Robinson+Cole

HOT HIPAA TOPICS

Rhode Island Quality Institute

LINN F. FREEDMAN, ESQ.
OCTOBER 14, 2016

15386534

© 2015 Robinson & Cole LLP

Overview

- Identifying and Protecting High-Risk Data
- Recent Risks to Healthcare Industry
  - IRS Warning
  - FBI Warning
  - Phishing/Spear-Phishing
  - Ransomware/Malware
  - HHS Guidance
- Healthcare Cyber Attacks
- Rhode Island Identity Theft Prevention Act Updates
- HIPAA and TCPA
- HIPAA and Mobile Devices
- Using Gmail/E-mail
- Transportation of PHI
- HIPAA Enforcement/Fines and Penalties

Identifying and Protecting High-Risk Data

- Personally Identifiable Information
  - Includes SS #, state-issued ID #, mother's maiden name, driver's license #, passport #, credit history, criminal history
- Name & Contact Information
  - Includes initials, address, telephone number, e-mail address, mobile number, date of birth
- Personal Characteristics
  - Includes age, gender, marital status, nationality, sexual orientation, race, ethnicity, religious beliefs

Identifying and Protecting High-Risk Data (cont'd)

- Financial Institution Data
  - Includes credit, ATM, debit card #s, bank accounts, payment card information, PINs, magnetic stripe data, security codes, access codes, passwords
- Health & Insurance Account Information
  - Includes health status and history, disease status, medical treatment, diagnoses, prescriptions, insurance account #, Medicare and Medicaid information
  - HIPAA compliance

Identifying and Protecting High-Risk Data (cont’d)

- Website Traffic
  - Privacy Policy
  - Terms and Conditions of Use
- Employment Information
  - Includes income, salary, service fees, compensation information, background check information
- Intellectual Property Information

Recent Risks to Healthcare Industry

- E-mail Spoofing
- Phishing/Spear-Phishing
- Ransomware
- Malware

IRS Issues Warning to Payroll/HR

- On March 1, 2016, the IRS issued a warning to payroll and HR professionals about a phishing scheme that affected numerous companies
- A phishing email is sent to employees working in the HR and/or payroll department which looks amazingly like it is from the company’s CEO
- The email is rigged to look like the real one, and is hard to detect that any response to the “real” email is re-routed to a hacker’s email
- CEO or another company executive asks the HR or payroll employee to send him or her personally identifiable information about employees of the company, including W-2s

IRS Issues Warning to Payroll/HR (cont'd)

- Email is called a "spoofing" email and contains the actual name of the executive and asks the employee things like "Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review" or "Can you send me the updated list of employees with full details (Name, Social Security number, Date of Birth, Home Address, Salary)"
- According to the IRS, "If your CEO appears to be emailing you for company employees' personal information, including SSNs, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

FBI Issues Warning

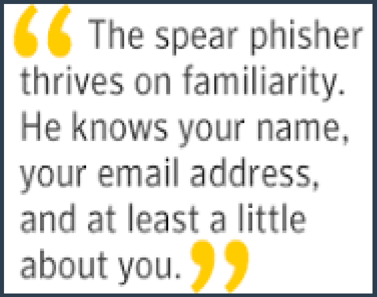
- FBI issued **warning** about the scams in April 2016, saying that there has been “a dramatic rise in the business e-mail compromise scam or “B.E.C.,” a scheme that targets businesses and has resulted in massive losses”
- FBI says that it has received complaints from victims in every state in the U.S. and at least 79 countries, from 17,642 victims
- The losses associated with the email scams total more than $2.3 billion

FBI Warning for Healthcare Cybersecurity

- FBI Ransomware Warning for Healthcare Cybersecurity

  - Issued in May 2016
  - FBI recommends:
    - Make sure employees are aware of ransomware and of their critical roles in protecting the organization’s data.
    - Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
    - Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
    - Disable macro scripts from office files transmitted over e-mail.

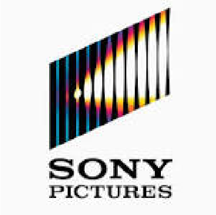
Phishing And Spear-phishing Scams
What Are They?


“The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you.”

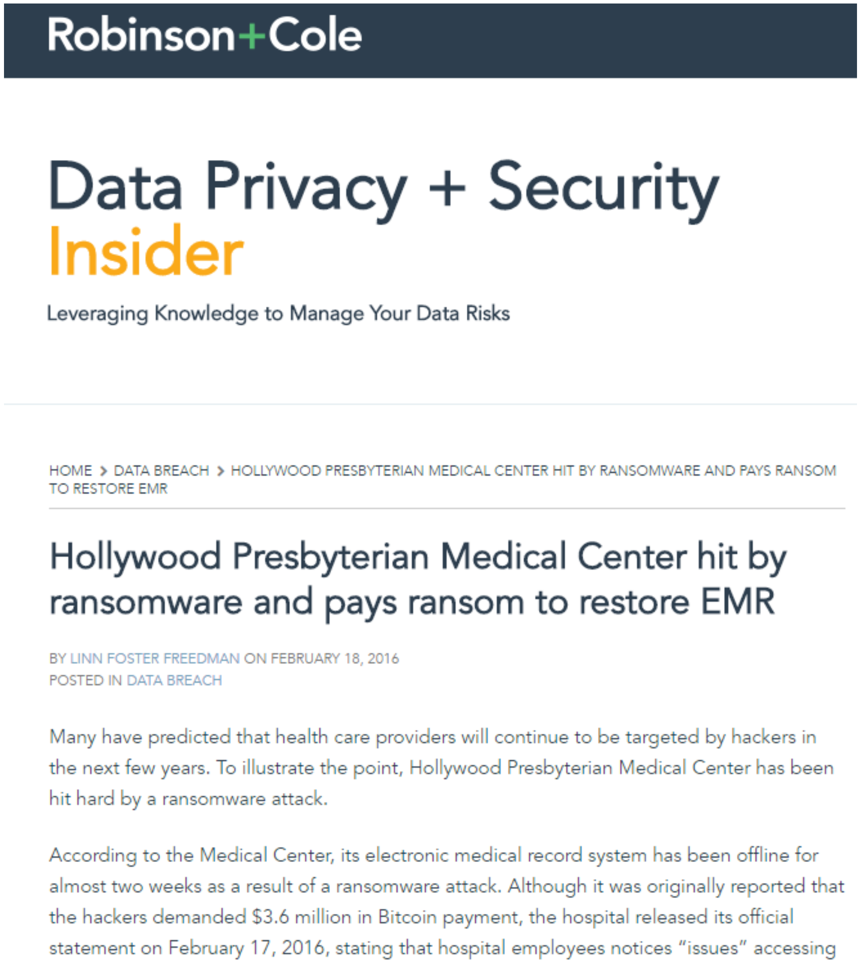
- ***Phishing*** is a malicious “spam-like” message sent in large batches to broad audience
- ***Spear-phishing*** is a form of phishing – messages appear to come from a familiar or trusted sender and target recipients
- Both have same goals:
  - To trick you into clicking on a malicious link or attachment or visiting a malicious web site.
  - To steal your login credentials, social security number, bank account or any other valuable data

