CE876 - Information Security Mng. & Eng.

Lecture 13: Sector Specific Security Standards

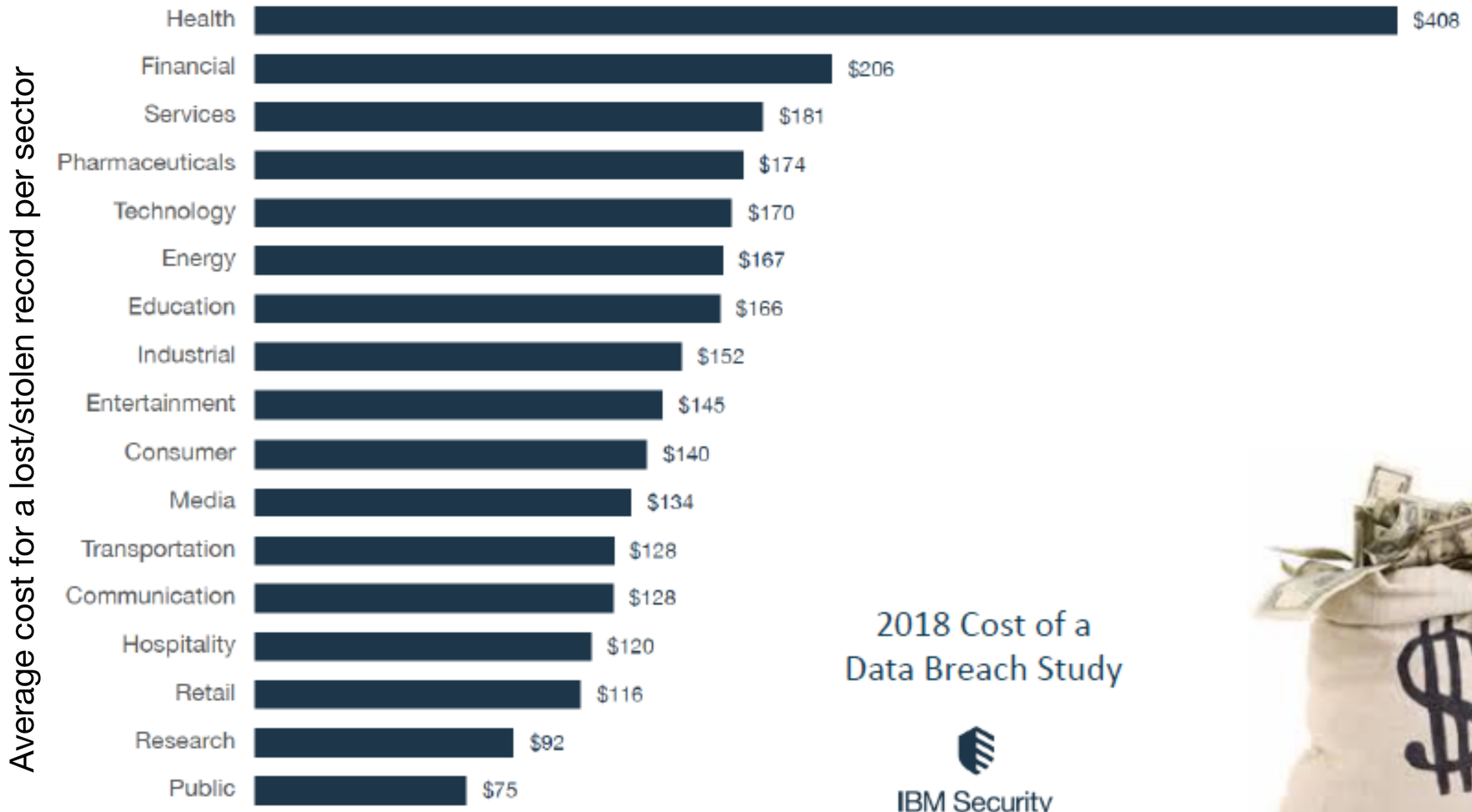
Seyedeh Atefeh Musavi / Mehdi Kharrazi
Department of Computer Engineering
Sharif University of Technology
Spring 1400

S4Lab

Acknowledgments: Some of the slides are fully or partially obtained from other sources. A reference is noted on the bottom of each slide to acknowledge the full slide or partial slide content.

