October 16, 2019

Secondary Uses of Health Data for Research and Development Purposes

Privacy+ Security Forum

David Peloquin, JD
Ropes & Gray

Joanna Bergmann, JD, MPH, MBE
Northwell Health

Brett Silton, JD
Verana Health

Agenda

- **Introduction**
- Secondary Uses of Health Data for Research Purposes
  - Secondary use of protected health information (PHI) under HIPAA
  - Intersection with revised Common Rule
  - Additional federal / state law protections for specific types of data
  - General Data Protection Regulation (GDPR) considerations
- Secondary Uses of Health Data by Business Associates for Development Purposes

Introduction

- Goal of session is to discuss “secondary uses” of health data
- What do we mean by secondary use?
  - Use of health data collected for a primary or initial purpose (e.g., clinical care) for a secondary purpose (e.g., research or product development)
  - We will explore secondary use by a health care provider that generated the data and service providers (e.g., business associates) that received the data in the course of performing services
- Examples
  - Health care provider wishes to use medical record data for research
  - Medical device manufacturer desires to use data generated in course of patient care to refine its diagnostic algorithms
  - Clinical laboratory wishes to use data generated in course of analyzing specimens for clinical trial recruitment purposes
  - Analytics company acting as a business associate wishes to de-identify data received from covered entities and license them to third parties

Agenda

- Introduction
- **Secondary Data Uses for Research Purposes**
  - Secondary use of protected health information (PHI) under HIPAA
  - Intersection with revised Common Rule
  - Additional federal / state law protections for specific types of data
  - General Data Protection Regulation (GDPR) considerations
  - California Consumer Privacy Act (CCPA) and secondary uses
- Secondary Uses by Business Associates for Development Purposes

Secondary Data Uses for Research Purposes

- What do we mean by “research”?
  - HIPAA defines “research” as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge”
  - Contrast to “quality improvement” or “quality assurance” activities, which are considered “health care operations”
  - Whether an activity is considered “research” for purposes of HIPAA focuses on the **primary purpose** of the activity
    - If primary purpose of activity is “quality improvement,” the activity will be regulated as “health care operations” and not as research for purposes of HIPAA
    - May still be regulated as “research” for purposes of Common Rule and FDA regulations

Uses / Disclosures for Research Purposes under HIPAA

- How can a covered entity use or disclose protected health information ("PHI") for research purposes under HIPAA?
  - Research is **not** considered a treatment, payment, or health care operations ("TPO") activity under HIPAA
  - Covered entity requires another legal basis for use and disclosure of PHI for research purposes

Uses / Disclosures for Research Purposes under HIPAA

- Potential bases for use / disclosure of PHI for research purposes include the following:
  - With subject **authorization**
    - Can authorize “future research” if future research is described in sufficient detail such that a reasonable person would understand that his or her PHI could be used or disclosed for a particular research project
    - June 2018 interim guidance from HHS Office for Civil Rights (OCR) suggested interest from OCR in providing further guidance on this topic
    - Increasingly non-covered entities (e.g., non-profit research foundations) obtain broad authorizations from patients to obtain PHI for secondary research uses
  - **Without subject authorization**, if one of the following legal bases is present:
    - Use is for purposes **preparatory to research**
    - **Waiver or alteration of authorization** by IRB or privacy board
    - **Limited data set** with data use agreement
    - Use / disclosure is limited to **decedents’** protected health information
    - **De-identified data**

Uses / Disclosures for Research Purposes under HIPAA

- A researcher can use PHI for purposes "preparatory to research" (e.g., preparing a research protocol, determining feasibility of research, identifying potential research subjects) if he/she makes the following representations to the covered entity:
  - Use or disclosure of PHI is sought solely to prepare a research protocol
  - Researcher agrees not to remove PHI from the covered entity
  - The PHI for which use is sought is necessary for the research purposes
- December 2017 guidance from OCR provided more detail on requirement that researcher not remove PHI from the covered entity
  - Guidance explains that "removing" PHI includes both physically taking such PHI out of a facility and downloading PHI onto a device
  - Remote access connectivity does not necessarily constitute a removal of PHI, provided the PHI is not printed, downloaded (except in limited circumstances), copied, saved, data scraped or faxed
- Could a covered entity engage a business associate to perform these activities?

