Commonwealth Medicine Publications   Commonwealth Medicine

2017-10-24

Data Sharing Agreements 101: What Hepatitis Programs Need to Know

Deborah Drexler
University of Massachusetts Medical School

Let us know how access to this document benefits you.

Repository Citation

Data Sharing Agreements 101: What Hepatitis Programs Need to Know

NASTAD & University of Massachusetts Medical School

October 24, 2017

Audio by phone: 1 877 369 0926 (Toll Free)
Webinar ID: 588-496-328

Emerging Opportunities for Public Health and Health Systems Data

- NASTAD's Health Systems Integration program includes a focus area on health systems data and opportunities for public health programs to use that data to improve HIV and hepatitis surveillance and programs
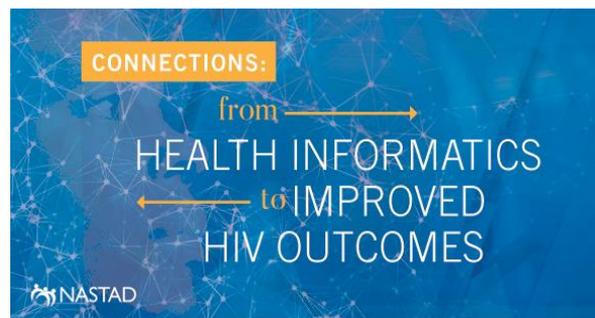
Claims data	Encounter data
(Medicaid, Medicare, commercial insurance, All-Payer Claims Databases)	(Electronic Health Records, Health Information Exchanges)

CONNECTIONS: from HEALTH INFORMATICS to IMPROVED HIV OUTCOMES

FINANCING HIV PREVENTION SERVICES

Collaboration and Innovation between Public Health and Medicaid Agencies

The Webinar Series & Technical Resources

- NASTAD partnered with informatics experts at the University of Massachusetts Medical School to create a webinar and technical resource series focused on health systems data opportunities for hepatitis C programs
  - Querying Claim Databases for HCV Testing and Treatment
    - *With accompanying technical resource*
  - Data Sharing Agreements 101: What Hepatitis Programs Need to Know
    - *With accompanying technical resource*
  - Leveraging EHRs and HIEs for Hepatitis C Surveillance, Prevention and Management: Exploring Ways that Public Health Departments May Utilize These Resources

Data Sharing Agreements 101: What Hepatitis Programs Need to Know

Deborah Drexler
University of Massachusetts
Medical School

Overview

- Step One: Planning for the Data Request

- Step Two: Understanding the Legal Landscape
  o HIPAA, and Other Laws and Requirements
  o The HIPAA Disclosure Rules: De-Identified Data
  o The HIPAA Disclosure Rules: Identified Data

- Step Three: Understanding Data Sharing Agreements
  o HIPAA Mandated Agreements
  o MOUs and Other Names
  o Provisions to Negotiate

NASTAD

Step One: Planning for the Data Request

Planning for the Data Request

- What is the purpose of the project?
- How will you use the dataset?
  - Need for identifiers?
- Which entity is in possession of the dataset?
  - Is the entity covered by HIPAA?
- Who will own the intellectual property?
- How will the data be transmitted?
- How will the data be stored?

Step Two: Understanding the Legal Landscape

Understanding the Legal Landscape

- HIPAA
  - Applies to health plans and health providers who conduct HIPAA standard electronic transactions.
  - Controls the use of personally identifiable health information.

- Other laws and requirements:
  - Identity theft laws.
  - "Super confidential" health data.
  - Contractual Requirements (i.e., SSA) .

The HIPAA Disclosure Rules: De-identified Data

A HIPAA-covered entity may disclose <u>de-identified</u> data at any time. A de-identified data set has none of the following identifiers:

- Name
- Geographic subdivisions smaller than state, including street address, city county, and zip code, except for the first three digits of a ZIP code if that area contains more than 20,000 people;
- All elements of dates related to an individual, except year, including birth date, admission date, discharge date, and death date, except that all ages over 89 and all elements of dates (including year) indicative of such age must be aggregated into a single category of age 90 or older
- Telephone number
- Fax number
- Email address
- Social Security Number

- Medical record number
- Health plan beneficiary number
- Account number
- Certificate or license number
- Any vehicle identifiers and serial numbers including license plate numbers
- Device identifiers and serial number
- Web URL
- Internet Protocol (IP) Address
- Biometric identifiers including finger or voice print
- Full-face photographic image or other photographic image that identifies a person
- Any other unique identifying number, characteristic or code.