Phishing and Spear-phishing - Growing and Expen$ive Problem

- Among email users who receive “bait” messages
  - **23%** open the bait messages
  - **11%** click on attachments and links in the bait messages
  - **1 in 10** open email attachments from unknown senders
  - **$1.8** million is average amount users cost their employer
- Recent major data breaches result from phishing or spear-phishing



Malware/Ransomware



Robinson+Cole

Data Privacy + Security
Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > DATA BREACH > HOLLYWOOD PRESBYTERIAN MEDICAL CENTER HIT BY RANSOMWARE AND PAYS RANSOM TO RESTORE EMR

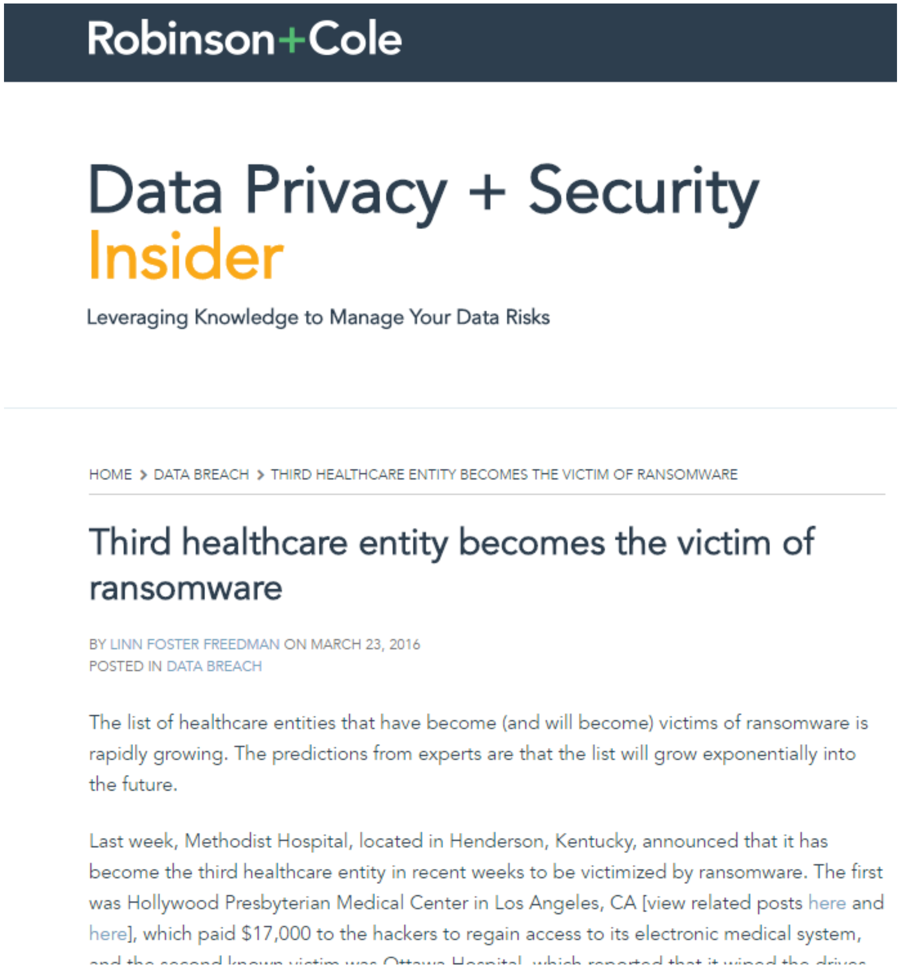
Hollywood Presbyterian Medical Center hit by ransomware and pays ransom to restore EMR

BY LINN FOSTER FREEDMAN ON FEBRUARY 18, 2016
POSTED IN DATA BREACH

Many have predicted that health care providers will continue to be targeted by hackers in the next few years. To illustrate the point, Hollywood Presbyterian Medical Center has been hit hard by a ransomware attack.

According to the Medical Center, its electronic medical record system has been offline for almost two weeks as a result of a ransomware attack. Although it was originally reported that the hackers demanded $3.6 million in Bitcoin payment, the hospital released its official statement on February 17, 2016, stating that hospital employees notices "issues" accessing

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > DATA BREACH > THIRD HEALTHCARE ENTITY BECOMES THE VICTIM OF RANSOMWARE