Uses / Disclosures for Research Purposes under HIPAA

- Waiver of HIPAA Authorization: Authorization can be waived by an IRB or a Privacy Board (similar to an IRB) for use or disclosure of PHI for research.
  - A covered entity can rely on a waiver by an outside IRB or Privacy Board
- To grant waiver, the IRB/Privacy Board must find the following:
  - Use of PHI has only minimal risk to the privacy of individuals
  - Research could not be practicably conducted without the waiver or alteration of authorization
  - Research could not practicably be conducted without access to and use of the PHI
- Waiver requires documentation:
  - Date/statement that the IRB has determined that the above criteria are satisfied
  - Description of the PHI for which waiver is granted
  - Signature of IRB/privacy board chair or designee

Uses / Disclosures for Research Purposes under HIPAA

- Limited Data Set with Data Use Agreement ("DUA"): A covered entity may disclose a limited data set to the researcher for research purposes pursuant to a data use agreement.
  - A limited data set excludes specified direct identifiers of the individual or of relatives, employers, or household members of the individual
  - The only identifying information that may remain are: dates such as admission, discharge, service, DOB, DOD; city, state, five digit or more zip code; and ages in years, months or days or hours
    - ***What about year and quarter?***
  - The DUA must
    - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
    - Limit who can use or receive the data; and
    - Require the recipient to agree to a series of conditions (e.g., use appropriate safeguards to prevent unauthorized uses and disclosures, not use or disclose the information other than as permitted by the DUA or required by law, not identify the information or contact the individual).

Uses / Disclosures for Research Purposes under HIPAA

- De-Identification of PHI. Two options:
  - Safe Harbor: Removal of **18 identifiers** specified in the HIPAA Privacy Rule provided that the covered entity does not have "actual knowledge" that the remaining information could be used alone or in combination with other information to identify an individual who is the subject of the information; or
  - Determination by an expert applying generally accepted statistical and scientific principles and methods determines that probability of re-identification is "very small"
- Under the "safe harbor" methodology, one can include a "re-identification code" in the data set provided that (i) the code is not derived from or related to information about the individual (e.g., not derived from the SSN); and (ii) the covered entity does not disclose the code for any other purpose
  - Often used in research setting to permit researchers to request additional information later

De-Identification Under HIPAA Safe Harbor Method

Privacy+ Security Forum

18 HIPAA Identifiers (related to individual or their relatives, household members or employer)	
1. Names	10. Social security numbers
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census: a. The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and b. The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000	11. Internet Protocol (IP) addresses
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older	12. Medical record numbers
4. Telephone numbers	13. Biometric identifiers, including finger and voice prints
5. Vehicle identifiers and serial numbers, including license plate numbers	14. Health plan beneficiary numbers
6. Fax numbers	15. Full-face photographs and any comparable images
7. Device identifiers and serial numbers	16. Account numbers
8. Email addresses	17. Certificate/license numbers, and
9. Web Universal Resource Locators (URLs)	18. Any other unique identifying number, characteristic, or code

When are entities involved in research business associates?

- Business associates are entities that use PHI to perform (i) certain functions regulated by HIPAA, such as health care operations or payment activities, on behalf of the covered entity, or (ii) certain services on behalf of the covered entity (e.g., legal, management consulting)
  - Researchers are not considered business associates because research is neither a “health care operation” nor a “payment” activity or one of the services that gives rise to a business associate relationship
- Are entities that act as vendors providing support to a research study business associates?
  - Consider whether the function performed would otherwise give rise to a business associate relationship
- If an entity is not a business associate, what terms should be used to bind the entity?

How does the HIPAA Privacy Rule intersect with research regulations for secondary research?

- Revisions regulations on human subjects research conducted or supported by federal departments and agencies (Common Rule) took effect in January 2019
  - New exemption for “secondary research” if the use of information is performed by an investigator who is regulated by HIPAA as a “covered entity” or “business associate” and the research is performed for purposes of “health care operations,” “research,” or “public health activities and purposes”
  - Likely to increase extent to which privacy professionals within covered entities are involved with research activities
- If results of analysis will be submitted to Food & Drug Administration (FDA) in support of marketing application, consider FDA regulations on human subjects research
- If results of research will be published in a peer-reviewed journal, consider journal requirements for IRB review

How do state privacy laws affect secondary research?

