Privacy is the New Security: Why Privacy Risks are Overshadowing Security Risks

Presented by:

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC

Vice President of Audit Strategy

CYNERGISTEK

CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

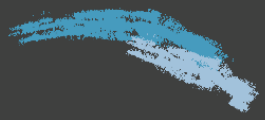
CynergisTek has been recognized by KLAS in the 2016 and 2018 Cybersecurity report as a top performing firm in healthcare cybersecurity.

1

Today's Agenda

1. Common Privacy Risks
2. Privacy outside of healthcare
3. Questions

Common Privacy Risks



CYNERGISTEK

3

Common Privacy Risks

- Improper accesses by employees
- Lost or stolen devices
- Cloud storage
- Social determinants of healthcare

CYNERGISTEK

4

Improper access by employees

- Organizations are still reporting instances were employees are accessing PHI for non-work related reasons
  - Family members
  - Friends
  - Co-workers
  - VIPs and Persons of Interest

5

User access monitoring

- Most organizations are not following the security rule that requires monitoring of access logs for all systems containing PHI.
- For those that do, their process if often not robust.

6

Lost or stolen devices

- Unsecure lost or stolen devices continues to be a top basis for privacy notifications
- Organizations have an extremely difficult time controlling BYOD.
- The storage capacity of such devices continues to grow

Cloud storage

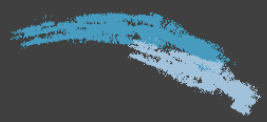
- Difficult to get BA with cloud vendors
- User set-up is the greatest risk even with a BA
- Cross border issues of cloud storage
- Employees are still using their own cloud services
  - Easier
  - Less expensive

Social determinants of healthcare

- More hospitals and health systems are working with external entities to resolve social determinants of healthcare
  - Living conditions
    - Eviction concerns
    - Unsafe living conditions
  - Nutritional issues
    - Lack of food
    - Lack of nutritional food

9

Current State of Privacy: Healthcare and Beyond



10

Current State of Privacy

- HIPAA Privacy and Breach Notification Rules set bright line standards for most health care providers, insurers and vendors
- GDPR influencer of development of new federal and state privacy schemes but has had limited impact on U.S. healthcare organizations
- All states and territories have breach notification requirements to notify consumers when data compromised
- 22 states have laws that protect health information and personal information more broadly than HIPAA or other federal standards
- California to require businesses to give consumers notice and choice when personal information collected and shared

CYNERGISTEK

11

Forces Driving Privacy Regulation

- GDPR—Broad principles establishing data privacy and security across the EU
- Protects all personal information in all settings
- Application to a broad section of U.S. companies
- Health care industry simply part of the overall scope of regulation
- Health care data considered sensitive with certain special restrictions

CYNERGISTEK

12

Impact of GDPR

- Limited impact on majority of domestic healthcare industry
  - Most physicians, hospitals, and health insurers do not collect the personal information of EU citizens except when they have encounters while visiting the U.S.
- GDPR does have implications for certain kinds of U.S. health care companies like pharmaceutical companies and bio/genetic testing firms
- Big impact for global or multinational companies servicing healthcare industry
  - Tech companies, managed business services, corporate parent or subsidiary in Europe

CYNERGISTEK

13

GDPR Challenges

- How best to comply with GDPR
- Isolating EU personal info subject to GDPR?
- Whether to apply GDPR for all activities including those outside of EU?
- Related issues involving data transfer from EU and mechanisms set up to facilitate movement of protected information
  - Privacy Shield and Model Contract Clauses
- What about Brexit?
  - If organization is multinational…monitor need to comply with UK laws

CYNERGISTEK

14

States Changing Definition of Health Information

- HIPAA applies to a defined set of information when created or maintained by a limited set of organizations
  - Covered entities
    - Group health plans, insurers and other payers
    - Healthcare providers that bill Medicare, insurance & health plans electronically
    - Healthcare clearinghouses
  - Business associates
    - Contractors & vendors of CEs who create, maintain or transmit PHI
- States broadly defining PII held by data owner or data processor

CYNERGISTEK

15

States Taking Action

State attorney generals (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.

