HIPAA, FERPA, PCI OH MY!

Jerry Smith
Information Security and Privacy Analyst
Privacy Office
Compliance Services
University of Utah Health
515 East 100 South, Suite 650
Salt Lake City, UT 84124
Jerry.Smith@Utah.edu

DISCLAIMER

I AM NOT AN ATTORNEY.

I AM NOT PRESENTING ANY LEGAL ADVICE. THIS INFORMATION IS BEING PRESENTED AS IS AND COMES FROM MY EXPERIENCE WORKING IN THE CONTEXT OF THE UNIVERSITY OF UTAH. WHAT YOU DO IN YOUR ORGANIZATION IS UP TO YOU. PLEASE SPEAK TO YOUR ORGANIZATIONAL IN HOUSE COUNSEL OR EXTERNAL COUNSEL FOR INFORMATION SPECIFIC TO YOUR ORGANIZATION.

FERPA

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

FERPA

- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

FERPA

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

FERPA

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

HIPAA

- Are you a Covered Entity (CE)?
- Do you transmit health care information in electronic form in a transaction covered by Section 160.103 of Title 45 CFR?
- Are you a healthcare clearing house?
- Are you a health plan?
- If none of these terms listed above does not any make sense, stand up and run to the nearest exit!

2017 HIPAA Enforcement Fine #1 – Lack of Timely HIPAA Breach Notification – $475,000 – Presence Health - Illinois

2017 HIPAA Enforcement Fine #2 – Failure to Conduct a HIPAA Risk Analysis and Implement Safeguards – $2,200,000 – MAPFRE Insurance Puerto Rico

Total fines for 2016 was $23.5 million. That was just for the fines, that did not include remediation and or corrective action plans.

Advocate Health Care Network - Illinois

Advocate Health Care Network (Advocate) had the largest OCR HIPAA settlement to date at the time of publication, with a $5.55 million agreement.

The Illinois-based healthcare system faced multiple alleged HIPAA violations and noncompliance issues. Advocate submitted three data breach notification reports to HHS between August 23, 2013 and November 1, 2013.

We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure," OCR Director Jocelyn Samuels said in a statement. "This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

PCI

- Oh wait! Before you run out, that was only one of the regulatory items that I was going to discuss today.
- Do you process credit card or payment card transactions?
- Better sit back down.
- What merchant level are you? How many transactions do you do in a year?

PCI

- Are you level 3 or 4?
- Still do your own self assessments, SAQ's?
- Have you ever had a breach?

  I hope not, wait a few minutes to find out more
- When do the new rules go into effect?

  February 1, 2018

PCI

- How much is Target going to pay MasterCard for their breach?

  $19 Million

- What is the number of transactions that move you from Level 2 to Level 1?

  6 Million

- Have you segmented your CDE from the rest of your environment?

In all, according to Target Corporation's most recent Form 10-K, through the end of 2016 Target had incurred $292 million of cumulative expenses related to the data breach, which after receipt of $90 million in insurance proceeds, resulted in total net expenses to Target from 2013-2016 of about $202 million. This settlement pushes the total cost to Target of the data breach to over $220 million. In addition, a multi-district consumer class action remains pending.

Where is My Stuff?

HIPAA PCI FERPA

©UNIVERSITY OF UTAH HEALTH, 2017

DATA

- **Where is my stuff?**
- We have been talking about the regs now we need to talk about the data. Where is it in the organization. We need to find it in the organization and find out where it resides. Sometimes that can be easy and sometimes it can be harder than you think, however, we want to make sure we know exactly where it all is located.