- State laws often provide additional protection to specific categories of health information, *e.g.*, genetic information, mental health information, HIV/AIDS information
  - Often unclear as to extent to which secondary use permissible
- One example is New York law on genetic information privacy (N.Y. Civ. Rights Law §79-l)
  - Requires specific form of informed consent for performance of genetic tests on biological samples
  - Prohibits disclosures of genetic test results absent patient consent
  - Permits genetic tests to be performed on **anonymous samples** for research or statistical purposes pursuant to IRB-approved protocols
    - Does this also permit secondary use of anonymous **genetic information** if there is IRB approval?
    - What is pathway for non-research secondary uses of genetic information?

How do state privacy laws affect secondary research?

- California Consumer Privacy Act (CCPA) poses several questions regarding secondary research uses of personal information
  - Exception to right of deletion for “research” if deletion would render impossible or seriously impair achievement of such research and consumer has provided informed consent
    - Research is defined as “public or peer-reviewed scientific, historical, or statistical research in the public interest”
    - Can a company’s internal research and development activities meet this standard?
    - Or could these activities fit within exception for “solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer’s relationship with the business”?
  - CCPA does not apply to “information collected as part of a clinical trial subject to the [Common Rule, FDA regulations on human subjects protection, or ICH GCP]
    - What about observational research?
    - What about secondary uses of data collected in clinical trials?

How does Part 2 affect secondary research?

Privacy+ Security Forum

- Federal regulations at 42 CFR Part 2 (“Part 2”) govern confidentiality of records held by programs providing federally-assisted substance use disorder diagnosis, treatment, or referral for treatment (“SUD”)
  - Part 2 permits SUD records to be disclosed without patient consent for research purposes if the recipient certifies that he or she is required to abide by HIPAA or the Common Rule
  - Proposed Rule issued in August 2019 would relax requirements to permit a Part 2 program that is also a HIPAA covered entity to disclose SUD records in accordance with HIPAA regardless of whether the SUD records are disclosed to a covered entity or entity subject to the Common Rule

EU General Data Protection Regulation (GDPR) and Secondary

- Health data are considered “special categories” of data under GDPR
- What is the Article 9 exception to permit processing “special categories” of data for secondary uses?
  - Obtaining the **explicit consent** of the data subject.
    - *Cf.* GDPR Recital 33 with Article 29 Working Party guidance on consent.
  - Processing necessary for reasons of **public interest in the area of public health**, (*e.g.*, quality and safety of health care and of medicinal products or medical devices) . . . on the basis of Union or Member State law.
  - Processing necessary for archiving purposes in the public interest, **scientific or historical research purposes,** . . . in accordance with Article 89(1) based on Union or Member State law.

EU General Data Protection Regulation (GDPR) and Secondary Uses of Health Data

- Which uses can be considered "compatible" with the primary processing of health data?