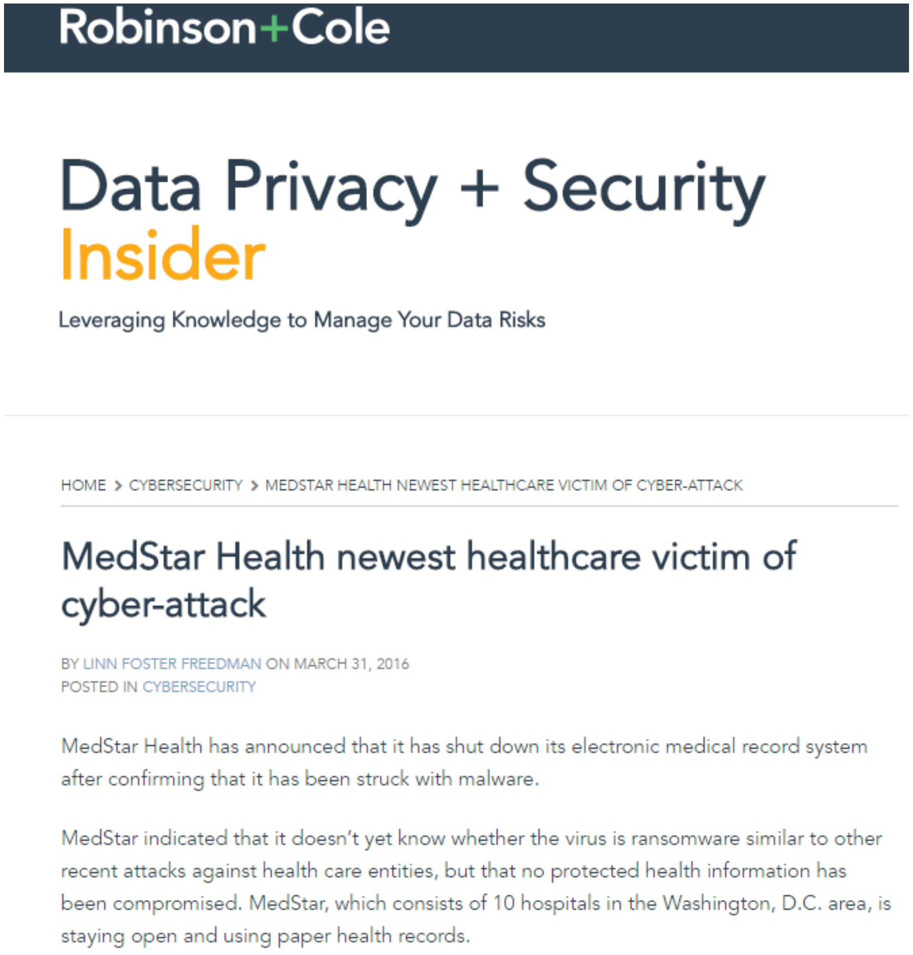
Third healthcare entity becomes the victim of ransomware

BY LINN FOSTER FREEDMAN ON MARCH 23, 2016
POSTED IN DATA BREACH

The list of healthcare entities that have become (and will become) victims of ransomware is rapidly growing. The predictions from experts are that the list will grow exponentially into the future.

Last week, Methodist Hospital, located in Henderson, Kentucky, announced that it has become the third healthcare entity in recent weeks to be victimized by ransomware. The first was Hollywood Presbyterian Medical Center in Los Angeles, CA [view related posts here and here], which paid $17,000 to the hackers to regain access to its electronic medical system, and the second known victim was Ottawa Hospital, which reported that it wiped the drives

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > CYBERSECURITY > MEDSTAR HEALTH NEWEST HEALTHCARE VICTIM OF CYBER-ATTACK

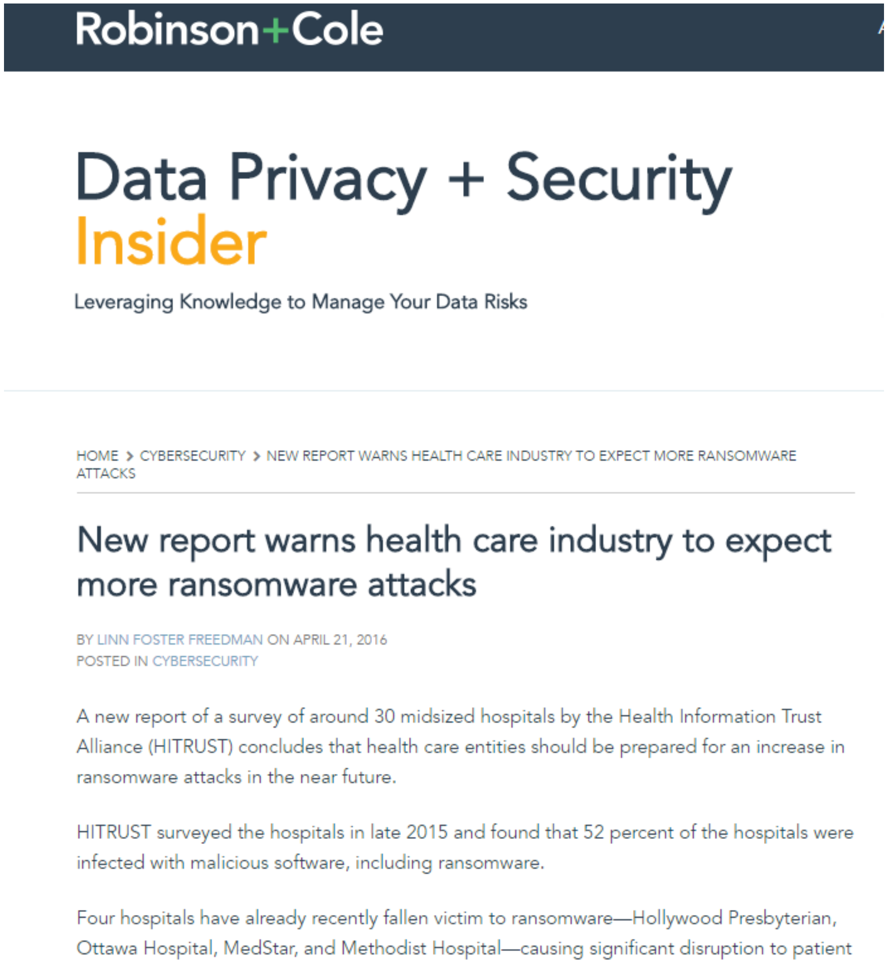
MedStar Health newest healthcare victim of cyber-attack

BY LINN FOSTER FREEDMAN ON MARCH 31, 2016
POSTED IN CYBERSECURITY

MedStar Health has announced that it has shut down its electronic medical record system after confirming that it has been struck with malware.

