

# The Intersection of Clinical Data Management and HIPAA

---

HOW TO ASSESS PRIVACY AND INFORMATION  
SECURITY COMPLIANCE OF CLINICAL DATA

Andrew Rodriguez, MSHI, HCISPP, CHPC, CHPS, CDP  
Corporate Privacy and Information Security Officer, Shriners Hospitals for Children

1

## Disclaimer

---

A presentation can neither promise nor provide a complete review of the myriad of facts, issues, concerns and considerations that impact upon a particular topic. This presentation is general in scope, seeks to provide relevant background, and hopes to assist in the identification of pertinent issues and concerns. The information set forth in this outline is not intended to be, nor should it be construed or relied upon, as legal advice. Recipients of this information are encouraged to contact their legal counsel for advice and direction on specific matters of concern to them.

Any opinions offered are my own and not those of my employer.

2

## Security Rule Requirements

§164.308 (A) *Risk analysis (Required)*. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.

§164.310 Physical safeguards. (d)(1) *Standard: Device and media controls*. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

§164.312 (d) *Standard: Person or entity authentication*. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

<https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=6014e7dc973ac6612a336d9f13c99f2a&mc=true&n=pt45.1.164&r=PART&ty=HTML>

3

## Why Do A Risk Assessment?

### Judge rules in favor of OCR and requires a Texas cancer center to pay \$4.3 million in penalties for HIPAA violations

A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and granted summary judgment to the Office for Civil Rights (OCR) on all issues, requiring MD Anderson to pay \$4,348,000 in civil money penalties to OCR. This is the second summary judgment victory in OCR's history of HIPAA enforcement and the \$4.3 million is the fourth largest amount ever awarded to OCR by an ALJ or secured in a settlement for HIPAA violations.

<https://www.hhs.gov/about/news/2018/06/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-violations.html>

4

## What We Know

---

### Three Breaches at MD Anderson

- April 2012, **STOLEN** laptop, not encrypted.
- July 2013, **LOST** unencrypted USB drive
- November 2013, **LOST** unencrypted USB drive

<https://www.hhs.gov/sites/default/files/alj-cr5111.pdf>

5

## What was Argued

---

Second, Respondent asserts that HIPAA doesn't apply in this case because the ePHI contained in the stolen and lost devices was research information that is outside of the statute and regulations' reach. Respondent brief at 43-44. This argument rests on what is at best a fanciful interpretation of governing regulations, and I find it to be without merit.

Respondent predicates this argument on its assertion that an exemption applies to all information or data that is used in research. Under Respondent's formulation, even patient data that reveals the names of patients, their social security numbers, their medical diagnoses, and the treatments that they are receiving is exempt from HIPAA requirements if used by someone in the course of research.

<https://www.hhs.gov/sites/default/files/alj-cr5111.pdf>

6

## What was Argued

Respondent has identified nothing in the regulations that even ostensibly supports that argument. It contends, however, that the preamble to the regulations governing unauthorized disclosure makes it plain that the regulations do not apply to research information as Respondent defines that term. It cites to language in the regulations' preamble: "[W]e cannot apply any restrictions or requirements on a researcher in that person's role as a researcher . . . In its role as researcher, the person is not covered, and protections do not apply to those research records." Respondent brief at 43 (citing 65 Fed. Reg. 82,462, 82,575 (Dec. 28, 2000)). But, and as OCR notes, this language was meant to apply to the very limited instance of research conducted by non-covered entities and business associates that receive information from covered entities. OCR reply at 10-11.

Respondent's argument also ignores the fact that there is a regulatory mechanism for a facility to segregate its research function from its clinical function and to exempt its research function from non-disclosure requirements. 45 C.F.R. § 164.105; 65 Fed. Reg. 82,462, 82,569 (Dec. 28, 2000). I make no findings regarding whether Respondent could have availed itself of this option and exempted certain ePHI from non-disclosure requirements. Suffice it to say that Respondent does not argue it made any effort to do so.

<https://www.hhs.gov/sites/default/files/alj-cr5111.pdf>

## Other Risks?



Cloud Computing



Mobile Devices



Web Apps



Storage  
(Local & Cloud)



E-Mail



Physical Security

# HIPAA Basics

---

## HIPAA is about

- Use
- Disclosure

## Types of Use and Disclosures (Authorization not required)

- Payment
- Treatment
- Operations

## Authorization Required (or IRB Waiver or Alteration)

- Research

9

# Protected Health Information

---

“Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual” that is:

Transmitted by electronic media;

Maintained in electronic media; or

Transmitted or maintained in any other form or medium.



