Complex, Crazy, and Challenging Privacy Issues

Marti Arvin
Executive Advisor
CynergisTek, Inc.

CYNERGISTEK

1

Disclaimer:

The views expressed in this presentation belong to the speaker and do not necessarily represent the views of her organization or other organizations.

Nothing in this presentation constitutes legal advice.

2

Agenda

1. Using big data and staying compliant
2. End users - proper access and disclosure for TPO
3. End users - proper access and disclosure for research
4. Privacy laws – staying current
5. Questions

3

4

Different sources of big data

- Electronic Health Records
- Health Information Exchanges
- Data warehouses
- Research repositories
- Combinations of some or all of the above

How is big data collected?

- From the patient for treatment
  - Through visits
  - Through the patient portal
- From the individual
  - through wearables
  - Provided to third parties
- From a research subject

When is HIPAA applicable to big data?

- When the information is individually identifiable health information created or received in any form by a covered entity
- PHI sneaks up on big data when the date set includes
  - Dates and/or
  - Unique identifying characteristics or codes and/or
  - Initials of the individual
- The issues above might not be relevant for a data set that has been de-identified using the statistical method

When is HIPAA applicable to big data?

- Remember for de-identification under the safe harbor the covered entity must
  - Remove all 18 identifiers for the individual, their family and any household members; and
  - Not have actual knowledge the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

What are the uses for big date in healthcare?

- Data analytics for treatment, payment, and/or health care operations
- For research
- Public Health Activities

9

Data analytics for TPO

- Multiple ways to use for data analytics
  - Comparison across
    - Different geographic locations
    - Different facilities
  - Evaluation of quality and outcomes measures
  - Assessment of revenue
  - Evaluation for fraud, waste and abuse

10

Big data for research

- For identification of cohorts in preparing a research protocol
- For identification of potential subjects
- To evaluate data from a prospective view to analysis a hypothesis

11

Big Data for Public Health Activities

- Identify
  - disease outbreaks and spread
  - public health trends based on
    - Age
    - Race
    - Income
    - Comorbities
    - Martial status
  - social determinants of health

12

Compliance issues for big data

- Who is collecting the information?
  - Providers
  - Researchers
  - Other
- Who is maintaining the information?
  - Where is being stored?
  - How is it being stored?
  - Who can access it?

13

Compliance issues for big data

- Who is governing the data's use and disclosure?
  - Is there a governance structure?
  - Who are the stakeholders involved?
- How is the data being protected?
- Who is responsible if the data is compromised?

14

15

Do your end users really know the limits of their access to PHI?

- Accessing specific records
- Disclosing information to the outside
- Limitations in specific situations
- Sharing information with business associates
- Training and education

16

Accessing specific records

- Their own record
  - Look only
  - Making changes
- Their minor child's record
  - If they are the personal representative
  - If they are not the personal representative for all records
- Their family member's record
- Records needed for certain activities
  - Child custody
  - Personal dispute
  - Concern for a colleague, neighbor, friend

17

Disclosing information to the outside

- Social media
  - Patient grants "permission"
  - What can be PHI.
- Media
- Organization's website
- Patient support groups
- Fundraising

18

Do your end users really know the limits of their access to PHI?

- Accessing under another person's username and password
- Minimum necessary
- Creating and/or using generic usernames and passwords
- Using more than one username and password for different hats the user might wear.
- Taking data when the person leaves your organization.
  - Data sets
  - Trainee documentation

19

Sharing information with business associates

- Does the business owner know
  - when a BAA is necessary?
  - understand what can be shared with a BA?
  - What needs to happen when the BA relationship ends?
  - What to do if a BA notifies the covered entity of a data compromise?

20

Training and Education

- Uses and disclosures for training and education
  - What can be access for educating your workforce?
  - What can be access for training others?
- Training and education on appropriate uses and disclosures
  - Frequent short snippets
  - Examples that impact the workforce directly

21

22

Using and disclosing information for research

- Who "owns" the PHI?
- Who "owns" the research data?
- Ensuring that documents are consistent
- Understanding the workflow for accessing information

23

Who "owns" the PHI?

- The PHI collected about a patient is usually owned by the organization not the clinician.
- When the clinician is accessing information for a research purpose they must fit a research exception or have a valid authorization from the patient/subject.
  - A valid informed consent is not sufficient unless it contains the elements of a valid authorization

24

Who "owns" the research data?

- Not all individually identifiable health information (IIHI) used or disclosed for research is PHI.
- If the organization is split, the IIHI held by the covered entity is PHI but the IIHI held by the research component is not.
- Depending on the sponsorship of the research the data may be owned by
  - The organization
  - The sponsor
  - Jointly
- A researcher may not be able to take PHI or IIHI with them if the move to another organization

25

Ensuring that documents are consistent

- Comparing the ICF, research protocol, and HIPAA authorization
  - Do they reference the same information?
  - Are they consistent regarding
    - sharing information?
    - Protections of information?
- Consistency between the waiver of authorization application, research protocol, and request for data from the covered entity.