MedStar indicated that it doesn't yet know whether the virus is ransomware similar to other recent attacks against health care entities, but that no protected health information has been compromised. MedStar, which consists of 10 hospitals in the Washington, D.C. area, is staying open and using paper health records.

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security
Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > CYBERSECURITY > NEW REPORT WARNS HEALTH CARE INDUSTRY TO EXPECT MORE RANSOMWARE ATTACKS

New report warns health care industry to expect more ransomware attacks

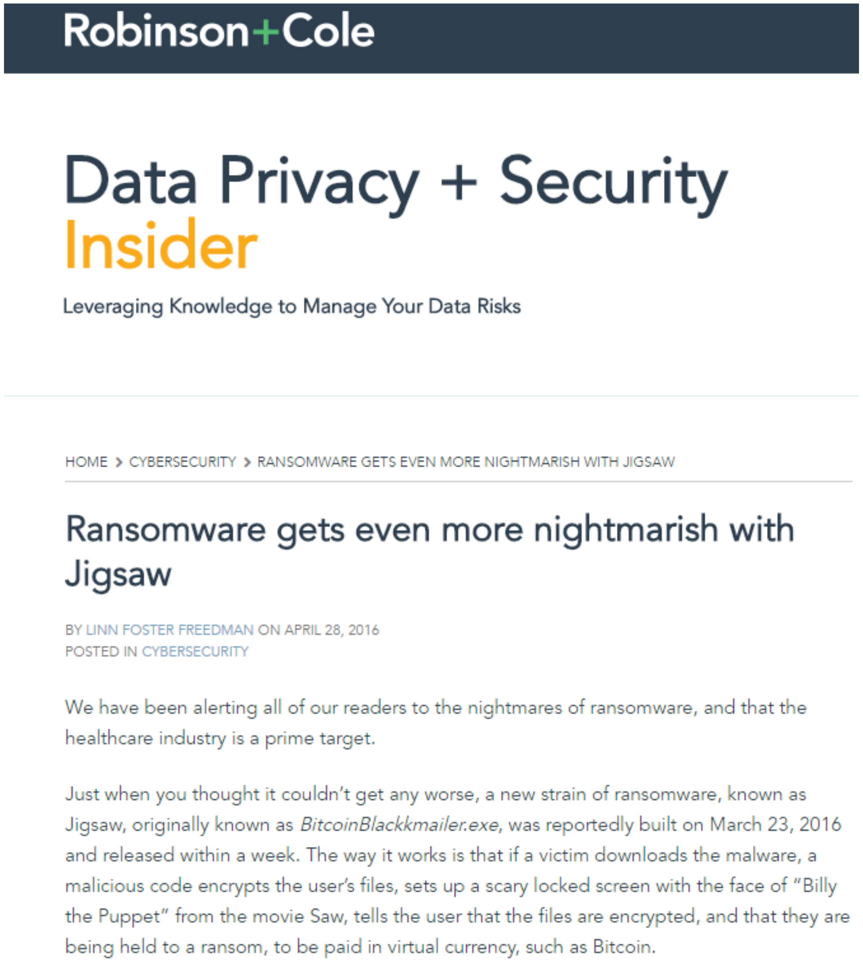
BY LINN FOSTER FREEDMAN ON APRIL 21, 2016
POSTED IN CYBERSECURITY

A new report of a survey of around 30 midsized hospitals by the Health Information Trust Alliance (HITRUST) concludes that health care entities should be prepared for an increase in ransomware attacks in the near future.

HITRUST surveyed the hospitals in late 2015 and found that 52 percent of the hospitals were infected with malicious software, including ransomware.

Four hospitals have already recently fallen victim to ransomware—Hollywood Presbyterian, Ottawa Hospital, MedStar, and Methodist Hospital—causing significant disruption to patient

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > CYBERSECURITY > RANSOMWARE GETS EVEN MORE NIGHTMARISH WITH JIGSAW

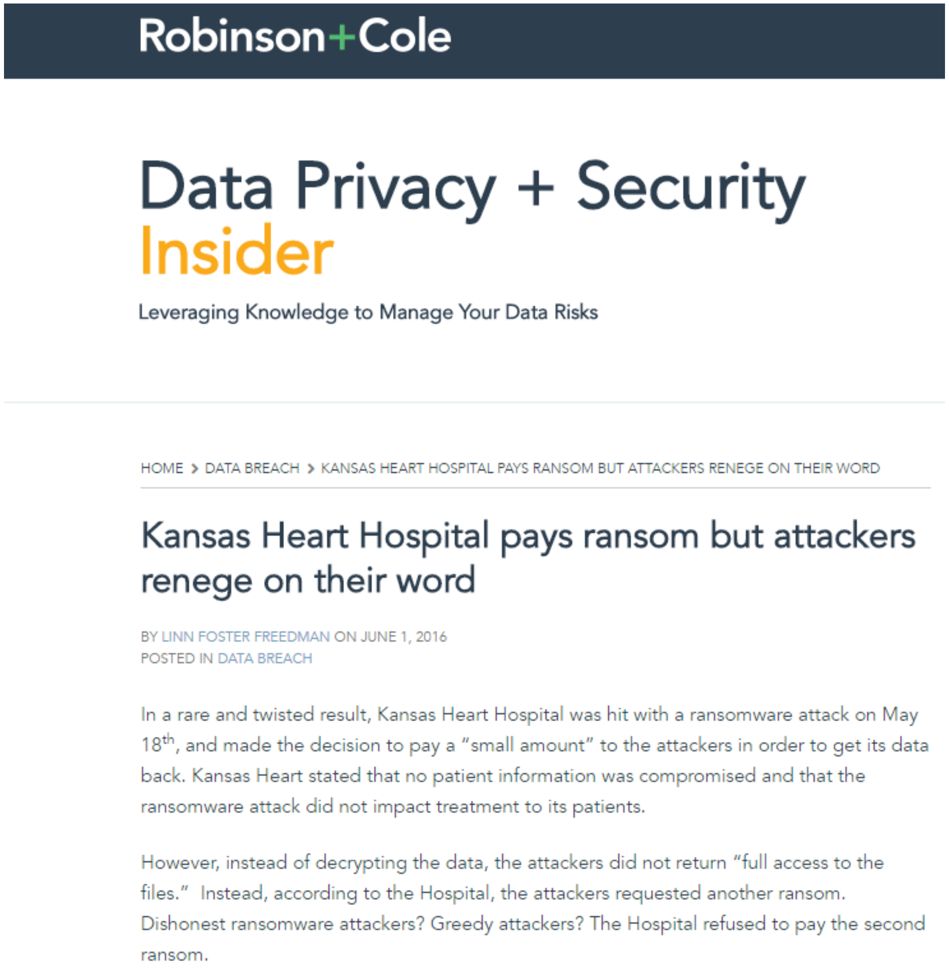
Ransomware gets even more nightmarish with Jigsaw

