FOLEY HOAG
SINCE 1943

The Interplay of HIPAA, Privacy and Data Security Principles, and Health Information Interoperability

MedInnovation Boston

June 25, 2018

Colin J. Zick
Foley Hoag LLP
(617) 832-1275
czick@foleyhoag.com

Colin J. Zick

Partner, Chair, Privacy and Data Security Practice and Co-chair, Health Care Practice

Boston | +1.617.832.1275 | czick@foleyhoag.com

- Counsels clients ranging from the Fortune 1000 to start-ups on issues involving information privacy and security, including state, federal and international data privacy and security laws and government enforcement actions.

- Advises on issues involving the transfer of data between jurisdictions, including GDPR, the EU-US Privacy Shield, and other relevant data privacy and security laws, cloud security, cyber insurance, the Internet of Things, and data breach response.

- Co-founded the firm's Privacy and Data Security Group (which he currently chairs) and regularly contributes to its "Security, Privacy and the Law" blog, www.securityprivacyandthelaw.com, and was recognized by JD Supra's 2017 Readers Choice Awards. Serves as outside counsel to the Advanced Cyber Security Center, and is a member of Law360's Privacy & Consumer Protection editorial advisory board.

All That Data!

- Therapies, diagnostics, and connected devices now gather huge amounts of data
- That data can be more valuable than the “thing” that is treating, diagnosing, or connecting, provided you have the legal ability to use that data, by:
  - Direct consent
  - Operation of law
  - Aggregation/anonymization
- Interoperability underlies all of this

HIPAA Overview

- HIPAA does not apply directly to many players in the health care system.
- Data privacy and security pose distinct and significant business and regulatory challenges.
- Data privacy and security issues are driven by more and more data and more uses for that data.

"The Real HIPAA Supports Interoperability"

"At ONC, we hear all of the time that the Health Insurance Portability and Accountability Act (HIPAA) makes it difficult, if not impossible, to move electronic health data when and where it is needed for patient care and health. This is a misconception, but unfortunately one that is widespread."

Aja Brooks, J.D. and Lucia Savage, J.D. of the Office of the National Coordinator for Health Information Technology, February 4, 2016

Available at https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/the-real-hipaa-supports-interoperability/#.WxlnCVqClBI.email

HIPAA Regulatory Refresher:

- PHI is any “individually identifiable health information” that is transmitted by a “covered entity” in connection with specified electronic transactions (which makes it “ePHI”)
- HIPAA privacy and security rules apply only to “ePHI”
- HIPAA privacy protects against improper use/disclosure of health information
- HIPAA security protects against improper access to health information

Does HIPAA Apply Directly?

- What kinds of businesses are “covered entities”?
  - Health care providers
  - Health plans
  - Health care clearinghouses
- Most providers are considered a “covered entity” but some could also be serving as a “business associate”

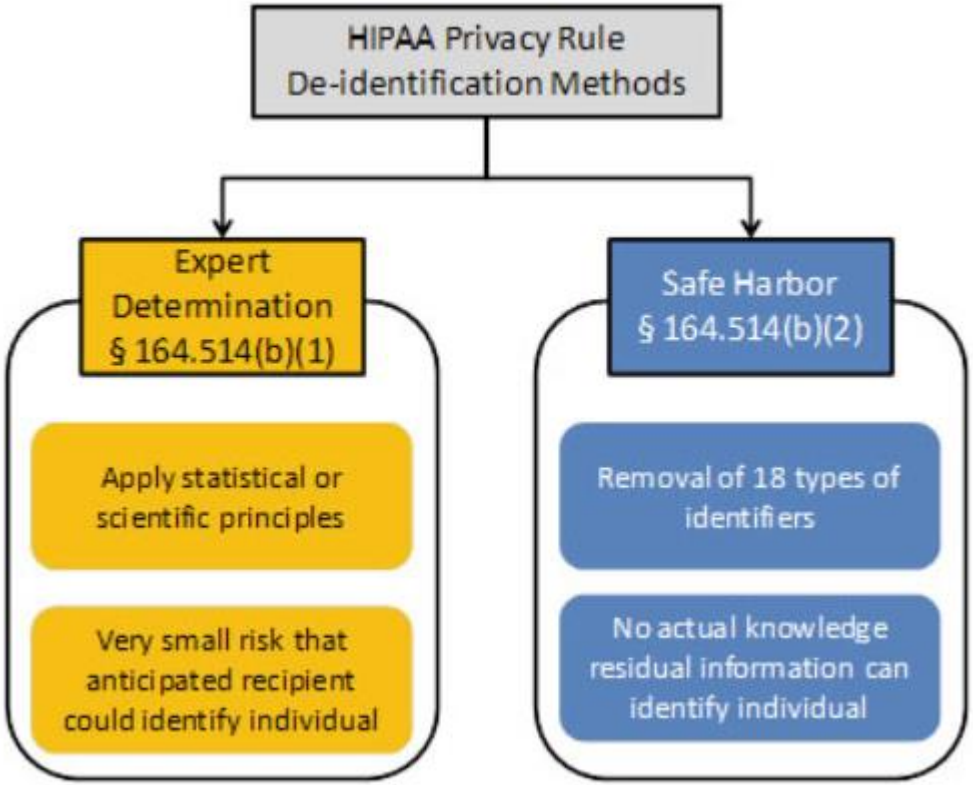
HIPAA Business Associate Rule: A Key Element in Interoperability