NASTAD

The HIPAA Disclosure Rules: Identified Data (1)

- A HIPAA-covered entity may disclose datasets containing personally identified data:
  - With patient consent.
  - Without consent, when required by law.
  - Without consent, for routine business purposes: treatment, payment, health care operations.

NASTAD

The HIPAA Disclosure Rules: Identified Data (2)

- A HIPAA-covered entity may disclose a "Limited Data Set" (LDS) without patient consent, but only for research or public health purposes.

- A "Limited Data Set" has only the following identifiers:
  - Any elements of dates (years, months, days, hours and minutes);
  - Geographic subdivisions down to cities and five digit zip codes;
  - Age in years, months or days or hours.

- The recipient of the LDS must sign a "LDS Data Use Agreement."

NASTAD

The HIPAA Disclosure Rules: Identified Data (3)

- A HIPAA-covered entity may disclose personally identified data without consent for research purposes in the following circumstances:

  - With a waiver of consent issued by an Institutional Review Board.
  - For review preparatory to research, if the data does not leave the possession of the covered entity.
  - When patients are all decedents.

- The HIPAA-covered entity must track these disclosures and inform patients about them if asked.

Step Three: Understanding Data Sharing Agreements Mandated Agreements

Mandated Agreements

- Certain data sharing agreements are mandated by HIPAA:

  - Business Associate Agreement
    - Mandatory when the recipient of the data is performing a function on behalf of the HIPAA-covered entity.
    - Recipient must agree to comply with all requirements of HIPAA

  - Limited Data Set Data Use Agreement
    - Mandatory when the recipient has received a Limited Data Set.
    - Recipient must agree to restricted use of the data and to comply with certain HIPAA requirements

- In either case, the parties may include additional, non-mandated provisions, which are subject to negotiation.

"MOUs" and Other Names

- A non-mandated data sharing agreement may be called different names.

- The name of the agreement is not consequential.

- An agreement between two departments of a legal entity is often referred to as a "Memorandum of Understanding."

  - Such agreements are not enforceable in a court of law.
  - But provisions are still a matter of negotiation, subject to internal policies.

NASTAD

Provisions to Negotiate

- Will the recipient of the data be working independently or on behalf of the disclosing entity?

- Who owns the data after transmission?

- Who owns the result of the project?

- Are there any restrictions on the recipient's use of the data?

  - Will the recipient be restricted from subcontracting any part of the project?
  - Is any training required for the users of the data?

- Are there any restrictions on the recipient's use of the project results?

- How will the data be transmitted?

  - Which entity is responsible for the data during transmission?
  - Are any particular security controls required?
  - When will transmission be considered complete?
  - What happens if transmission fails ?

Provisions to Negotiate (continued)

- How will the data be stored?

  - Are any particular security controls required during storage?
  - Does the disclosing entity have the right to access the stored data?

- What happens if there is a privacy or security breach?

  - Who is responsible for notification and mitigation efforts?

- Will the data need to be returned or destroyed at the end of the project?

- Under what circumstances can the agreement be terminated?

- What happens upon termination? Do any provisions of the agreement survive termination?

- Can the agreement be amended and how?

Questions? Comments?

- Deborah Drexler, University of Massachusetts Medical School, deborah.drexler@umassmed.edu

- Amy Killelea, NASTAD, akillelea@nastad.org

- Alyssa Kitlas, NASTAD, akitlas@nastad.org

- Edwin Corbin-Gutierrez, NASTAD, ecg@NASTAD.org

Future Presentations in This Series

- Leveraging EHRs and HIEs for Hepatitis C Surveillance, Prevention and Management: Exploring Ways that Public Health Departments May Utilize These Resources
  - Tuesday, October 31 from 3-4 PM ET Register here and complete the pre-webinar questionnaire here

Thank you to Gilead Sciences for supporting this project

Resources

- **NASTAD Resources**
  - NASTAD primer on health systems data opportunities for HIV programs: [Connections: From Health Informatics to Improved HIV Outcomes](#)
  - [NASTAD's Health Systems Integration Informatics Page](#)

- **Additional Health Systems Data Resources**
  - [HIV Health Improvement Affinity Group; HRSA, CDC, and CMS](#)
  - [Health Information Technology and Informatics, NACCHO](#)
  - [Public Health Informatics, ASTHO](#)
  - [Joint Public Health Informatics Taskforce (JPHIT)](#)
  - [Digital Bridge](#)