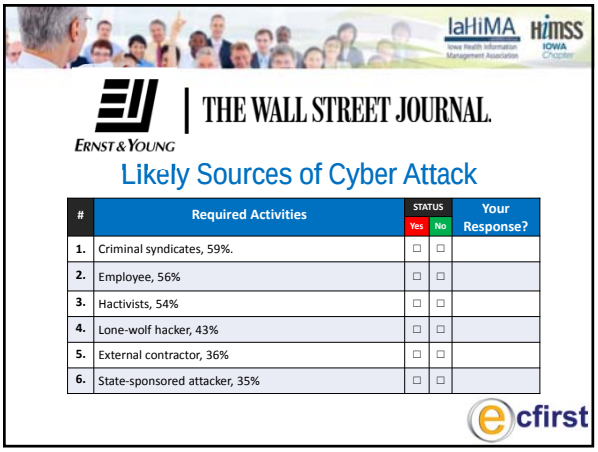
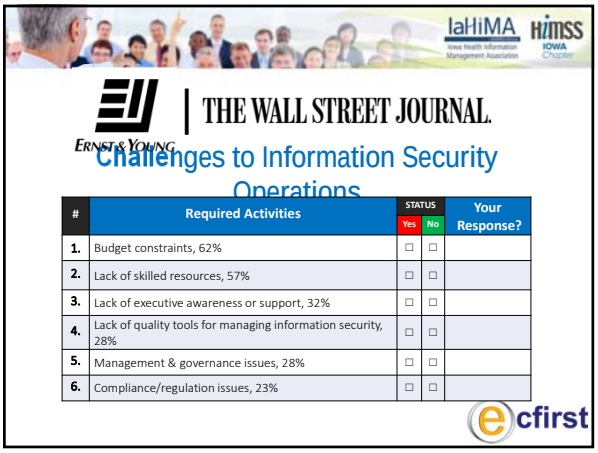
Healthcare Cyber Risk = Business Risk





Healthcare Cyber Risk = Business Risk

Cyber Soft Spots: Prepared?

THE WALL STREET JOURNAL.

Hackers Exploit Staffers!

- Social media posts give hackers valuable info
- Phishing emails to gullible employees
- **Fake phishing email** sent by a large U.S. bank to its more than 100,000 employees resulted in a 20% click rate! *Average is a 2% click rate*
- 30% of data breaches result from employee error

"We spend an ocean of money on cyber security. It is the only expense where I ask if it's enough."
John Stumpf, Wells Fargo, Chief Executive

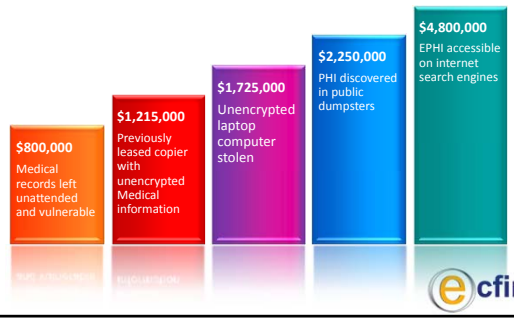
Encryption: Ready?

THE WALL STREET JOURNAL.

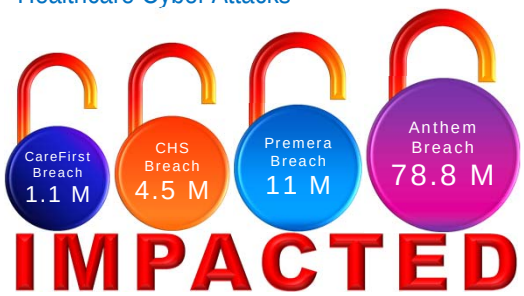
- **Largest Cyber Attack on Federal Data**
- **127-page Security Clearance Form Compromised**
- **22 Million People Impacted**

Many of the records held by the U.S. government's Office of Personnel Management were not encrypted. *PHOTO: BLOOMBERG NEWS*

Risk to a Healthcare Entity



Healthcare Cyber Attacks



Cost of Breaches: Eight Figure Risk!