BY LINN FOSTER FREEDMAN ON APRIL 28, 2016
POSTED IN CYBERSECURITY

We have been alerting all of our readers to the nightmares of ransomware, and that the healthcare industry is a prime target.

Just when you thought it couldn't get any worse, a new strain of ransomware, known as Jigsaw, originally known as *BitcoinBlackkmailer.exe*, was reportedly built on March 23, 2016 and released within a week. The way it works is that if a victim downloads the malware, a malicious code encrypts the user's files, sets up a scary locked screen with the face of "Billy the Puppet" from the movie Saw, tells the user that the files are encrypted, and that they are being held to a ransom, to be paid in virtual currency, such as Bitcoin.

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > DATA BREACH > KANSAS HEART HOSPITAL PAYS RANSOM BUT ATTACKERS RENEGE ON THEIR WORD

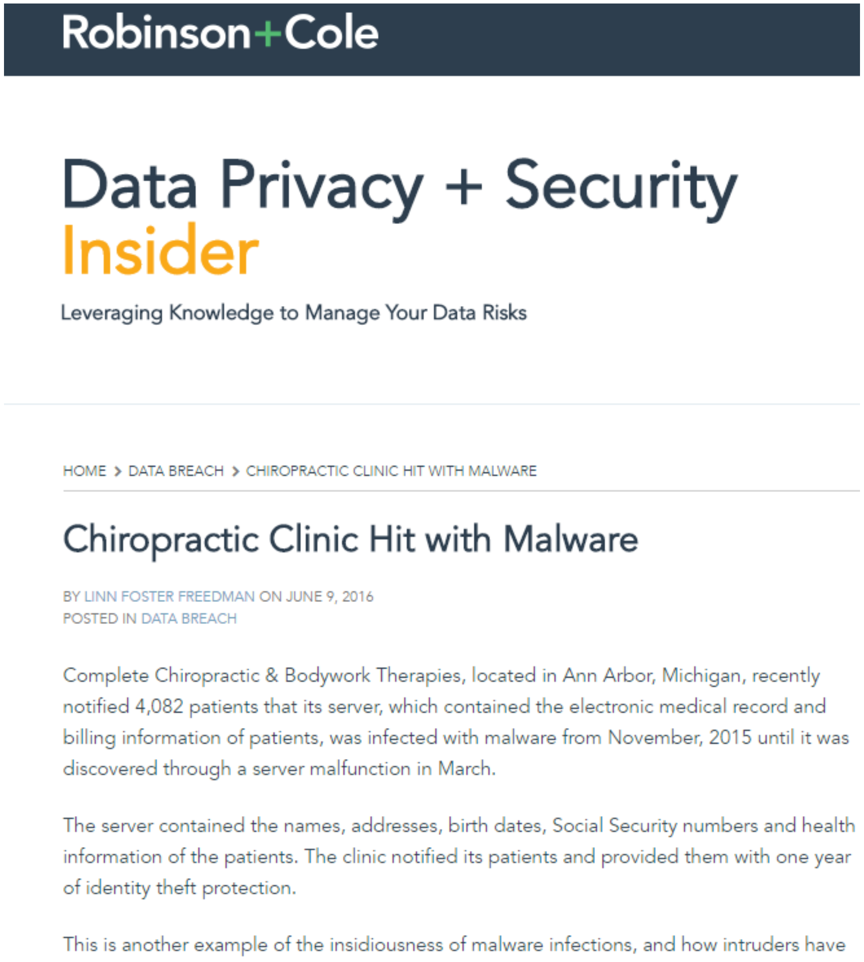
Kansas Heart Hospital pays ransom but attackers renege on their word

BY LINN FOSTER FREEDMAN ON JUNE 1, 2016
POSTED IN DATA BREACH

In a rare and twisted result, Kansas Heart Hospital was hit with a ransomware attack on May 18th, and made the decision to pay a "small amount" to the attackers in order to get its data back. Kansas Heart stated that no patient information was compromised and that the ransomware attack did not impact treatment to its patients.

However, instead of decrypting the data, the attackers did not return "full access to the files." Instead, according to the Hospital, the attackers requested another ransom. Dishonest ransomware attackers? Greedy attackers? The Hospital refused to pay the second ransom.

