. specific authority to exchange data
- Scope of sharing: prerequisites, conditions & limits
- Within a state – applicability of multiple laws, need to harmonize
- Variety and changing systems, manner of exchange, technological capability
- Growing complexity, multiple points of data transfer, HIE laws
Variation in Law Across Jurisdictions

All levels of government have the power to enact laws as well as different jurisdictions, such as federal, tribal, state and local governments. This allows for a great amount of variation in legal frameworks.
Navigating the law

**Concern:** Variations in law among jurisdictions

**Solutions:**
- Create exceptions in agreement to accommodate certain parties
- Meet legal requirements of most restrictive party’s law
- Change in law or regulation to accommodate sharing
- Have party with greatest authority act as a data clearinghouse
Data sharing – Establishing and documenting terms of sharing

» Sets out legal authority, terms for sharing, provides for monitoring and accountability for compliance with terms

» Different agreements for different circumstances

» Often require several agreements at once, such as a BAA, SLA and user agreement
What’s in a name?

» **Data sharing agreement (DSA)**

» **Data use agreement (DUA)**

A legally enforceable agreement that operationalizes the (electronic) sharing of data among different parties, including organizations and individuals, while protecting data rights including privacy and confidentiality rights.
What’s in a name?

» Memorandum of understanding (MOU)

A legally non-binding agreement between two or more parties that outlines terms, scope and details of a mutual understanding, noting each party's requirements, roles, and responsibilities. It often avoids a lengthy contract review process and is therefore easier to execute.
Interagency agreement

» An interagency agreement is a document, generally between government agencies and/or departments, that defines cooperative work between them

» It is subset of MOUs specifically between two or more government agencies

» May be easier to enter into than other types of agreements

» Also be subject to state legal requirements and limitations in statutes, regulations, or guidelines
DUA vs. MOU

» Memorandum of understanding expresses a convergence of will and understanding between parties, indicating an intended common line of action

» MOU most often is used in cases where parties do not intend to imply a legal commitment to each other, but do wish to engage in an agreement of principle
Establishing and documenting terms of sharing

» Data sharing agreements & MOUs can share similar terms and provisions

» Sets out legal authority, terms for sharing, provides for monitoring and accountability for compliance with terms
DUA/MOU elements

» **Parties**
  » Name all known parties
  » Provide for the ability to add additional parties after initial agreement is operational

» **Purpose**
  » Articulate the overall purpose of the data sharing collaboration
  » Articulate each particular use of the data

The purpose of this Agreement is to provide MDH with data specified in this Agreement related to recipients of Minnesota Health Care Programs (MHCP) as necessary for communicable disease surveillance, control, and prevention. This data includes information on individuals that have been diagnosed with, or exposed to, communicable diseases reportable to MDH, as well as data on immunizations provided to MHCP recipients. Additionally, DHS needs access to the MDH Minnesota Immunization Information Connection (MIIC) system for the purpose of assessing immunization coverage levels for MHCP enrollees, and for quality assurance and quality improvement initiatives.
## DUA/MOU elements

### Legal Authority

- **General authority**
- **Specific authority**

<table>
<thead>
<tr>
<th>Citation</th>
<th>Description and detail regarding legal authority to collect, use and share the data, including limitations on use or disclosure of the data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minn. Stat. 144.05, subdivision 1</td>
<td>The state commissioner of health has general authority under Minnesota Statutes, section 144.05 to conduct studies and investigations, collect and analyze health and vital data, and identify and describe health problems.</td>
</tr>
</tbody>
</table>
| Minn. Stat. 144.211-144.227 | Section 144.213 within the Vital Statistics Act establishes the Office of Vital Records with the authority to promulgate rules (Minn. R. 4601) for the collection, filing and registering of vital records information and to maintain a statewide system of vital records. Section 144.225 specifies disclosure of information from vital records. Vital records data are public with the following exceptions:  
  - 144.225, subd. 2: Demographic data on birth records is confidential data if a mother was not married to the child’s father when the child was conceived nor when the child was born, unless the mother authorizes this data to be public.  
  - 144.225, subd. 2a: Health data (information from which an identification of risk for disease, disability, or developmental delay in a mother or child can be made) collected in conjunction with birth registration or fetal death reporting is classified as private data.  
  - 144.225, subd. 6: The named identity of a group purchaser collected in association with birth registration is nonpublic data. Notwithstanding data classified as confidential, private, or nonpublic, the data may be released to the individuals and entities specified within section 144.225. |
| Minn. R. 4601 | Minnesota Statutes, section 13.05, subpart 5 requires a responsible authority to “establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure.” Work assignments of individuals in the MIIC Operations Unit reasonably require access to not public birth record data and this IDUA describes how that data will be made available. |
DUA/MOU elements