Ransomware Attacks

Healthcare Cyber Risk = Business Risk

Entity: Hollywood Presbyterian Medical Center

Amount Demanded: $3.6 million in Bitcoin
Amount Paid: $17,000 in Bitcoins
Date of Incident: February 5, 2016
 # Impacted: None

- Malware locks systems at Hollywood hospital by encrypting files & demanded a ransom for the decryption key.
- Hollywood Hospital paid extortionists a $17,000 bitcoin ransom to unlock its data.
- Hackers had originally demanded $3.4 million from the Hollywood Presbyterian Medical Center.
- The hospital stated that patient's medical records were not accessed by the hackers at any point.

Entity: Prime Healthcare (CVMC & DVH)

Amount Demanded: Unknown
Amount Paid: Refused to pay ransom
Date of Incident: March 18, 2016
 # Impacted: None

- Ransomware attacks against hospitals are becoming common place in 2016.
- Chino Valley Medical Center (CVMC) & Desert Valley Hospital (DVH), both part of Prime Healthcare Services Inc., had systems compromised by a cyber attack.
- Hackers got into one of the hospital's computers & then spread a malware program to encrypt the data on computers.
- The hackers then demanded a ransom to unlock the servers.
- No ransom is believed to have been paid as Prime Healthcare had multiple levels of backup data, which was used to recover the data.
- News reports stated that the attack "did cause significant disruptions of IT systems".

Entity: Methodist Hospital

Amount Demanded: Unknown
Amount Paid: Refused to pay ransom
Date of Incident: March 18, 2016
 # Impacted: None

- Incident was a result of a malicious email that made it through the spam filter & was opened by a user.
- Methodist responded quickly to the virus and immediately shut down the system to control the virus from spreading.
- While the system was down, a backup system was activated.
- The backup system ran smoothly & allowed the hospital to continue its daily operations without interruption.
- No patient data or records were compromised.

Learning from Latest HIPAA Settlements

Entity: Feinstein Institute for Medical Research (FIMR)

Fine: $3.9 million
Duration of CAP: Three Years
Date of Fine: March 17, 2016
Date of Incident: September 2, 2012

- OCR's investigation began after Feinstein filed a breach report indicating that on September 2, 2012, *laptop computer with EPHI of ~13,000 patients & research participants was stolen from an employee's car.*
- EPHI stored in the laptop included the names of research participants, dates of birth, addresses, SSN, diagnoses, laboratory results, medications, & medical information relating to potential participation in a research study.
- *FIMR's security management process was limited in scope, incomplete, & insufficient to address potential risks & vulnerabilities to the CIA of EPHI held by the entity.*
- Feinstein lacked policies & procedures for authorizing access to EPHI by its workforce members; failed to implement safeguards to restrict access to unauthorized users, & lacked policies & procedures to govern the receipt & removal of laptops that contained EPHI into & out of its facilities.

Entity: Feinstein Cont'd..

Attestation:

- An attestation signed by an owner or officer of FIMR attesting that the Policies & Procedures are being implemented & have been distributed to all appropriate members of the workforce, & that FIMR has obtained all of the compliance certifications.
- An attestation signed by an owner or officer of FIMR attesting that all workforce members have completed the initial training required by this CAP & have executed the training certifications.
- An attestation signed by an owner or officer of FIMR listing all locations owned or controlled by FIMR, the corresponding name under which each location is doing business, the corresponding phone numbers and fax numbers, & attesting that each such location has complied with the obligations of the CAP.
- An attestation signed by an owner or officer of FIMR stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate & truthful.

Healthcare Cyber Risk = Business Risk

Entity: Feinstein Cont'd..

Attestation:

- An attestation signed by an owner or officer of FIMR attesting that it is obtaining and maintaining written or electronic training certifications from all workforce members that require training that they received training pursuant to the requirements set forth in this CAP.
- An attestation signed by an owner or officer of FIMR attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate & truthful.

OCR Guidance

- "Research institutions subject to HIPAA must be held to the same compliance standards as all other HIPAA-covered entities. For individuals to trust in the research process & for patients to trust in those institutions, they must have some assurance that their information is kept private & secure."