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security
Insider

Leveraging Knowledge to Manage Your Data Risks

HOME > DATA BREACH > CHIROPRACTIC CLINIC HIT WITH MALWARE

Chiropractic Clinic Hit with Malware

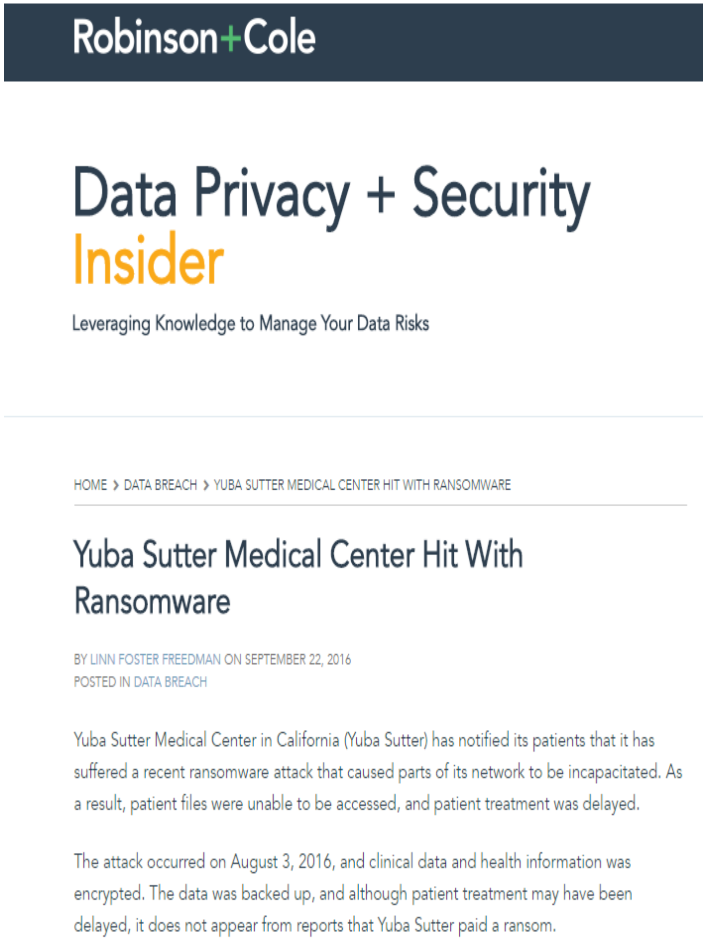
BY LINN FOSTER FREEDMAN ON JUNE 9, 2016
POSTED IN DATA BREACH

Complete Chiropractic & Bodywork Therapies, located in Ann Arbor, Michigan, recently notified 4,082 patients that its server, which contained the electronic medical record and billing information of patients, was infected with malware from November, 2015 until it was discovered through a server malfunction in March.

The server contained the names, addresses, birth dates, Social Security numbers and health information of the patients. The clinic notified its patients and provided them with one year of identity theft protection.

This is another example of the insidiousness of malware infections, and how intruders have

Malware/Ransomware (cont'd)



Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

HOME › DATA BREACH › YUBA SUTTER MEDICAL CENTER HIT WITH RANSOMWARE

Yuba Sutter Medical Center Hit With Ransomware

BY LINN FOSTER FREEDMAN ON SEPTEMBER 22, 2016
POSTED IN DATA BREACH

Yuba Sutter Medical Center in California (Yuba Sutter) has notified its patients that it has suffered a recent ransomware attack that caused parts of its network to be incapacitated. As a result, patient files were unable to be accessed, and patient treatment was delayed.

The attack occurred on August 3, 2016, and clinical data and health information was encrypted. The data was backed up, and although patient treatment may have been delayed, it does not appear from reports that Yuba Sutter paid a ransom.

HHS Issues Guidance on Ransomware

- July 11, 2016
- HHS issued a Fact Sheet that provides guidance on
  - (i) how HIPAA Security Rule compliance can assist health care organizations combat ransomware attacks, and
  - (ii) the applicability of HIPAA's Breach Notification Rule to ransomware attacks
    - Once ransomware detected, must initiate security incident and response procedures
    - Whether or not the presence of ransomware is a breach is fact-specific
    - Must apply applicable breach notification provisions to determine whether notification is required

The Shift to Medical Information

- Medical information worth **10-20 x** more than a credit card number
- Riper target because of the ability to sell large batches of personal data for profit
- Hospitals tend to have lower security so it is easier to get large amounts of data for medical fraud
- Medical identity theft is often not immediately identified or detected (unlike credit card fraud)

The Shift to Medical Information (cont'd)

- Cybersecurity investigators and fraud experts interviewed the underground market for patient data
  - ○ Data for sale includes:
    - Names, birth dates, policy numbers, diagnosis codes and billing information
  - ○ Used to create fake IDs to buy medical equipment or drugs for resale or combine patient number with false provider number and file made-up claims with insurers
  - ○ Sold for approximately $10-$20 each

Statistics from 2015

- **98%** of record leaks were due to large-scale breaches targeting the healthcare industry
- More than **111 million** individual's' data was **lost** due to hacking or IT incidents in the U.S. alone
- 56 breaches due to hacking or IT incidents in 2015 UP from 31 in 2014
- Only 97 breaches were due to loss or theft last year, down from 140 in 2014
- Only **5%** of healthcare organizations use single sign-on for Google Apps or Office 365

–Bitglass Healthcare Breach Report

10 Largest Healthcare Cyber Attacks of 2015

1. **Anthem** 78.8 million
2. **Premera** 11 million
3. **Excellus** 10 million
4. **UCLA Health** 4.5 million
5. **Medical Informatics Engineering** 3.9 million
6. **CareFirst** 1.1 million
7. **Beacon Health System** 220,000
8. **Advantage Dental** 151,626
9. **Muhlenberg Community Hospital** 84,681
10. **Maine General Health** –Unknown

10 Largest Healthcare Cyber Attacks in 2015

These **healthcare cyber attacks** affected over 109,671,626 individuals –or, approximately 1/3 of the population of the United States.