» **Communications**
  » Publication and dissemination of results
  » Public disclosure of data, de-identification requirements
  » Communication standards between parties to the agreement

» **Definitions**
  » Any entities or elements that are unique to this data collaboration or require a definition for shared understanding
  » Terms used within the agreement that might not have a shared meaning or understanding across sectors
  » Naming conventions and standards for data elements
DUA/MOU elements

1. DEFINITIONS

“Agreement” means this Agreement.

“CDC” means the Centers for Disease Control and Prevention.

“De-identified immunization data” means any immunization data that does not identify nor provide a reasonable or ready basis to identify an individual.

“IIS Immunization Data” means demographics and immunization status of individual persons collected by IIS regardless of whether in the form of raw data or appearing in other IIS features and functions as described in Paragraph 7. Once an immunization record is entered into IIS, the record stored in the IIS database is IIS Immunization Data.

“IIS patient record” means the IIS Immunization Data for an individual.

“Immunization record” means any record regardless of source documenting the status of individual persons.

“Party” or “Parties” means either or both DOH and Provider/Plan.

“Provider-verified immunization record” means a valid record produced or verified by a health care professional or facility documenting the immunization status of an individual. To be valid, the record must be in writing, dated, and indicate the name of the health care provider responsible for administering or reviewing each immunization, or a unique stamp of the provider or facility at which the provider practices.
DUA/MOU elements

» Data to be provided + description of data
  » Elements
  » Data provider, data recipient
  » Frequency
  » Format
  » Method of exchange

9. Information to be provided. Each party will provide the IIS core data elements, incorporated by the CDC in its IIS Functional Standards, 2013-2017, provided: (1) the sending party collects and has the capability to provide the core data element, and is permitted by its law to share the core data element and (2) the receiving party has the capability and capacity to receive the core data element. Appendix A identifies core data elements that each party is able to provide to and/or receive from other parties. Any party may agree to provide or receive additional data elements, to further the purpose of this MOU, as set out in Appendix A.
## Appendix A

In the table below, each party to this MOU identifies IIS core data elements and any additional data elements that it is able to provide to other parties and receive from other parties. Unless indicated otherwise, the IIS core data elements below are identical to CDC's list at [http://www.cdc.gov/vaccines/programs/iis/func-stds.html - appB](http://www.cdc.gov/vaccines/programs/iis/func-stds.html - appB), as accessed May 20, 2015.

<table>
<thead>
<tr>
<th>Core Data Element</th>
<th>Maryland</th>
<th>Jurisdiction B</th>
<th>Jurisdiction C</th>
<th>Jurisdiction D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient ID (previously listed as &quot;Medicaid Number&quot;)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient ID: Assigning Authority ID (i.e., owning source)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient ID: Type (e.g., medical record number, IIS ID)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Name: First</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Name: Middle</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Name: Last</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Alias Name: First</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Alias Name: Middle</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Alias Name: Last</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Date of Birth</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Gender</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Multiple Birth Indicator</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Birth Order</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Responsible Person Name: First</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Responsible Person Name: Middle</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Responsible Person Name: Last</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Responsible Person Name: Relationship to Patient</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Mother's Name: First</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Mother's Name: Middle</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Mother's Name: Last</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: Street</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: City</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: State</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: Country</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: Zipcode</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Patient Address: County of Residence</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Race</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Ethnicity</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Recommended</td>
</tr>
<tr>
<td>Birth Facility Name</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Patient Birth State</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Patient Primary Language</td>
<td>✓ if available</td>
<td></td>
<td></td>
<td>Optional</td>
</tr>
</tbody>
</table>
DUA/MOU elements

» Privacy and security requirements
  » Custodial responsibility and data stewardship practices
  » Roles and responsibilities of the parties to agreement
  » Permissible use, linking, sharing and disclosure
  » Governing law – HIPAA, FERPA, 42 CFR Part 2, state law
  » Policies and procedures for reporting data breaches or unauthorized disclosures
6.2 **DUTIES RELATING TO PROTECTION OF INFORMATION.**

(a) **General Oversight Responsibilities.** Each Agency shall be responsible for ensuring proper handling and safeguarding by its employees, subcontractors, and authorized agents of Protected Information collected, created, used, maintained, or disclosed. This responsibility includes:

(b) **Training:** Ensuring that employees and agents comply with and are properly trained regarding, as applicable, the laws listed above, and

(c) **Duty to ensure proper handling of information.** Each Agency shall ensure proper handling and safeguarding of Protected Information by its employees, subcontractors, and authorized agents. This includes ensuring employees and agents comply with and are properly trained regarding, as applicable, the laws listed above in paragraph 6.1.