Entity: North Memorial Health Care

Fine: $1,550,000 **Duration of CAP:** Two Years

Date of Fine: March 16, 2016 **Date of Incident Report:** Sept. 27, 2011

- OCR initiated its investigation of North Memorial following receipt of a breach report, which indicated that an unencrypted, *password-protected laptop was stolen from a business associate's workforce member's locked vehicle, impacting the EPHI of 9,497 individuals.*
- North Memorial gave its business associate, Accretive Health, Inc., access to North Memorial's hospital database, which stored the EPHI of 289,904 patients.
- Accretive also received access to non-EPHI as it performed services on-site at North Memorial.
- North Memorial failed to complete a risk analysis to address all of the potential risks & vulnerabilities to the EPHI that it maintained, accessed, or transmitted across its entire IT infrastructure -- including but not limited to all applications, software, databases, servers, workstations, mobile devices & electronic media, network administration & security devices, & associated business processes.
- North Memorial is required to develop an organization-wide risk analysis & risk management plan.

Entity: North Memorial Cont'd..

Attestation:

- An attestation signed by an officer of North Memorial attesting that the policies and procedures and risk management plan: (a) have been adopted; (b) are being implemented; & (c) have been distributed to all appropriate workforce members.
- An attestation signed by an officer of North Memorial attesting that it has obtained & is maintaining written or electronic certifications from all workforce members that are required to receive training that they received the requisite training pursuant to the requirements set forth in this CAP.
- An attestation signed by an officer of North Memorial listing all of North Memorial's locations, the name under which each location is doing business, the corresponding mailing address, phone number and fax number for each location, & attesting that each location has complied with the obligations of this CAP.

Entity: North Memorial Cont'd..

Attestation:

- An attestation signed by an officer of North Memorial stating that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content, & believes that, upon such inquiry, the information is accurate & truthful.

OCR Guidance

- "Two major cornerstones of the HIPAA Rules were overlooked by this entity. Organizations must have in place compliant BAAs as well as an accurate & thorough risk analysis that addresses their enterprise-wide IT infrastructure."

Entity: Complete P.T., Pool & Land Physical Therapy, Inc. (CPT)

Fine: $25,000 **Duration of CAP:** Three Years

Date of Fine: February 16, 2016 **Date of Incident Report:** August 8, 2012

- On August 8, 2012, OCR received a complaint alleging that Complete P.T. had impermissibly disclosed numerous individuals' EPHI, when it posted patient testimonials, including full names and full face photographic images, to its website without obtaining valid, HIPAA-compliant authorizations.
- Complete P.T.:
  - ❑ Failed to reasonably safeguard EPHI;
  - ❑ Impermissibly disclosed EPHI without an authorization; and
  - ❑ Failed to implement policies and procedures with respect to EPHI that were designed to comply with HIPAA's requirements with regard to authorization.

Entity: CPT Cont'd..

Attestation:

- An attestation signed by CPT's owner attesting that the Policies and: (a) have been adopted; (b) are being implemented; (c) have been distributed to all members of the workforce; & (d) that CPT obtained all the compliance certifications.
- An attestation signed by the owner of CPT attesting that all members of the workforce have completed the initial training required by this CAP & have executed the training certifications.
- An attestation signed by the owner of CPT listing all CPT locations, the corresponding name under which each location is doing business, the corresponding phone numbers & fax numbers, & attesting that each location has complied with the terms of the CAP.
- An attestation signed by CPT's owner or designee stating that they have reviewed the Implementation Report, have made a reasonable inquiry regarding its content & believe that, upon such inquiry, the information contained therein is accurate, truthful, & complete.
- An attestation signed by CPT's owner or designated Privacy Officer attesting that it is obtaining & maintaining written or electronic training certifications from all workforce members & that such persons received training pursuant to the requirements set forth in this CAP.

Healthcare Cyber Risk = Business Risk

Entity: CPT Cont'd..

Attestation:

- An attestation signed by CPT's owner or designated Privacy Officer attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate, truthful, & complete.

OCR Guidance

- "The HIPAA Privacy Rule gives individuals important controls over whether & how their PHI is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her PHI can be made for marketing. All covered entities, including physical therapy providers, must ensure that they have adequate policies & procedures to obtain an individual's authorization for such purposes, including for posting on a website &/or social media pages, & a valid authorization form."