Not all sectors are equal

S4Lab



2018 Cost of a Data Breach Study

IBM Security

[Curex: Secure and Private Health Data Exchange, Chrisos Xenakis, Int. Workshop on security and privacy in healthcare, 2019]

Agenda

S4Lab

- Today we will review two well-known health sector standards
- HIPAA
- HITRUST Common Security Framework

HIPAA

- Health Insurance Portability and Accountability Act (1996)
- Covers both privacy and security of PHI (protected health information)
  - Security rule
    - How to apply CIA
    - Include administrative, technical, and physical safeguards
  - Privacy rule
    - How to disclose/use PHI
- Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.
- Requirements for all forms of PHI
  - Including paper, oral and electronic, etc.

[Image: https://www.e-commercealert.com/article338.shtml]

[HIPAA: The Security Rule, Health Information Privacy U.S. Department of Health & Human Services, 2020]

A great difference

S4Lab

- In general, you may use or disclose protected health information for treatment, payment, and health care operations without obtaining a patient's written permission.
- For other purposes, such as marketing, you may need to obtain an individual's authorization to use or disclose the patient's protected health information.
- Your agreements with business associates must explicitly require them to comply with HIPAA, including breach notification requirements.

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

Types of Data Protected by HIPAA

S4Lab

- Written documentation and all paper records.
- Spoken and verbal information including voice mail messages.
- Electronic databases and any electronic information, including research information, containing PHI stored on a computer, smart phone, memory card, USB drive, or other electronic device.
- Photographic images.
- Audio and Video recordings.
- …

[HIPAA Privacy and Security Annual Renewal Training For Employees, University of Alabama, 2018]

Rules for covered entity

S4Lab

- As a covered entity, you have responsibilities to patients under the HIPAA Privacy Rule, including:
  - Notice of privacy practices
  - Patient access to their information
  - Amending patient information
  - Accounting of disclosures
  - Rights to restrict information

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

Administrative safeguards

S4Lab

- Security management processes to identify and analyze risks to e-PHI and implementing security measures to reduce risks.
- Staff training to ensure knowledge of and compliance with your policies and procedures.
- Information access management to limit access to electronic health records to protect health information, including the information in EHRs.
- Contingency plan to respond to emergencies or restore lost data.

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

Physical safeguards

S4Lab

- Facility access controls, such as locks and alarms, to ensure only authorized personnel have access into facilities that house systems and data.
- Workstation security measures, such as cable locks and computer monitor privacy filters, to guard against theft and restrict access to authorized users.
- Workstation use policies to ensure proper access to and use of workstations.

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

Technical safeguards

S4Lab

- These safeguards include hardware, software, and other technology that limits access to e-PHI.
- Examples of required technical safeguards include:
  - Access controls to restrict access to PHI to authorized personnel only
  - Audit controls to monitor activity on systems containing e-PHI, such as an electronic health record system.
  - Integrity controls to prevent improper e-PHI alteration or destruction.
  - Transmission security measures to protect e-PHI when transmitted over an electronic network.

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

From stakeholders POV

S4Lab

- Let’s see the HIPAA from a different points of view
- Who are the HIPAA’s stakeholders other than patients?

From stakeholders POV

S4Lab

- Let’s see the HIPAA from a different points of view
- Who are the HIPAA’s stakeholders other than patients?
- **Hospitals**
  - Hosting and being responsible for healthcare datasets.
- **Research Centers**
  - Use an individual’s data, in particular biomedical data, for scientific research purposes.
- **Private Businesses and Other Organizations**
  - Industrial research enterprises & commercial enterprises.

[Implementació de Projectes Europeus en Ciberseguretat, Liobet D. N., Jofre M., Hospital General de Granollers, 2021]

HIPAA costs

- The costs associated with HIPAA depend on the type and size of the business.
  - For example, it would cost more for a big hospital to be compliant than for a small clinic or clearinghouse.
- It also depends on the culture and the business environment.
  - A business that depends heavily on Internet technology for data transactions, with conservative views on privacy and security, would likely spend more on its compliance efforts.
- The cost can be divided into one time or reoccurring costs.
  - Big hospitals may hire lawyers, consultants, vendors, and technical writers to work on HIPAA compliance. These costs would be one time.
  - The recurring costs include collection of confidential trash for shredding, disaster recovery services and/or offsite storage for backup media, printing, and mailing costs of Notice of Privacy Practices to patients, routine privacy auditing and monitoring activities, computer system updates and remediation, and training related costs.