At least one identifier

10

# Identifiers

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

- **Names**
- 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:
  - The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
  - The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
- 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
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet Protocol (IP) addresses
- **Medical record numbers**
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- **Account numbers**
- Any other unique identifying number, characteristic, or code, except as permitted by Re-identification Section of HIPAA.
- Certificate/license numbers

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

# De-Identified Information

## De-identified

- Removal of 18 identifiers
- The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information
- Low risk of re-identification
- Analytical value is dramatically decreased

## Limited Data Set

### Limited Data Set allows for:

- Dates
- Geographic information

### Notes:

- Excludes all other identifiers such as names, medical record number, and email addresses.
- Increased analytical value due to allowing dates and geographic information.
- Risk of re-identification greater than de-identified data but less than a data set with more identifiers.

13

## Authorization vs. Consent

### Clinical Research Study

- Consent to participate in study

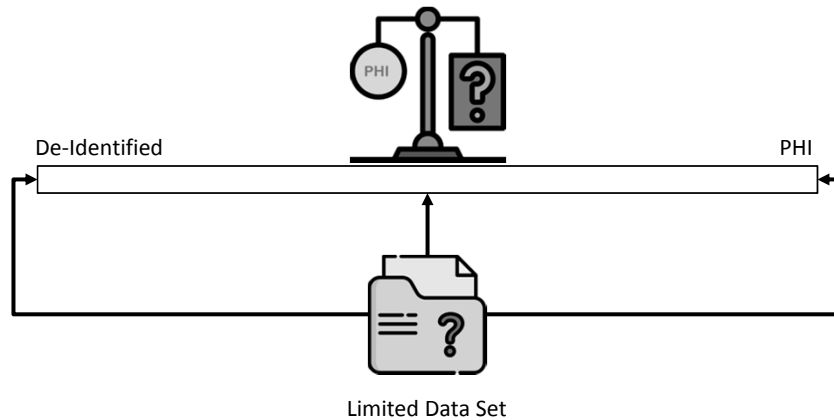
### HIPAA

- Authorization to use or disclose data
- May be embedded in consent
- Has specific requirements that need to be met for it to be valid

14

## Where Does Clinical Research Information Fall?

---



15

## Scope of Data

---

- Does the dataset or database contain information from or about patients of this organization ?
- Does this dataset or database contain information from other healthcare organizations?

16



## What is the Primary Source of Data?

---

- EMR (report or export)
- EMR (Chart Abstraction)
- Other Clinical System
- Dataset from Previous Research
- Surgery or Procedure Log (outside of EMR)
- Paper Medical Records
- Interviews (outside a clinic visit)
- Questionnaires
- Electronic devices (Biomedical Devices)
- Records provided by patient
- CRF (if stated in protocol)

17

## What are the Secondary Sources of Data?

---

- EMR (report or export)
- EMR (Chart Abstraction)
- Other Clinical System
- Dataset from Previous Research
- Surgery or Procedure Log (outside of EMR)
- Paper Medical Records
- Interviews (outside a clinic visit)
- Questionnaires
- Electronic devices (Biomedical Devices)
- Records provided by patient
- CRF (if stated in protocol)

18

## Devices used to Collect Data

---

- Clinical device
- Computers owned by the organization
- Tablet owned by the organization
- Other device owned by the organization
- Computers not owned by the organization
- Tablet not owned by the organization
- Other device not owned by the organization
- Online forms (specify)
- Paper forms

19

## Storage of Data Set (Formats)

---

- Spreadsheet (Excel, Numbers, Calc)
- Word Processor (Word, Pages, Writer)
- Desktop Database (Access, FileMaker Pro, Base)
- CSV, XML, JSON, TXT (specify)
- PDF, TIFF, XPS
- SQL Database
- NoSQL/Document Database
- Other Database
- Other

20

## Locations of Datasets

For the following, specify if system or technology is owned or licensed by the covered entity or another organization:

- Clinical Trial Management System
- Electronic Data Capture System
- Business Intelligence System
- Folder on Server
- Folder on Desktop or Laptop
- USB Drive
- Cloud Storage
- Web or Cloud Application
- Questionnaire Solution
- Data analytics Solution