26

Understanding the workflow for accessing information

- The clinician/researcher split personality.
- Just because you can does not mean you should.
- Who is evaluating the documentation to ensure appropriate sharing?
  - Waiver of authorization terms
  - Authorization terms

27

28

Privacy laws – staying current

- California Consumer Privacy Act
- General Data Protection Regulations
- What is Washington doing?
- Other states

29

California Consumer Protection Act

- Effective January 1, 2020
- Gives California consumers rights with respect to their personal information
- A consumer is defined broadly to include employees/families, prospective customers contacting us through their job, applicants for employment
- Applies to for-profit businesses with California presence that;
  - Have gross revenue in excess of $25 million; or,
  - Buy, receive, sell, or share for commercial purposes the personal information of 50,000+ California consumers, households, or devices; or,
  - Derive 50% or more of its revenues from selling personal information

30

4 Basic Privacy Rights Given to California Consumers

- The right to know what personal information a business has collected about them, where it was sourced from, what it is being used for, whether it is being disclosed or sold, and to whom it is being disclosed or sold
- The right to "opt out" of allowing a business to sell their personal information to third parties
- The right to have a business delete their personal information; and
- The right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act.

Health Care Exemptions in the CCPA

HIPAA COVERED ENTITIES

ENTITIES COVERED BY CALIFORNIA HEALTH CARE PRIVACY LAW (CMIA)

BUSINESS ASSOCIATES FOR ACTIVITIES COVERED BY HIPAA

NON-HIPAA COVERED PII HELD BY A COVERED ENTITY SAFEGUARDED TO SAME EXTENT AS PHI

UNDERSTANDING OF IMPACT IS EVOLVING

- Effective May 25, 2018
- Protects information of EU residents
- Applies to an entity operating
  - Within the EU
  - Outside of the EU that processes personal information of an individual physically in the EU if it
    - Offers goods or services to such individual
    - Monitors the behavior of such individual
- Personal data in information, documents or electronic data related to an identified or identifiable natural person
  - This is a person who can be identified directly or indirectly

General Data Protection Regulations

33

- Two types of data handlers applies to:
  - Controllers
    - Entity or person that determines the purpose and means of processing of personal data
    - This might include a sponsor, PI, or primary research site
  - Processors
    - Covered by GDPR when engaged by a controller to provide data processing services.
- Special rule for transferring personal information outside the EU

General Data Protection Regulations

34

- Processing is any operation performed on personal data including collecting the information.
- Must have consumer's consent before data is collected or shared
- Consent must be explicit i.e. checking a box or something similar to opt-in
- Breach reporting
  - Must notify regulator without undue delay
    - Notice should be no later than 72 hours after awareness of incident
  - Notice to the individual only if likely to be high risk to the individual's rights and freedoms

General Data Protection Regulations

- Anonymization
  - direct and indirect identifiers removed
  - Technical safeguards added
  - Zero risk of re-identification
- Pseudonymization
  - Processing of personal data in a way that it cannot be linked to a specific subject without the use of additional information
    - Honest Broker concept
  - Coded data is identifiable personal data under GDPR
  - Coded data where the research team does not have access to the code is not PHI under HIPAA

General Data Protection Regulations

What is Washington State doing?

- Proposed legislation that would be similar to the CCPA and GDPR
  - Failed to pass in the past two attempts
- Washington Uniform Health Care Information Act 70.02 RCW
- Breach notification changes
  - Expands definition of personal information
  - Changes requirements of notification content
  - 30 days to report
  - Not applicable to HIPAA covered entities as it relates to PHI

37

Other state privacy laws and activities

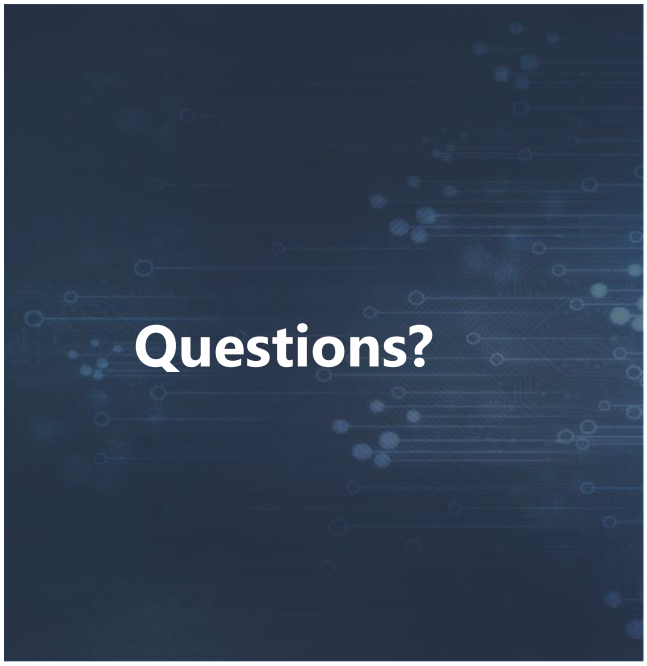
State attorneys general (AGs) are bringing enforcement actions to protect consumer information from unauthorized disclosure.

AGs in Massachusetts, New York, and New Jersey have been extremely aggressive.

Millions of dollars in settlements from healthcare systems and an assortment of IT services vendors for failing to safeguard data containing sensitive personal information.

PA Supreme Court found a Common Law duty to use reasonable safeguards to prevent its theft or unauthorized access.

38



Thank You!

Marti Arvin
Executive Advisor
Marti.Arvin@CynergisTek.com
+1 (512) 402-8550 x7051

Follow Us:

twitter.com/cynergistek
youtube.com/cynergistek
facebook.com/cynergistek/
linkedin.com/company/cynergistek-inc-/