[HIPAA security compliance challenges: The case for small healthcare providers, Chen, J. Q., & Benusa, A., International Journal of Healthcare Management, 2017]

Challenges for Small Health Care Provider

S4Lab

- The expertise needed for implementing and maintaining HIPAA compliance includes general IT skills, knowledge in healthcare IT products and services, and deep understanding of the regulatory requirements.
- None of the mentioned technical skills are readily available in typical small healthcare providers.
- IT staffing is the last thing on their minds because they do not have the financial resources to acquire IT personnel with the right set of skills, nor the scale of economy justify such hiring.

Small Health Care Provider Fails to Implement Multiple HIPAA Security Rule Requirements

Metropolitan Community Health Services (Metro), doing business as Agape Health Services, has agreed to pay $25,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Metro is a Federally Qualified Health Center that provides a variety of discounted medical services to the underserved population in rural North Carolina and these facts were taken into account in reaching this agreement.

[Image: https://www.hhs.gov/]

[HIPAA security compliance challenges: The case for small healthcare providers, Chen, J. Q., & Benusa, A., International Journal of Healthcare Management, 2017]

During the COVID-19 national emergency

S4Lab

- OCR (Office for Civil Rights) will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. This notification is effective immediately.
- A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients.
- Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

[Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, HIPAA, Health Information Privacy U.S. Department of Health & Human Services, 2020]

Another challenge: HIPAA updates

S4Lab

- Keeping up with the changing regulatory requirements is a big challenge.
- As the technology and security landscape keep evolving, the U.S. Congress passes new laws or modifies existing laws to strengthen health information protection or to mend the loop holes.

[HIPAA security compliance challenges: The case for small healthcare providers, Chen, J. Q., & Benusa, A., International Journal of Healthcare Management, 2017]

An example

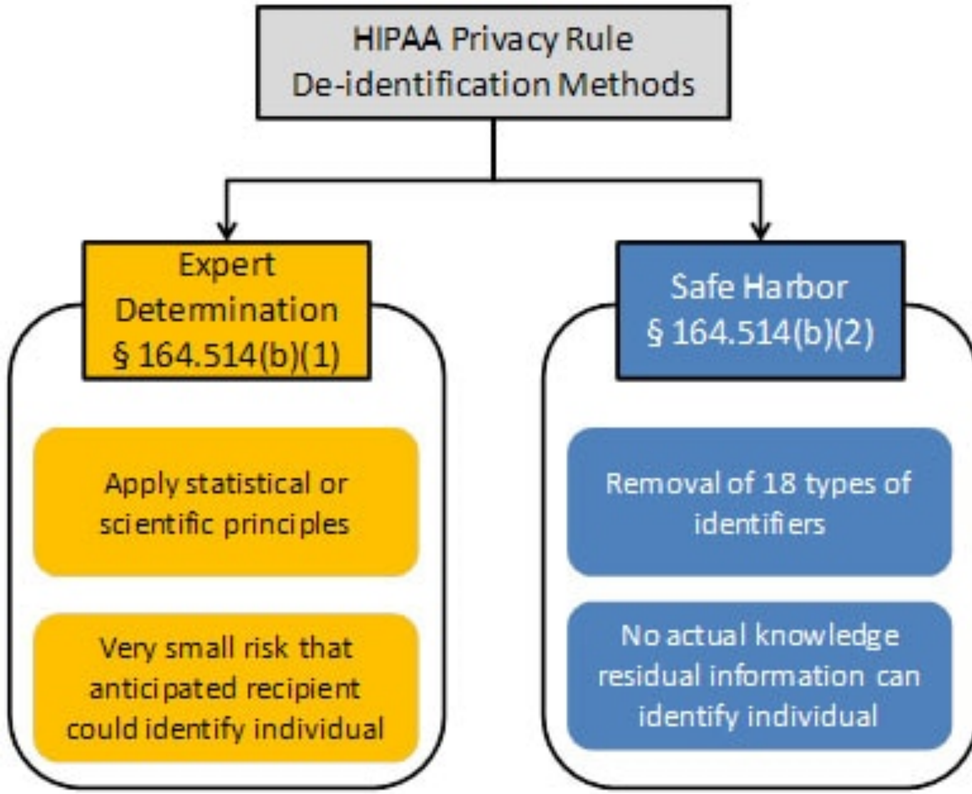
- RegEye (an Ophthalmology and Optometry practice) recently upgraded the operating system on all its workstations to Windows 10. Such a seemingly routine upgrade involved many hours of research and remedies in security.
  - For example, by default settings of many Windows 10 new features, data and settings are automatically backed up or sent to remote servers owned by Microsoft.
- Bitlocker in Windows 10 will automatically backup user's encryption key to OneDrive; Data Sync allows the operating system to sync settings and data into Microsoft's remote servers.
  - If those default settings are not changed, the business is at risk of violating HIPAA privacy and security rules.

