CYBERSECURITY AND HIPAA

Idaho Medical Association

Kim C. Stanger

Andrew Shaxted

(10-20)

HOLLAND&HART LLP

This presentation is similar to any other seminar designed to provide general information on pertinent legal topics. The statements made and any materials distributed as part of this presentation are provided for educational purposes only. They do not constitute legal advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the speakers. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. If you have specific questions as to the application of the law to your activities, you should seek the advice of your legal counsel.

Andrew Shaxted

Senior Director, Technology

+1 773 658 0241 | andrew.shaxted@fticonsulting.com | Boise, ID

ABOUT ANDREW SHAXTED

Andrew Shaxted works with global healthcare, life sciences, and med device companies to audit, advise, and implement policies and procedures required under US and international data privacy law. In his work, Andrew drafts expert reports, advises execs and board members on an array of data privacy risk topics, supports data breach response events, and works with organizations to implement data privacy risk management programs.

Mr. Shaxted holds a B.A. from Purdue University and a J.D. from DePaul University. He speaks regularly at industry conferences on the topic of emerging data privacy trends and was recently featured on CNBC's Squawk Box to discuss the implications of the California Consumer Privacy Act (the CCPA). Andrew holds his CIPM, CIPP/E as well as CIPP/US certifications. Andrew is licensed to practice law in Illinois.

Representative Engagements:

- Designed and implemented a global data privacy compliance program for a multi-national, publicly-traded healthcare technology and services company.
- Designed and implemented a Global Data Privacy Program and enhanced data mapping process for a German-based Fortune 150 Pharma and Lifesciences company.
- Performed an end-to-end HIPAA Security Rule and HIPAA Privacy Rule assessments across a portfolio of med devices, analytics software products, and back-office Revenue Cycle Management services totaling ~600 assessments points.
- Drafted an expert report for a California-based substance abuse and behavioral health provider, identifying gaps under the HIPAA Security Rule in response to impending OCR enforcement actions.
- Drafted an expert report to be used in civil proceedings for a New Jersey based fertility clinic and pharmacy to substantiate HIPAA Security Rule compliance.

Areas of Expertise

- Data Privacy
- Enterprise Risk Management
- Strategic Communication
- Technology
- Product Development

Certifications

- CIPM
- CIPP/US
- CIPP/E
- Oracle Cloud Certification
- Admitted Attorney: Illinois

Professional Affiliations

- American Bar Association
- Illinois State Bar Association
- International Association of Privacy Professionals
- USC Gould School of Law Institute for Corporate Counsel

Education

- B.A. Purdue University
- J.D. DePaul University

HOLLAND&HART LLP

Information Governance, Privacy & Security Practice Offerings

DATA PRIVACY ADVISORY

Data privacy assessments, program implementation, Data Subject Access Request (DSAR) solutions

E-DISCOVERY CONSULTING

Best-of-breed technology, workflow, data re-use, review of process efficiencies and training

INFORMATION GOVERNANCE CENTER OF EXCELLENCE (COE)

Data mapping, IG policy and frameworks, HIPAA compliance

DATA COLLECTION & FORENSIC INVESTIGATIONS

Global forensic collection and investigative services including EMEA and APAC

E-DISCOVERY MANAGED SERVICES

Project management, overflow staff and services, software management and maintenance

LEGAL HOLDS

System selection, implementation, hold migration, change management

BACKUP REMEDIATION

FTI can create a plan to systematically evaluate and reduce your preserved backup tapes.

SECONDMENTS & EXPERT STAFF AUGMENTATION

IG, privacy and discovery specialists for stop-gap, overflow work and long-term needs

OPTIMIZATION OF MICROSOFT OFFICE 365 APPLICATIONS

Data migration and preservation, collection workflows for Microsoft O365 email, One Drive, Teams, SharePoint, Yammer and more