21

## Distribution of Data Set

- Sent to email address within organization
- Sent to email address outside the organization
- Fax
- Postal Mail
- For the following indicate if system or technology is owned or licensed by the covered entity or another organization:
  - Moved or copied file server / folder
  - Moved or copied to USB drive
  - Moved or copied to device
  - Moved or copied to cloud services
  - Moved or copied via FTP/SFTP.
  - Direct data entry into system (Web or Cloud app).
- Other

22

## Identifiers

---

- Names
- Geographic information
- All elements of dates (except year)
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet Protocol (IP) addresses
- Medical record numbers
- Biometric identifiers including finger and voice prints
- Health plan beneficiary numbers
- ***Full-face photographs and any comparable images***
- Account numbers
- Any other unique identifying number, characteristic, or code, except as permitted by Re-identification Section of HIPAA
- Certificate/license numbers

23

## Recreation of Data

---

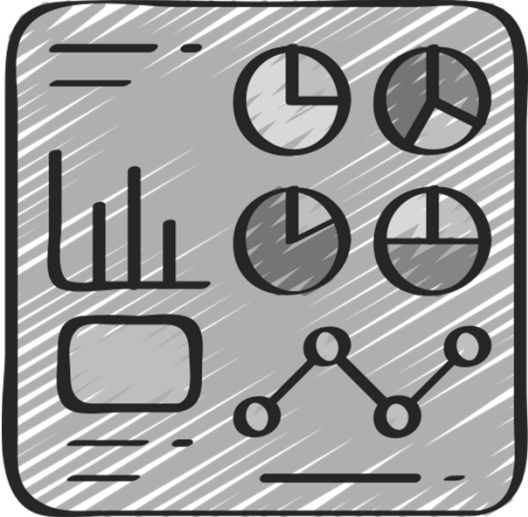
- Are there any data elements in the dataset that could not be created if lost?
  - If so, describe the data and how it is backed up?

### Examples Responses:

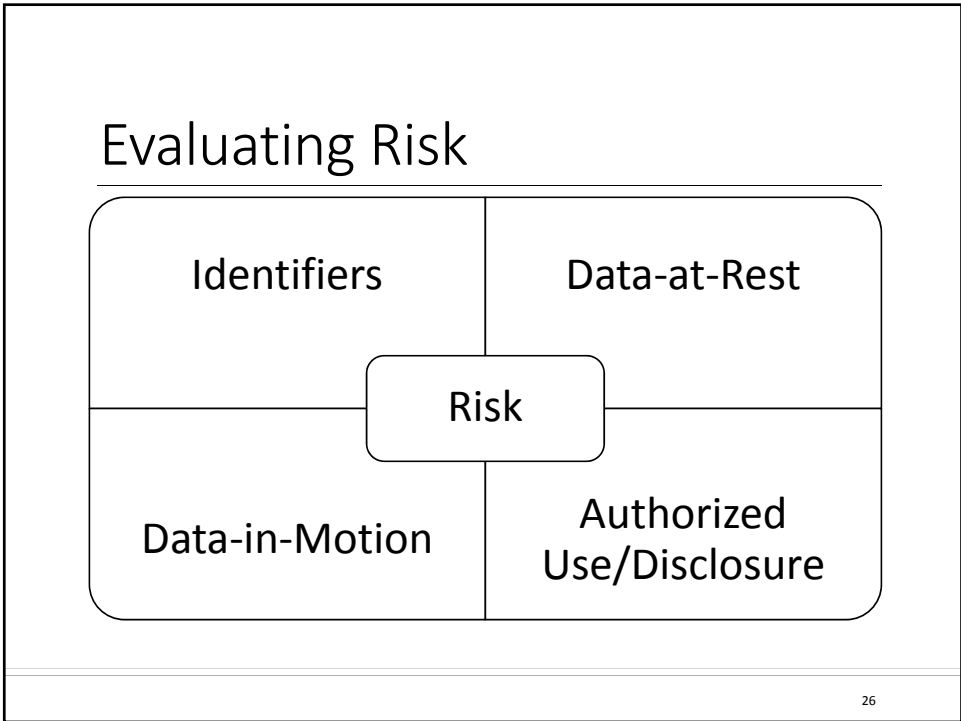
- No, all data in the dataset is pulled from an EMR and can be recreated by running the same report.
- Yes, the data from the dataset from the questionnaire service could not be recreated if the vendor lost the data. However, the dataset has been exported to spreadsheet as backup.
- No, the data was captured in real time from a treadmill and exported. However, the data is stored on a server which is backed up.