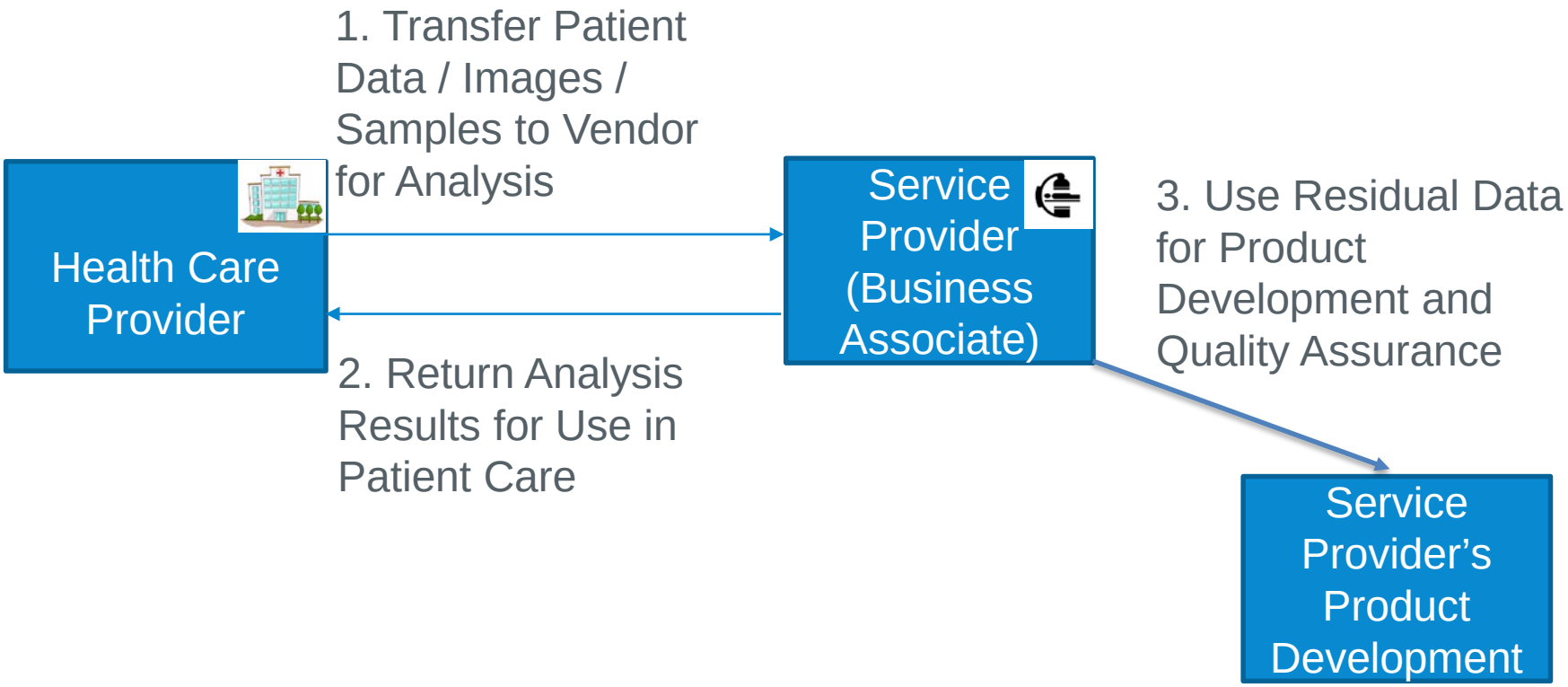
> Personal data shall be . . . collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes**.
>
> GDPR, Art. 5(1)(b)

- European Data Protection Board (EDPB) guidance suggests compatibility may be appropriate permission for secondary research, though highlights need for further guidance.
  - "These conditions, due to their horizontal and complex nature, will require specific attention and guidance from the EDPB in the future. **For the time being, the presumption of compatibility, subject to the conditions set forth in Article 89, should not be excluded, in all circumstances**, for the secondary use of clinical trial data outside the clinical trial protocol for other scientific purposes."

Agenda

- Introduction
- Secondary Uses of Health Data for Research Purposes
  - Secondary use of protected health information (PHI) under HIPAA
  - Intersection with revised Common Rule
  - Additional federal / state law protections for specific types of data
  - General Data Protection Regulation (GDPR) considerations
- **Secondary Uses of Health Data by Business Associates for Development Purposes**

Reuse of Patient Data – Common Scenario



Secondary Use Questions

- What restrictions govern the ability of a service provider to use PHI for development and quality assurance purposes?
  - Limited to using PHI on behalf of the covered entity, *except that business associate can obtain permission from covered entity to*:
    - Use the PHI for its own “management and administration” purposes
    - Use the PHI to perform “data aggregation” on behalf of multiple covered entities
    - De-identify PHI with express permission of covered entity
  - Consider limitations on secondary use contained within underlying services agreement

Secondary Use Questions

- If using images (e.g., retina or iris scans), consider applicability of state biometric privacy laws
  - These laws contain various exceptions for information collected by health care providers
  - Key question is extent to which biometric data can be considered anonymized under these laws

Summary

- Secondary uses of health data hold much promise given the advent of “big data” research and the growth of real world evidence (‘RWE”)
- Several questions to ask when using such data for secondary purposes
  - What is the purpose of the secondary use of data?
    - Research to develop generalizable knowledge
    - Quality improvement
    - Product development
  - Which legal regimes govern the use of the data?
  - What pathway(s) does the relevant legal regime permit for secondary uses of data?
  - Does the relevant legal regime distinguish between identified and de-identified data?

QUESTIONS

THANK YOU