Entity: University of Washington Medicine (UWM)

Fine: $750,000 **Duration of CAP:** Two Years

Date of Fine: December 15, 2015 **Date of Incident:** Nov. 27, 2013

- OCR initiated its investigation of the UWM following receipt of a breach report, which indicated that EPHI of approximately 90,000 individuals was accessed after *an employee downloaded an email attachment that contained malicious malware*.
- The malware compromised the organization's IT system, affecting the data of two different groups of patients:
  - ❑ Approximately 76,000 patients involving a combination of patient names, medical record numbers, dates of service, and/or charges or bill balances; &
  - ❑ Approximately 15,000 patients involving names, medical record numbers, other demographics such as address & phone #, dates of birth, charges or bill balances, SSNs, insurance identification or Medicare #'s.

Entity: UWM Cont'd..

Attestation:

- An attestation signed by an owner or officer of UWM attesting that UWM has complied with the obligations of the CAP.
- An attestation signed by an officer of UWM attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content, & believes, based upon such inquiry, that the information is accurate & truthful.

OCR Guidance

- "All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise. An effective risk analysis is one that is comprehensive in scope & is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data."

Entity: Triple-S Management Corporation ("Triple-S")

Fine: $3.5 million **Duration of CAP:** Three Years

Date of Fine: November 30, 2015

Date of Incident: March 31, 2015, February 27, 2015, August 13, 2015

- On March 31, 2015, TSA reported to OCR that on October 15, 2014, *an unauthorized disclosure* occurred when enrolment staff placed the incorrect member ID cards in mailing envelopes, resulting in beneficiaries receiving the member ID card of another individual.
- On February 27, 2015, TSA reported to OCR that on December 12, 2014, an unauthorized disclosure of PHI occurred when beneficiaries Health Plan Identification numbers was placed on labels used in a mailing to their beneficiaries.
- On August 13, 2015, TSA reported to OCR that on January 28, 2015, a preventive mailing was sent to beneficiaries that included PHI for another member on the back of the member's letter. PHI impermissibly disclosed included members' names, addresses and the name of the preventative test the member should have their doctor perform.

Entity: Triple-S Cont'd..

Attestations:

- An attestation signed by an owner or officer of Triple-S attesting that the Policies & Procedures are being implemented, have been distributed to all workforce members, & that Triple-S is in compliance.
- An attestation signed by an owner or officer of Triple-S attesting that all workforce members have completed the initial training required by this CAP & have executed training certifications.
- An attestation signed by an owner or officer of Triple-S listing each legal entity within Triple-S & each Triple-S Business Associate, including mailing addresses, the corresponding name under which each entity is doing business, & the corresponding phone #'s & fax #'s, & attesting that each such entity has complied with the obligations of this CAP.
- An attestation signed by an owner or officer of Triple-S stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate & truthful.

Entity: Triple-S Cont'd..

Attestation:

- An attestation signed by an owner or officer of Triple-S attesting that it is obtaining & maintaining written or electronic training certifications from all persons that require training that they received training pursuant to the requirements set forth in this CAP.
- An attestation signed by an owner or officer of Triple-S attesting that he or she has re- viewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate & truthful.

OCR Guidance

- "OCR remains committed to strong enforcement of the HIPAA Rules," said OCR Director Jocelyn Samuels. "This case sends an important message for HIPAA Covered Entities not only about compliance with the requirements of the Security Rule, including risk analysis, but compliance with the requirements of the Privacy Rule, including those addressing BAA & the minimum necessary use of PHI."

Healthcare Cyber Risk = Business Risk

Entity: Lahey Hospital & Medical Center (Lahey)

Fine: $850,000 **Duration of CAP:** Two years

Date of Fine: November 25, 2015 **Date of Incident:** August 11, 2011

- Lahey notified OCR that a *laptop was stolen* from an unlocked treatment room during the overnight hours.
- The laptop was on a stand that accompanied a portable CT scanner, the laptop operated the scanner & produced images for viewing through Lahey's Radiology Information System and Picture Archiving and Communication System.
- The laptop hard drive contained the PHI of 599 individuals.

Entity: Lahey Cont'd..