24

Risk Analysis



25



# Identifiers

Sample Risk Assessment

Type of Identifiers	Risk
Includes Social Security Number, Name and Date of Birth	Very High
Includes Name and Date of Birth	High
Includes Medical Record Number or other account number which is not public	Medium
Limited Data Set	Low
De-Identified Data Set	Very Low

27

# Data-at-Rest

Sample Risk Assessment

Type of Access	Risk
Access Restricted to organization or Access Permitted outside the organization	Very High
Access Restricted to research department	High
Access Restricted to researchers	Medium
Access Restricted to researchers audit-log of access	Low
Encrypted Access Restricted Audit-log of access	Very Low

Factors to consider: Identifiers and Agreements

28

# Data-in-Motion

Sample Risk Assessment

Type of Access	Risk
Sent to unauthorized recipient	Very High
Sent not encrypted (email, FTP, web upload) to authorized recipient	High
Encrypted file (password protected) shared via online storage or unencrypted USB	Medium
Sent encrypted (email, FTP, web upload) to authorized recipient	Low
Sent encrypted recipient covered under a Data Use Agreement	Very Low

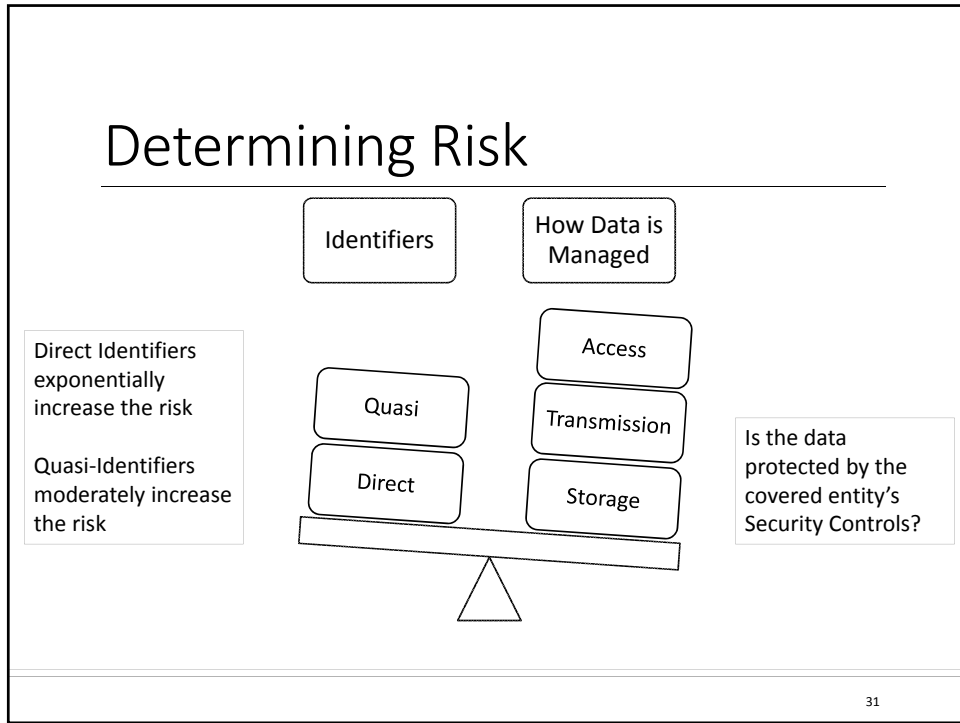
Factors to consider: Identifiers and Agreements

# Authorized Use and Disclosure

Sample Risk Assessment

Type of Access	Risk
Accessed by individuals outside of the covered entity	Very High
Accessed by individuals of the covered entity but not on the research team	High
Accessed by researchers but no formal documentation exists	Medium
Accessed by researchers who are assigned to the study where informal documentation exists	Low
Accessed by researchers who are assigned to work on the study where documentation exists	Very Low

Factors to consider: Identifiers and Agreements





# Questions

---



Contact Information:

Andrew Rodriguez  
andrew@ipscompliance.com