CYNERGISTEK

16

States Taking Action

AZ appellate court said HIPAA is the standard for negligence

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

CYNERGISTEK

17

50 Shades of Breach

- Research and review the laws in each state in which your organization does business or holds the PII of a state's residents.
  - How does that state define PII?
  - What is a "breach" and when is the breach reportable; who must receive notification; and, when must notifications be made?
  - What are the applicable state data protection or data disposal standards?
  - Are there industry specific cybersecurity program requirements (e.g. MI, MS, NY, OH, SC)?
  - How do state laws and requirements apply to 3rd party vendors when they maintain data PII?

CYNERGISTEK

18

Develop Situational Awareness

- Identify and inventory what PII is created, transmitted or maintained by, or on behalf, of your organization.
  - Include data in all forms and from any source (e.g. employees, patients or enrollees, online marketing, or website tracking).
  - What is the state of residency for each individual that has contributed PII?
  - It may be necessary to refer to state specific definitions of "what is PII?" to perform a complete inventory.

CYNERGISTEK

19

California as a Driving Force

- Dozens of laws dealing with privacy & security last 15 years
- Some are never heard from again
- Some don't get passed elsewhere but have broader implications (e.g. website privacy policies) or become national models (e.g. data breach notification, protecting SSNs)

CYNERGISTEK

20

California Consumer Protection Act

- Goes into effect 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

CYNERGISTEK

21

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.

CYNERGISTEK

22

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

UNDER-STANDING OF IMPACT IS EVOLVING

CYNERGISTEK

23

Compliance Challenges

- Assessing if your organization has a for-profit member or data controller in its family tree
- Identifying California residents
- Single national approach or California specific?
- Developing operations that can adjust for those residents who exercise rights
- Understanding what entities in health care and using health care information are covered or not

CYNERGISTEK

24

Drivers for National Privacy Legislation

- Series of ongoing cyber attacks and security breaches – mostly not involving health care
  - Uber, Facebook, Exquifax, Yahoo, Marriott/Starwood, FEMA
- Recognition of the growing gaps in the reach of non-HIPAA information through proliferation of websites, mobile apps and wearables handle more health information
- Expanded use of employer wellness programs that employ data from social media and employee health data

CYNERGISTEK

25

Aggregating Data for New Uses in Healthcare

- "When a Health Plan Knows How You Shop." (New York Times)
  - Health plan prediction models using consumer data from data brokers (e.g., income, marital status, number of cars), to predict emergency room use and visits to urgent care.
- "Tracking Your Pregnancy on an App May Be More Public Than You Think" (Washington Post)
  - As apps help moms monitor their health proliferate, employers and insurers pay to keep tabs on the vast and valuable data to identify high risk pregnancies, premature births, the top medical questions researched or when new moms planned to return to work.

CYNERGISTEK

26

Health Care in the National Debate

- Sector specific approach dealing with issue of non-HIPAA health data not on the table Congress will not expand HIPAA
- Health care industry – regulated by HIPAA – could be left alone by exemption from application of national law, similar to CCPA
- New provisions could apply to HIPAA entities – layered on top of HIPAA

CYNERGISTEK

27

Possible Outcomes

- New provisions likely would cover non-HIPAA health care data, and entities that handle that data
- Could lead to different standards
- Overlap issue of pre-emption – would health care industry want to be covered if strong preemption of state law?
- New national law could replace HIPAA entirely
- Nothing changes

CYNERGISTEK

28

Key Issues To Watch

- Pre-emption of state laws
- Consumers with Private Right of Action
- Scope of individual rights
- Permitted disclosures vs. areas where permission from consumers is needed
- Enforcement and by who

CYNERGISTEK

29

Looking Into My Crystal Ball

- Not likely to have national privacy or breach notification legislation in this Congress
- States will not wait for Congress, continuing to expand the definition of PII and setting additional breach notification requirements
- Look for more states to adopt NAIC's Uniform Cybersecurity Programs for Insurers
- If 3-5 influential states pass "California-like" laws, will the tech industry unify its support for a federal law to push Congress into action?

CYNERGISTEK

30

Thank You!


Questions?
Marti Arvin
Executive Advisor
marti.arvin@cynergistek.com
512.450.8550 x7051