Attestations:

- An attestation signed by an officer of Lahey attesting the Policies & Procedures & also an attestation signed by an officer of Lahey attesting the mechanisms required.
- An attestation signed by an officer of Lahey attesting that any revised Policies and Procedures have been fully implemented & that all members of the workforce who have access to EPHI have completed training on any revised Policies & Procedures consistent with the requirements.
- An attestation signed by an officer of Lahey stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate & truthful.

OCR Guidance

- "It is essential that entities apply appropriate protections to workstations associated with medical devices such as diagnostic or laboratory equipment," said OCR Director Jocelyn Samuels. "Because these workstations often contain EPHI & are highly portable, such EPHI must be considered during an entity's risk analysis, & entities must ensure that necessary safeguards that conform to HIPAA's standards are in place."

Entity: Cancer Care Group (CCG)

Fine: $750,000 **Duration of CAP:** Three years

Date of Fine: September 2, 2015 **Date of Incident:** August 29, 2012

- OCR received notification from Cancer Care regarding a breach of unsecured EPHI after a *laptop bag was stolen from an employee's car*.
- The bag contained the employee's computer and unencrypted backup media, which contained the names, addresses, dates of birth, Social Security numbers, insurance information and clinical information of approximately 55,000 current and former Cancer Care patients.
- OCR's subsequent investigation found that, prior to the breach, Cancer Care was in widespread non-compliance with the HIPAA Security Rule. *It had not conducted an enterprise-wide risk analysis* when the breach occurred in July 2012.

Entity: CCG Cont'd..

Attestation:

- An attestation signed by an officer of CCG attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content & believes that, upon such inquiry, the information is accurate & truthful.

OCR Guidance

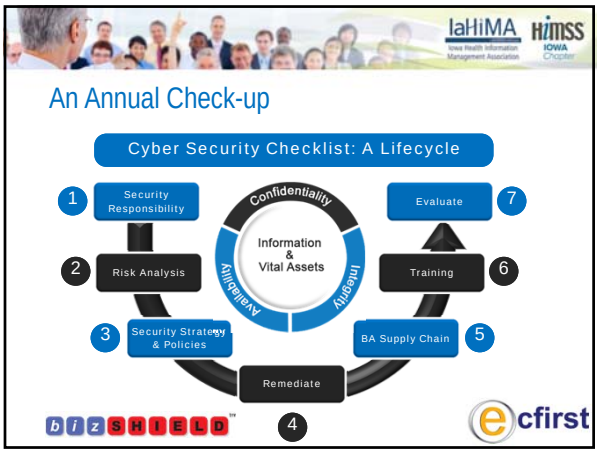
- "Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to PHI," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices & electronic media reduces the likelihood of a breach of PHI."

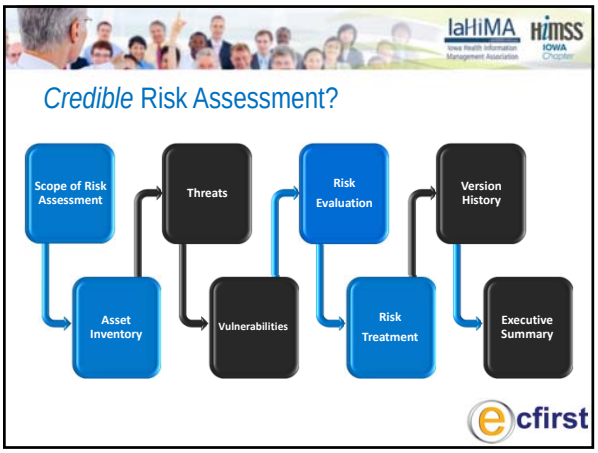
Healthcare Data Breaches Summary, 2015

Anthem BlueCross	78.8 Million Impacted	CareFirst BlueCross BlueShield	1.1 Million Impacted
PREMERA BLUE CROSS	11 Million Impacted	BEACON	220,000 Million Impacted
Excellus BlueCross BlueShield	10 Million Impacted	Advantage Dental	151,626 Million Impacted
UCLA Health	4.5 Million Impacted		84,681 Million Impacted
mie	3.9 Million Impacted	MaineGeneral Health	# of Impacted Members is Unknown

2016 Compliance & Cyber Security Dashboard

Healthcare Cyber Risk = Business Risk





Healthcare Cyber Risk = Business Risk