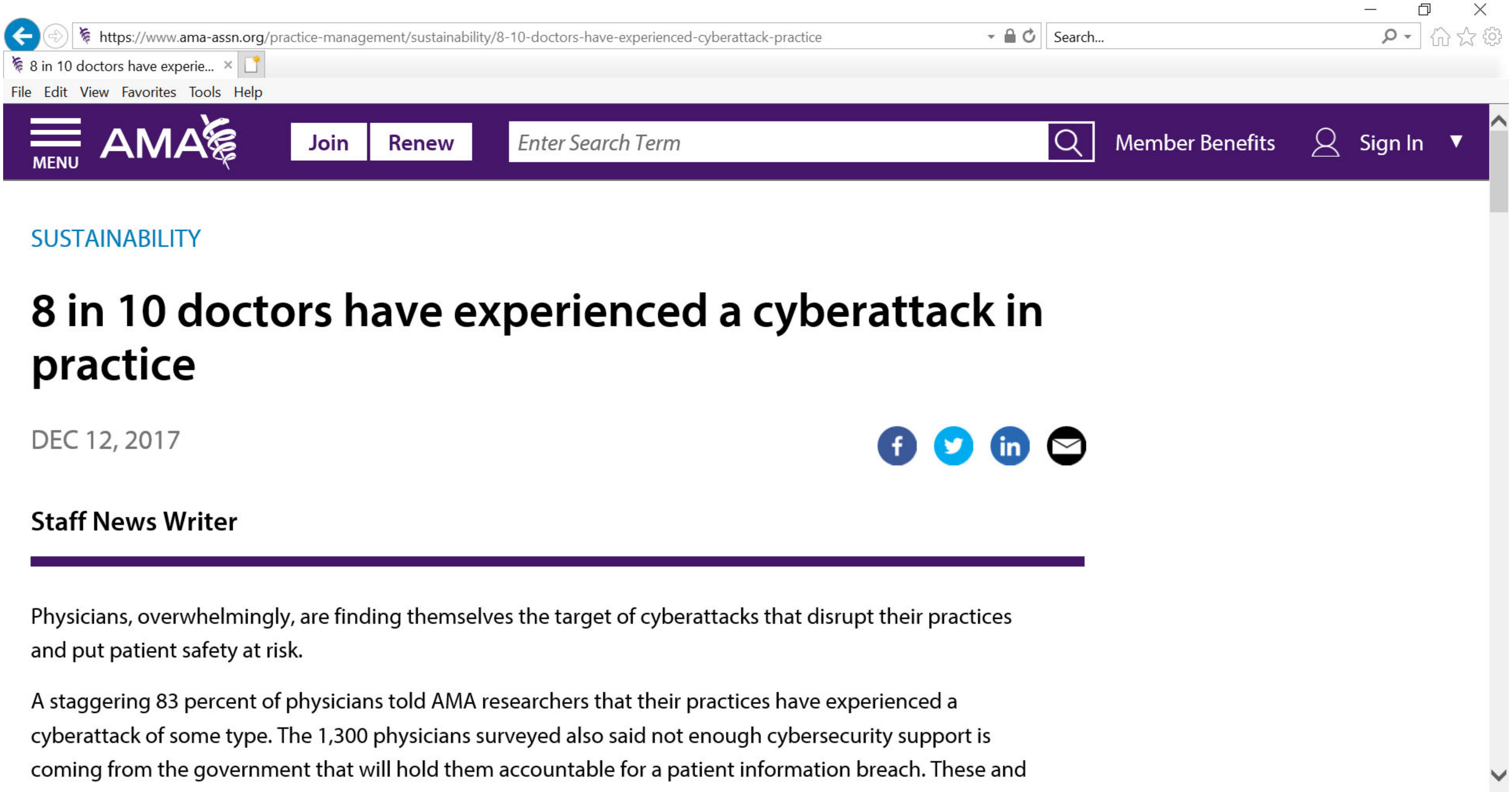
DATA REMEDIATION & DEFENSIBLE DISPOSITION OF DATA DEBRIS

Backup tapes, legacy email and systems, business apps, file shares

RECORDS RETENTION TECHNOLOGY AND POLICIES

Defensibly refresh records management policies and implement new technologies

Cybersecurity Threats


https://www.ama-assn.org/practice-management/sustainability/8-10-doctors-have-experienced-cyberattack-practice
Search...
8 in 10 doctors have experie...
File Edit View Favorites Tools Help
MENU
AMA
Join
Renew
Enter Search Term
Member Benefits
Sign In