- A Covered Entity may not disclose PHI to a Business Associate without "satisfactory assurance" that the PHI will be appropriately safeguarded, *i.e.*, a written contract with specific provisions
- The rule does not apply to disclosures:
  - By a Group Health Plan, Health Insurance Issuer or HMO to the plan sponsor if the plan document and certification requirements are met
  - By a health plan that is a governmental program (under limited circumstances)

HIPAA Authorizations Can Facilitate Interoperability

- **An authorization must specify a number of elements, including:**
  - a description of the protected health information to be used and disclosed,
  - the person authorized to make the use or disclosure,
  - the person to whom the covered entity may make the disclosure,
  - an expiration date, and,
  - in some cases, the purpose for which the information may be used or disclosed.
  - With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.
- The HIPAA Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of protected health information for research purposes is to be altered or waived.

HIPAA De-Identification: Another Means to Data Use and Sharing



HIPAA De-Identification - Details

The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

- (A) Names
- (B) All geographic subdivisions smaller than a state….
- (C) All elements of dates (except year) … ages over 89 …
- (D) Telephone numbers
- (L) Vehicle identifiers and serial numbers, including license plate numbers
- (E) Fax numbers
- (M) Device identifiers and serial numbers
- (F) Email addresses
- (N) Web Universal Resource Locators (URLs)
- (G) Social security numbers
- (O) Internet Protocol (IP) addresses
- (H) Medical record numbers
- (P) Biometric identifiers, including finger and voice prints
- (I) Health plan beneficiary numbers
- (Q) Full-face photographs and any comparable images
- (J) Account numbers
- (R) Any other unique identifying number, characteristic, or code; and
- (K) Certificate/license numbers

Contracts Can Promote Effective Data Use

- **Contracts are key to effective data use:**
  - Consents and authorizations
  - Terms of use and privacy policies
  - Notices of privacy practices
  - Licenses
  - HIPAA business associate agreements

Data Use Agreements Can Promote Interoperability

- **A data use agreement can:**
  - establish the permitted uses and disclosures of the limited data set;
  - identify who may use or receive the information;
  - prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law;
  - require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement;
  - require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware;
  - require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the agreement; and
  - prohibit the recipient from identifying the information or contacting the individuals.

HIPAA Limited Data Sets Can Avoid Roadblocks that Stop PHI

- Under HIPAA, a “limited data set” of information may be disclosed to an outside party without a patient’s authorization if certain conditions are met.
- First, the purpose of the disclosure may only be for research, public health or health care operations.
- Second, the person receiving the information must sign a data use agreement.
- This agreement has specific requirements which are discussed in the prior slide.

HIPAA Limited Data Sets (cont.)

A “limited data set” is information from which “facial” identifiers have been removed. Specifically, as it relates to the individual or his or her relatives, employers or household members, **all the following identifiers must be removed in order for health information to be a “limited data set”:**

- names;
- street addresses (other than town, city, state and zip code);
- telephone numbers;
- fax numbers;
- e-mail addresses;
- Social Security numbers;
- medical records numbers;
- health plan beneficiary numbers;
- account numbers;
- certificate license numbers;
- vehicle identifiers and serial numbers, including license plates;
- device identifiers and serial numbers;
- URLs;
- IP address numbers;
- biometric identifiers (including finger and voice prints); and
- full face photos (or comparable images).
- **The health information that may remain in the information disclosed includes:**
- 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.

Transfers of European Data: EU-US Privacy Shield

- 3d February 2016: Article 29 Working Party issued a statement:
  - The new Privacy Shield: they want to see the documents.
  - Alternative transfer tools (SCC, BCR) :

    The robustness of these tools must be analyzed in light of four essential guarantees for intelligence activities:

    1. Processing should be based on clear, precise and accessible rules.
    2. Necessity and proportionnality, with regard to the legitimate objectives pursued, need to be demonstrated.
    3. An independent oversight mechanism should exist, that is both effective and impartial.
    4. Effective remedies need to be available to the individual.