[HIPAA security compliance challenges: The case for small healthcare providers, Chen, J. Q., & Benusa, A., International Journal of Healthcare Management, 2017]

De-Identification.

S4Lab

- HIPAA Rules do not govern the use or disclosure of health information that does not identify an individual.
  - You can share de-identified PHI, but just removing name, address, and social security number may NOT make information “de-identified”.
  - The Privacy Rule designates two processes through which a covered entity can determine that protected health information is de-identified.
- Re-identification should also be cared for.



[Image: https://www.hhs.gov/]

[Guide to Privacy and Security of Health Information, The Office of National Coordinator for Health Information Technology, 2015]

Mere conduits

S4Lab

- Those entities that serve as “mere conduits” for the transmission of protected health information (PHI) are not subject to HIPAA liability and obligations as business associates (BAs).
  - An entity that maintains [PHI] on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the [PHI].
  - Physical courier services such as the US Postal Service and UPS as well as their “electronic equivalents”.

[HIPAA Final Rule Confirms That ISPs Transmitting PHI Are Not Business Associates, Joseph Lorenzo Hall , CDT, 2013]

Mere conduits (2)

S4Lab

- There had still been some concern about whether an entity providing PHI transmission services to a HIPAA-covered entity would be considered a BA (business associates).
- Providers of transmission services, including ISPs, faced inconsistent interpretations that created an uncertain playing field:
  - If these service providers wanted to handle traffic from hospitals and doctors offices, which would undoubtedly include PHI, would they need to treat those transmissions differently or otherwise modify their business to comport with HIPAA?
  - 2013 Rule update: “business associate” includes any person that “provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information ” (emphasis added).
- Historically, some cloud service providers were able to absolve themselves from any HIPAA responsibilities by claiming the “Conduit Exception Rule”.

[HIPAA Final Rule Confirms That ISPs Transmitting PHI Are Not Business Associates, Joseph Lorenzo Hall , CDT, 2013]

Is there any missing point?!

S4Lab

“HIPAA is not an overall health information privacy law. There have always been gaps in what was covered by HIPAA”

Kirk Nahra, Partner, WilmerHale Law Firm.

[Entities Deal With More Data Outside HIPAA; ‘We Are Seeing Tensions’, Nina Youngstrom, HCCA, 2021]

Not always applicable

S4Lab

- When employees are required to show their employers proof of a positive COVID-19 test before they get sick leave or a vaccination before returning to work, the implications are profound—but they don't enter the realm of the HIPAA privacy rule.

[Entities Deal With More Data Outside HIPAA; 'We Are Seeing Tensions', Nina Youngstrom, HCCA, 2021]

Wellness data vs health data

S4Lab

- The development of the quantified self movement (the trend of constant self-measurement) challenges classical approach to protect health data has been through strict anonymization or de-identification rules.
- In the domain of health, “wellness data” does not always constitute health data in the existing legal framework
- But could reveal medical or personal information and therefore needs to be adequately protected.
- Regulating this new category of data requires new perspectives on the issue of personal data protection that can better inform the corporate governance of data flows.
- Indeed, beyond states and Individuals, companies hold increasing amounts of the data that is and will be created.

[A Purpose-Based Taxonomy for Better Governance of Personal Data in the Internet of Things Era: The Example of Wellness Data, Levallois-Barth, C., & Zylberberg, H., In Data Protection and Privacy: (In)visibilities and Infrastructures, 2017]

Google Project Nightingale

S4Lab

- In 2019 hospital chain Ascension (the second-largest U.S. healthcare system) was partnering with google in project Nightingale.
- The health system will use google's cloud platform and g-suite patient records, which allows google to have access to patient records from ascension hospital patients in 21 states.
- In the eight months since Nightingale launched, Ascension has shared an estimated 50 million patient files from 21 states with Google.
- Under Google's interpretation, the company is merely a "business associate" helping Ascension better render its services—and thus warrants a different level of scrutiny than an actual health-care provider.

[Google's Nightingale Health Record Project Legal Under HIPAA, but Privacy Concerns Mount, eccovia, 2020]

[Google's Totally Creepy, Totally Legal Health-Data Harvesting, Sidney Fussell, The Atlantic, 2019]

[Entities Deal With More Data Outside HIPAA; 'We Are Seeing Tensions', Nina Youngstrom, HCCA, 2021]

QA