(d) **Minimum necessary access to information.** The collection, creation, use, maintenance, and disclosure of Protected Information shall be limited to only those individuals employed by each agency, or those employed by the subcontractors or agents of each agency, whose work assignments reasonably require access to the Protected Information, entities or individuals who are authorized by statute to gain access to the Protected Information, and entities and individuals given access by the express written direction or permission of both agencies.

(e) **Information Requests.** Unless provided for otherwise in this Agreement, if either agency receives a request to release any Protected Information, the other agency must be immediately notified. The Agency whose data is requested will consult with the other Agency’s Authorized Representative as to how to respond to the request. The response to the request shall comply with applicable law.
DUA/MOU elements

» Disposition of data

WA DOH and OR DHS agree to destroy all confidential information obtained under this agreement once the purposes of the project have been accomplished. Information which cannot be destroyed or of which destruction is not feasible shall be maintained in a secure environment. WA DOH and OR DHS agree to include compliance with these requirements as a requirement for contractors. Retention is pursuant to state archive laws that will dictate data disposal.

» Period of agreement

» Termination

11. TERMINATION.
   a. Either Party may terminate this Agreement effective as of the end of any calendar quarter, provided the terminating Party gives written notice of termination to the other Party at least 30 days before the end of the quarter.
   b. Either Party may terminate this Agreement for cause after the other Party has failed to cure a material breach, provided the terminating Party gives the other Party written notice of breach and provides at least 14 days for the other Party to cure the breach.
DUA elements (not likely in MOU)

- **Boilerplate**
  - Entire agreement
  - Severability
  - Limitations on liability
  - No third party beneficiaries
  - Modification
  - Warranties
What has your experience been?

- Has your organization signed any DUAs/MOUs?
- Why did you choose one versus the other?
- What lessons have you learned?
Business Associate Agreements

» HIPAA Privacy Rule requires all covered entities to sign a Business Associate Agreement (BAA) with any business associate they hire that may come into contact with protected health information (PHI)

» A business associate is any organization that creates, receives, maintains or transmits PHI on behalf of a covered entity

» A Business Associate Agreement is a written agreement that specifies each party’s responsibilities when it comes to PHI
Examples of Business Associates

- Medical billing
- Attorney
- Accountant
- Transcriptionist
- Email provider
- IT vendor
- Cloud storage
- File sharing
- Encryption software
- Shredding
- Claims processor
- Administration
- Consultant
- Rx benefits manager
Who is not considered a business associate?

» Conduit exception – entities that simply transport or transmit PHI are not considered BAs.

• Examples:
  • United States Postal Service
  • Internet Service Providers
  • Couriers and electronic equivalents

» HIPAA makes a distinction between transmission (including incidental storage associated with such transmission) and ongoing storage
Business Associate Agreements Requirements

» Establish the permitted and required uses and disclosures of PHI by the BA

» Provide that the BA will not use or further disclose the information other than as permitted or required by the contract or as required by law

» Require the BA to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI
BAA Requirements, cont.

» Require the BA to report to the CE any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI

» Require the BA to disclose PHI as specified in its contract to satisfy a CE’s obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings
To the extent the BA is to carry out a CE’s obligation under the Privacy Rule, require the BA to comply with the requirements applicable to the obligation.

Require the BA to make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the BA on behalf of, the CE for purposes of HHS determining the CE’s compliance with the HIPAA Privacy Rule.
BAA Requirements, cont.

» At termination of the contract, if feasible, require BA to return or destroy all PHI received from, or created or received by BA on behalf of, the CE

» Require the BA to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the BA with respect to such information

» Authorize termination of the contract by the CE if the BA violates a material term of the contract
Business associate subcontractors

» A business associate subcontractor is a person or entity to which a BA delegates a function, activity or service.

» Contracts between BAs and business associate subcontractors are subject to the same HIPAA requirements.

» Therefore, contracts between BAs and business associate subcontractors are almost identical.
Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].