    They will issue an opinion but in the meantime, it is possible to use these alternative transfer tools.

Main Features of the Privacy Shield

- Precise content not disclosed yet.
- Same mechanism as the earlier Safe Harbor scheme.
- Key new points:
  - Stronger obligations on US companies.
  - Means of redress for European citizens.
    1. US companies themselves
    2. Alternative dispute mechanism
    3. European DPAs
    4. Arbitration mechanism
  - Limitation to the access to Europeans data by US public authorities for national security purpose
  - But will it last?

Transfer of Data to Non-EU Countries

Transfers to countries which do not provide an adequate level of protection (including the US) :

- Current transfer tools :
  - to the US : Privacy Shield.
  - Standard Contractual Clauses (SCC) issued by the Commission.
  - Binding Corporate Rules.
  - Consent.

- Additional transfer tools as from May 2018:
  - SCC issued by a Supervisory Authority.
  - Code of Conduct approved by the Supervisory Authority with binding and enforceable commitments from data importer.
  - Certification with binding and enforceable commitments from data importer.

New GDPR Obligations Starting May 2018

Notification of data breach:

To the Supervisory Authority

Level: where it is likely to result in a risk to the rights and freedoms of individuals.

Without undue delay, no later than 72 hours

Content of notification:

- Nature of the breach
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

To Data Subjects

Level: where a breach is likely to result in a high risk to the rights and freedoms of individuals.

Without undue delay

Content of notification:

- Nature of the breach in clear and plain language
- Name and contact details of the DPO
- A description of the likely consequences of the breach
- Description of the measures taken

New Obligations (cont)

Agreements between controllers and processors

- Heavier obligations and liabilities for processors.

- Contracts between controllers and processors are now mandatory and must include:
  - the subject matter and duration of the processing;
  - the nature and purpose of the processing;
  - the type of personal data and categories of data subjects;
  - the obligations and rights of the controller;
  - a list of mimimum terms, obligations of the processors to ensure that both the controller and the processor comply with GDPR.

New Obligations (cont)

EU Data Subjects' Rights

- Information
- Access
- Rectification
- **Erasure ("right to be forgotten")**
- Restriction
- **Data portability**
- Objection

Pseudonymisation and Interoperability

- **GDPR encourages "pseudonymisation" of personal data**
- The GDPR does not apply to data that "does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is no longer identifiable."
- The GDPR introduces a new concept in European data protection law – "pseudonymisation" – for a process rendering data neither anonymous nor directly identifying.
- Pseudonymisation is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately.
  - Pseudonymisation may reduce the risks associated with data processing, while also maintaining the data's utility.
  - GDPR creates incentives for controllers to pseudonymized the data that they collect. Pseudonymized data is not exempt from GDPR, GDPR relaxes several requirements on controllers that use the technique.

Dick Cheney's Heart: The Worst Case for Interoperability

- In 2008, a team of security researchers proved they could gain access through a pacemaker's wireless control system
- Vice President Cheney had an implanted pacemaker
- This led to the communications capabilities of his pacemaker being disabled
- "Disconnection" is not a viable business model
- The risk is still real and continuing:
  "J&J warns diabetic patients: Insulin pump vulnerable to hacking," Reuters, October 4, 2016

Good Interoperability News from Apple

- Apple will soon allow third-party apps to access the health data stored in its Health app.
- Apple currently works with 500 hospitals and clinics, where patients can pull their health information from electronic health records into the Apple Health app.
- Now, those patients will be able to move that data from the Health app into third-party apps if developers have used the Apple Health Records application programming interface.
  - Health app users will be able to import medication data from Apple into Medisafe, a medication management app.
  - Apps with this kind of capability will become available this fall, when Apple will release its new iPhone operating system, iOS 12.
- Is this a HIPAA issue? Since Apple itself is not storing the data or using it for healthcare purposes, it may not be a HIPAA business associate subject to HIPAA. Apple didn't mention HIPAA at all during its Health Records API announcement.

The Future of Interoperability

- If anything, U.S. law will move toward the GDPR and its more constricted views on privacy and patient consent
- This is both a threat to interoperability and an opportunity
- However, it is not clear that the U.S. will be able to respond in the next 1-2 years.

Colin Zick

Partner and Co-Chair, Health Care and Privacy & Data Security Practice Groups

Foley Hoag LLP

czick@foleyhoag.com
617.832.1275