Healthcare Cyber Attack Updates

- ***Anthem*** announced data breach on February 4, 2015
- Affected approximately ***80 million*** members
- Class actions lawsuits popped up everywhere
  - Failure to encrypt personal information, delays in disclosing the breach and failing to adequately protect member data
- ***90 class actions*** filed
- Waiting on hearings regarding consolidation

Healthcare Cyber Attack Update (cont'd)

- ***Premera*** announced data breach on March 17, 2015
- Affected approximately ***11 million*** members
- Days after announcement, ***five class*** actions
- ***Investigations from three states*** –Washington, Alaska and Oregon
- Class actions based on the allegation that Premera waited too long to inform customers of the breach

Healthcare Cyber Attack Update (cont'd)

- ***Excellus Blue Cross Blue Shield*** announced data breach on September 9, 2015
- Affected approximately ***10 million*** members
- Two class actions
    - Allegations of negligence and breach of contract, and that two years of credit monitoring for children who were affected by the breach is insufficient

Healthcare Cyber Attack Update (cont’d)

- Banner Healthcare reported data breach of 3.7 million July 2016
  - Started with credit and debit card purchases for food and beverage
  - Migrated to employee and patient data
  - Including SSNs
  - Within a week, two class action lawsuits filed

Rhode Island Identity Theft Protection Act

- Completely revamped data breach notification rule in June 2015, effective as of July 2, 2016
  - If you experience a “breach of the security of the system” that poses a “significant risk of identity theft” to a resident of Rhode Island, whose personal information was or is reasonably believed to have been acquired by an unauthorized person, you must notify the affected individual(s)
  - “Breach of the security of the system “ is unauthorized access, or acquisition of unencrypted computerized data information that compromises the security, confidentiality or integrity of the personal information

Rhode Island Identity Theft Protection Act (cont'd)

- "Personal information " is an individual's first name or first initial and last name in combination with any one or more of the following:
  - Social Security number
  - Driver's license number or ID card number
  - Account number or credit or debit card number in combination with any required security code, access code, password or PIN
  - **Medical or health insurance information**
  - E-mail address with any required security code, access code, or password that permits access to an individuals' personal, medical, insurance or financial account

Rhode Island Identity Theft Protection Act (cont'd)

- Notification must be made no later than **45 calendar days** after confirmation of the breach
- Notification must include: brief description of breach, including number of affected individuals, type of information breached, date of breach, date of discovery of breach, description of remediation services, and description of individual's ability to file or obtain a police report or request a security freeze

Rhode Island Identity Theft Protection Act (cont'd)

- Penalties for violations
  - Up to $100 per reckless violation
  - Up to $200 per willful violation
- * A provider of health care, health care service plan, health insurer, or covered entity governed by HIPAA/HITECH shall be deemed in compliance with the revised Identity Theft Protection Act
- But HIPAA breach notification is 60 days and RI is now **45** days

Rhode Island Identity Theft Protection Act (cont'd)

- New data security requirements
  - If you store, collect, process, maintain, acquire, use, own or license personal information about a Rhode Island resident, you must "implement and maintain a risk-based information security program" of "reasonable security procedures and practices" that is "appropriate to the size and scope" of your organization, "the nature of the information and the purpose for which the information was collected."
  - Must have a written data retention policy
  - Medical records qualify
  - Implement Written Information Security Program
  - Update HIPAA compliance program

HIPAA and TCPA

Telephone Consumer Protection Act

- Prohibits the use of automated telephone dialing systems or artificial or prerecorded voice to consumers without prior express written consent (includes telemarketing to cell phones, and text messages)
- Strict liability with statutory damages of $500 per violation (up to $1,500 per violation if willful or knowing)
- Litigation against health care companies involving debt collection, patient notifications, prescription sales, etc.

HIPAA and TCPA (cont'd)

- Calls to residential phone lines exempt from TCPA consent requirements for the following type of health care messages:
  - Appointment and exam confirmations and reminders;
  - Wellness checkups;
  - Hospital pre-registration instructions;
  - Pre-operative instructions;
  - Lab results;
  - Post-discharge follow up intended to prevent readmission;
  - Prescription notification; and
  - Home health care instructions

HIPAA and TCPA (cont'd)

- HOWEVER, those exemptions do not apply for calls and texts to cell phones unless you have express written consent of patient
- Also must:
  - Only be sent to number provided by the patient
  - State the name and contact info of the provider
  - Limited to the purposes listed on previous slide
  - Be less than one minute OR less than 160 characters
  - Not be more than one phone message or text per day or three communications per week
  - Offer an opt-out, and honor opt-outs immediately
  - Make sure to include express consent on in-take forms

HIPAA and Mobile Devices

- Laptops, USB, portable hard drive, and smartphones are high risk if they contain PHI
  - Stolen unencrypted mobile devices still an issue every day
  - Lost laptops and USB drives
  - Connecting to an unsecure Wi-Fi network
- If a mobile device contains PHI and the PHI is accessed, used, or disclosed by an unauthorized individual you will be required to notify under HIPAA (and possibly state law)

HIPAA and Mobile Devices (cont'd)

- Risks with using USB drives
  - Cyber criminals starting to write viruses and worms that specifically target USBs
  - So small they're easy to lose
  - If a lost or stolen USB drive contains sensitive personal information that's not encrypted or secure

HIPAA and Mobile Devices (cont'd)

How to manage mobile devices used by health care providers and professionals

- Decide whether mobile devices will be used to access, receive, transmit or store PHI or used as part of an internal network or system
- Consider how mobile devices affect the risks to PHI
- Identify mobile device risk management strategy
  - **BYOD Policy**
- Train employees about mobile device privacy and security awareness and best practices

HIPAA and Mobile Devices (cont'd)

How can you protect and secure PHI when using a mobile device?

- Use a complex password or other user authentication (but not enough to fall in safe harbor)
- Install and enable encryption
- Install and activate remote wiping and/or remote disabling
- Disable and do not install or use file sharing applications
- Install and enable a firewall

HIPAA and Mobile Devices (cont'd)

(cont'd)

- Install and enable security software
- Keep your security software up to date
- Research mobile applications/software BEFORE downloading
- Maintain physical control over the device
- Use adequate security to send or receive PHI over public Wi-Fi networks
- Delete/destroy all stored PHI before discarding or reusing a mobile device

HIPAA and Gmail & Other Free E-mail Providers

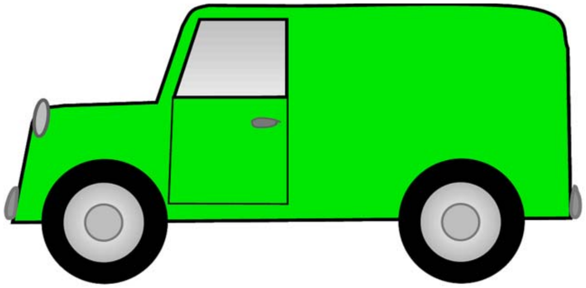
- Use of Gmail to communicate with patients or transmit PHI leaves the information open to vulnerabilities, as well as hefty consequences for non-compliance
- PHI sent via standard Gmail is not protected
- Must put in place ‘reasonable safeguards’ to protect the PHI that is sent via e-mail
- Gmail terms state Google has access to all data transmitted through Gmail account
- Google mines all data