Business associate subcontractors

» A business associate subcontractor is a person or entity to which a BA delegates a function, activity or service

» Contracts between BAs and business associate subcontractors are subject to the same HIPAA requirements

» Therefore, contracts between BAs and business associate subcontractors are almost identical
Audits and penalties

» HHS can audit BAs and business associate subcontractors for compliance

» Ultimate responsibility for protection of PHI rests with the CE

» A CE should require in their BAA that the BA disclose any subcontractor relationships and require a Subcontractor BAA be signed
What has your experience been?

- Has your organization evaluated your contractors to ensure necessary BAAs are in place?
- How often do you review these contracts?
- Did you use the HHS sample agreement or develop your own BAA?
User agreement

• Agreement for use of a data system that establishes the responsibilities of the user and the acceptable uses of the data

» User agrees to terms set by the controlling entity (privacy, confidentiality, security, access, violations, termination)

» Binds the user to state and federal laws governing the data system
User agreement

»User agreements should be utilized when individuals are being provided with access to a data system for routine, ongoing activities

• Example: Doctor has access to immunization information system to obtain information regarding patient vaccinations and reminder notifications
If the person or entity performs functions on behalf of, or provides services to, a covered entity, then require a BAA.

If they are doing both, then require both a BAA and user agreement.

If the person or entity is using information for their own behalf for permitted uses, then require a user agreement.
What has your experience been?

- Do you utilize user agreements in your organization?
- What has been your experience in developing such agreements?
- What lessons have you learned?
When is consent required?

**It depends**

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What data?</td>
<td></td>
</tr>
<tr>
<td>From whom was it obtained?</td>
<td></td>
</tr>
<tr>
<td>For what purpose was it obtained?</td>
<td></td>
</tr>
<tr>
<td>To whom is it to be disclosed?</td>
<td></td>
</tr>
<tr>
<td>For what purpose is it to be disclosed?</td>
<td></td>
</tr>
<tr>
<td>How will it be disclosed?</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Laws: General Rules

1. Protection applies only to personally identifiable information

2. Personally identifiable information can only be disclosed with the individual’s consent, unless an exception applies
Review privacy law for:

» **Description of information that is protected**

» **Exceptions to consent**

» **Requirements for valid consent**
  ▶ Who can consent  ▶ Type of consent
  ▶ Form of consent  ▶ Elements to be included
  ▶ Process to obtain consent

» **Limitations on redisclosure and/or secondary uses by data recipient**
Forms of consent for disclosure of information

» Oral
» Written
» Electronic
Consent forms: General elements & notices

» Name of patient / individual
» What may be disclosed
» Who may disclose it
» Who may receive it
» Purpose for which information may be disclosed
» Signature of patient or representative
HIPAA compliant consent form

HIPAA required elements & notices

- Revocation of consent
- Refusal to consent
- Expiration of consent
- Redisclosure of information
- Right to copy of authorization form
Navigating the law

*Informed consent as a solution* . . .

*people just want to be asked* . . .

**Concern:** May not be easy to design or implement an informed consent process

**Concern:** reduce value of data

--- Self-selection

--- Justice – inclusion of under-represented and vulnerable groups

**Concern:** Need the population data for population health
What has your experience been?

- If you utilize consent forms, for what purpose?
- How do you ensure that consent forms are clear and written in plain language?
- What lessons have you learned?
Service Level Agreement (SLA)

» Defines the level of service (reliability) expected by a customer from a supplier
» Defines responsibilities of both parties
» Lays out the metrics by which the service is measured
» Sets out the remedies or penalties, if any, should the agreed-on service levels not be achieved

• Used in conjunction with an IT vendor contract
Service Level Agreement (SLA)

» Service providers often have standard SLAs, but they can (and should) be negotiated

» SLAs should be reviewed by legal counsel because they usually slant in favor of the supplier

» SLAs generally include components in 2 areas, service and management
Service Elements:
- Service specifics and standards
- Conditions of service availability
- Responsibilities of each party
- Escalation procedures
- Cost/Service tradeoffs
Mgmt Elements

- Measurement standards + methods
- Reporting Process
- Content and frequency
- Dispute resolution, indemnification
- Mechanism to update agreement
Service availability:
Amount of time the service is available for use.

Defect rates:
Counts or percentages of errors in major deliverables.

Technical quality:
Measurements of technical quality using analysis tools.

Security:
Measurements of controllable security compliance actions.

Business results:
Business process metrics such as key performance indicators.
What has your experience been?

- Have you negotiated an SLA?
- What types of metrics have you used to ensure the quality of service?
- What lessons have you learned?
Thank you!

Jennifer Bernstein, JD, MPH
jbernstein@networkforphl.org

I ❤️ LAWYERS