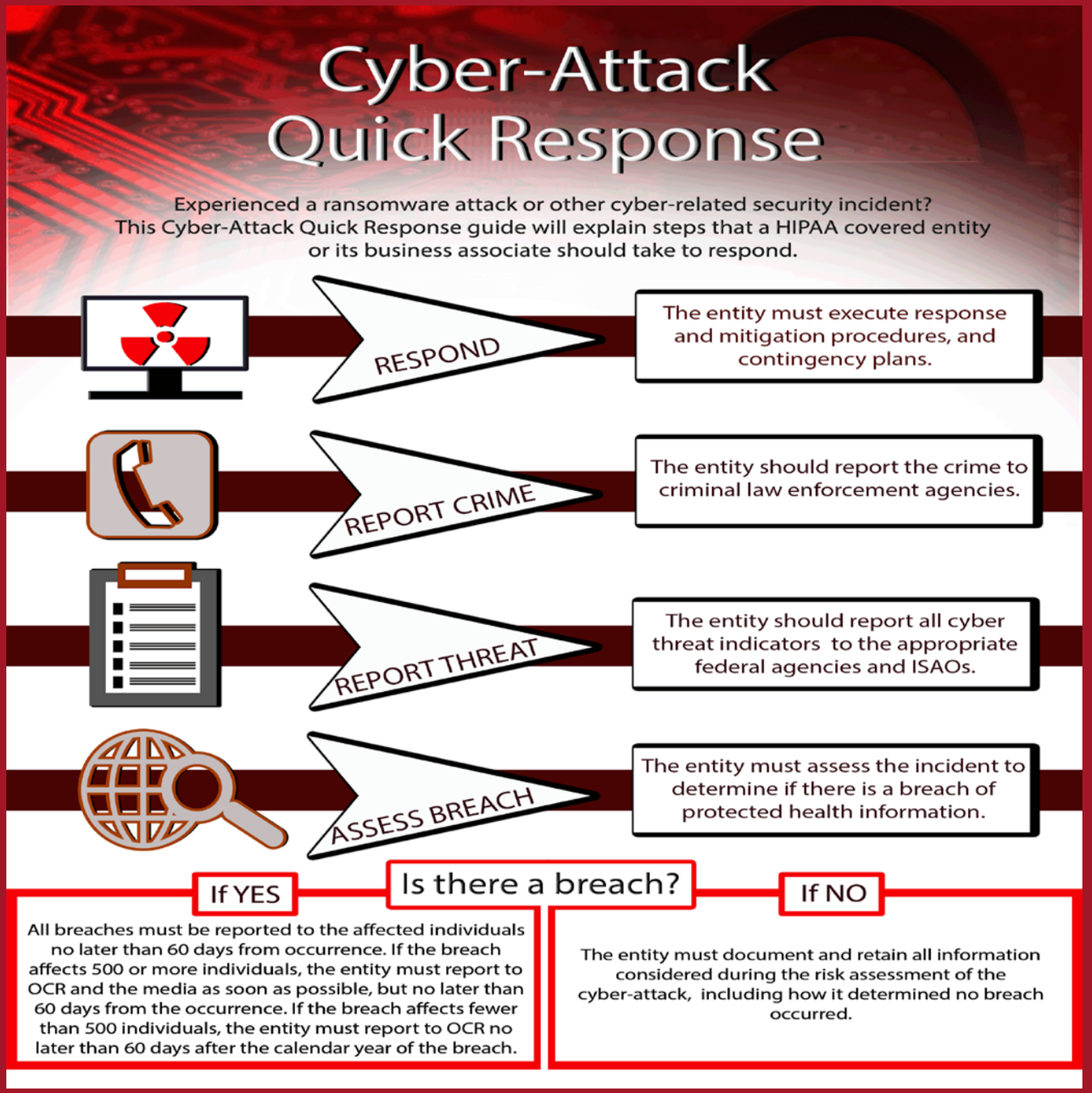
DATA

- Data at rest – are you encrypting?
- If not, are you considering encrypting?
- If you are not considering encrypting, is there a chance that you could reconsider and think about it again?
- If there is no chance that encryption is not a project for your regulated data in the near future, you need to rethink that and try to get encryption into your environment! This is for data on the wire and data at rest!

INCIDENT RESPONSE

- Do you have an incident response plan?
- Does it contain these components or something similar?
- Preparation/Prevention
- Detection
- Containment
- Eradication
- Recovery/Return to Service/Notify

HHS CYBER-ATTACK QUICK RESPONSE



HEALTH
UNIVERSITY OF UTAH

HIPAA BREACH

- Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals, and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting.

HIPAA BREACH

- OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach.

HIPAA BREACH

- An entity that discovers a breach affecting fewer than 500 individuals has an obligation to notify: individuals without unreasonable delay, but no later than 60 days after discovery; and OCR within 60 days after the end of the calendar year in which the breach was discovered.

RISK ASSESSMENT

- Breach Risk Analysis:
- Factor 1: Nature/extent of PHI involved, types of identifiers, and re-identification risk
- Factor 2: Unauthorized user or unauthorized recipient
- Factor 3: Was PHI actually accessed or used?
- Factor 4: Extent risk to PHI has been mitigated (NDA)

PCI BREACH

A data breach now costs organizations an average total of $3.8 million (over €3.3 million). Is your business prepared to mitigate a compromise and its impact on your bottom line and reputation? Research shows that having an incident response team in place can provide significant savings.

PCI BREACH

- In the event of a PCI Breach, you probably will need to bring in a PCI Forensic Investigator.
- https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
- You also will move to a Level 1 which means third party audits, expensive!

- **Questions?**