Best Practices when Using E-mail

- Encryption
- Virtual Private Network/RSA
- Verify Selected Recipients
- Use Standard Confidentiality Disclaimers in Outlook
- “Sensitive” communications should be given special protections against disclosure to 3rd parties
  - It is the responsibility of the employee directing the communication to determine if the communication is “sensitive”

Transportation of PHI

- Use a chain of custody log
  - Tracking data, the times and dates of transfers, names and signatures of individuals releasing the information, and a general description of the information being released
- Paper records in non-transparent envelopes and boxes, electronic records encrypted
- Contracts in place with vendors who transport and store the PHI
  - With indemnification and insurance



Enforcement/Fines and Penalties (cont'd)

2015

- **Cornell Prescription Pharmacy**
  - $125,000
  - Correct deficiencies in hits HIPAA compliance program
  - Affected 1,610 patients
  - Disposal of unsecured documents containing PHI in an unlocked, open container on Cornell's premises
- **St. Elizabeth's Medical Center**
  - $218,400
  - Correct deficiencies in its HIPAA compliance program
  - Failed to conduct risk analysis of document sharing application containing e-PHI of 498 individuals, and failed to timely identify and respond to known security incident

Enforcement/Fines and Penalties (cont'd)

- **Cancer Care Group, P.C.**
  - $750,000
  - Correct deficiencies in its HIPAA compliance program
  - 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
- **Lahey Hospital and Medical Center**
  - $850,000
  - Laptop stolen from an unlocked treatment room during the overnight hours
  - Laptop operated a scanner and produced images for viewing through Lahey's Radiology Information System & Picture Archiving and Communication System
  - Contained PHI of 599 individuals.

Enforcement/Fines and Penalties (cont'd)

- **Triple-S Management Corporation**
  - $3.5 million
  - Failure to implement appropriate administrative, physical, and technical safeguards to protect the privacy of its beneficiaries' PHI;
  - Impermissible disclosure of PHI to outside vendor with which it did not have an appropriate business associate agreement;
  - Use or disclosure of more PHI than was necessary to carry out mailings;
  - Failure to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI; and
  - Failure to implement security measures sufficient to reduce the risks and vulnerabilities to its ePHI to a reasonable and appropriate level.
- **University of Washington Medicine**
  - $750,000
  - e-PHI of approximately 90,000 individuals was accessed after an employee downloaded an email attachment that contained malicious malware
  - Malware compromised the organization's IT system

HIPAA Enforcement/Fines and Penalties (cont'd)

2016

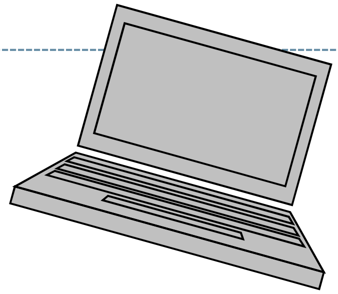
Lincare, Inc.

- $239,800
- OCR's investigation of Lincare began after an individual complained that a Lincare employee left behind documents containing PHI of 278 patients after moving residences

Complete P.T., Pool & Land Physical Therapy, Inc.

- $25,000
- Impermissibly disclosed numerous individuals' PHI, when it posted patient testimonials, including full names and full face photographic images, to its website without obtaining valid, HIPAA-compliant authorizations

HIPAA Enforcement/Fines and Penalties (cont'd)



North Memorial Health Care

- $1.55 million
- By failing to implement a business associate agreement with a major contractor and failing to institute an organization-wide risk analysis to address risks and vulnerabilities to its patient information

Feinstein Institute for Medical Research

- $3.9 million
- Laptop computer containing ePHI of approximately 13,000 patients and research participants was stolen from an employee's car

HIPAA Enforcement/Fines and Penalties (cont’d)

Raleigh Orthopedic Clinic, P.A. of North Carolina

- $750,000
- By failing to execute a business associate agreement prior to turning over PHI of 17,300 to a potential business partner.

New York Presbyterian

•$2.2 million

•Disclosure of two patients’ PHI to film crews and staf during the filming of “NY Med,” an ABC television series

HIPAA Enforcement/Fines and Penalties (cont'd)

Catholic Health Care Services of the Archdiocese of Philadelphia

- $650,000
- Theft of a CHCS mobile device compromised the PHI of 412 nursing home residents

Oregon Health & Science University

- $2.7 million
- Widespread vulnerabilities
- OHSU submitted two reports involving:
  - Unencrypted laptop
  - A stolen unencrypted thumb drive
- Storage of the electronic protected health information (ePHI) of over 3,000 individuals on a cloud-based server without a business associate agreement

University of Mississippi Medical Center

- $2.75 million
- Breach of unsecured ePHI affecting approximately 10,000 individuals

HIPAA Enforcement/Fines and Penalties (cont'd)

Advocate Health Care Network

- $5.5 million
- Three breach notification reports pertaining to separate and distinct incidents involving its subsidiary, Advocate Medical Group
- Combined breaches affected the ePHI of approximately 4 million individuals

HIPAA Enforcement/Fines and Penalties (cont'd)

Care New England Health System

- $400,000
- Woman & Infants Hospital of Rhode Island, a covered entity member of business associate CNE, lost unencrypted backup tapes containing the ultrasound studies of approximately 14,000 individuals, including patient name, data of birth, date of exam, physician names, and, in some instances Social Security Numbers
- Business Associate Agreement between WIH and CNE did not incorporate revisions required under the HIPAA Omnibus Final Rule

Linn Foster Freedman
lfreedman@rc.com

Robinson + Cole
One Financial Plaza
Suite 1430
Providence, RI 02903

Thank you

QUESTIONS?

www.dataprivacyandsecurityinsider.com