SUSTAINABILITY

8 in 10 doctors have experienced a cyberattack in practice

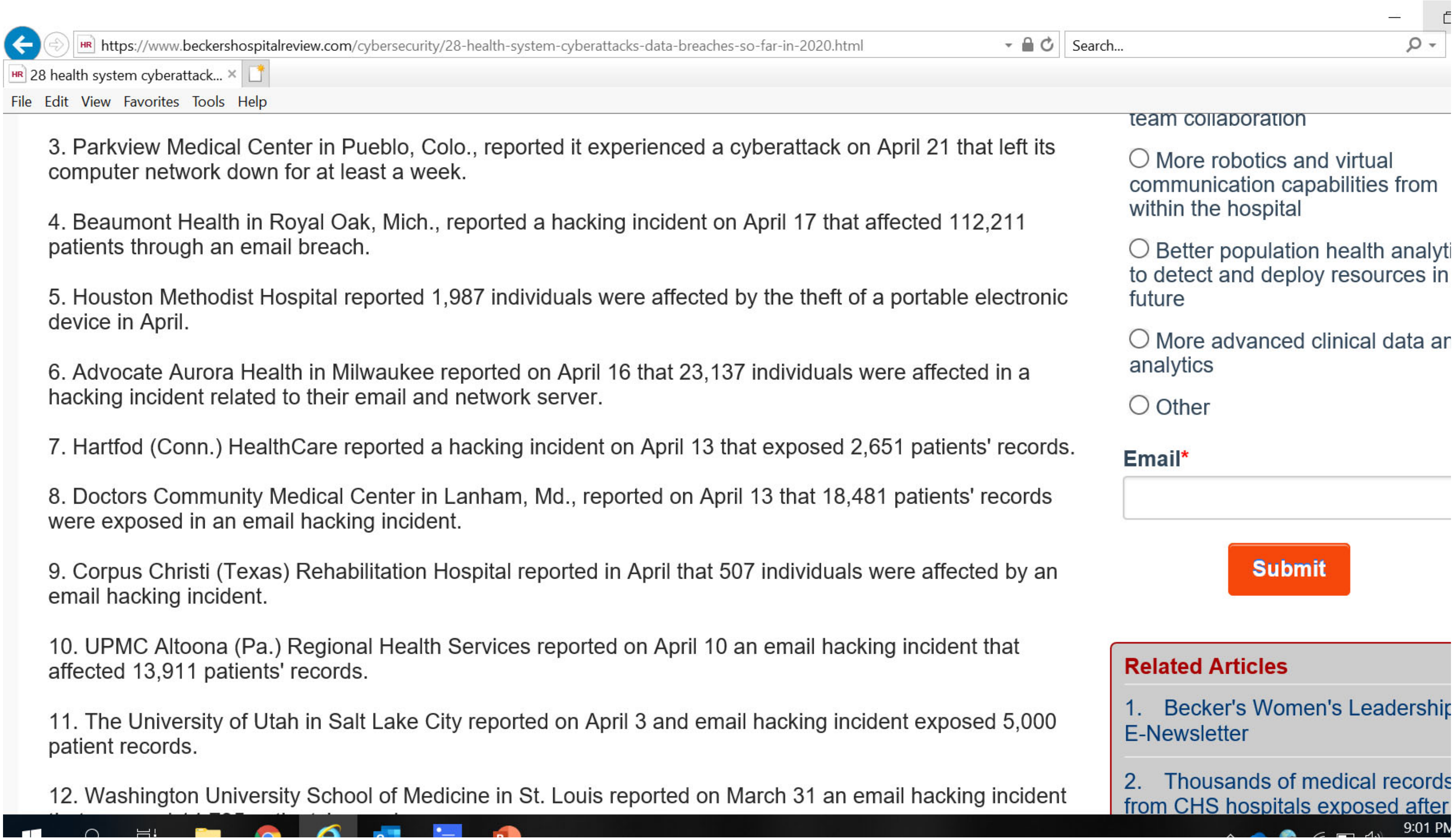
DEC 12, 2017

Staff News Writer

Physicians, overwhelmingly, are finding themselves the target of cyberattacks that disrupt their practices and put patient safety at risk.

A staggering 83 percent of physicians told AMA researchers that their practices have experienced a cyberattack of some type. The 1,300 physicians surveyed also said not enough cybersecurity support is coming from the government that will hold them accountable for a patient information breach. These and

Cybersecurity Threats


https://www.beckershospitalreview.com/cybersecurity/28-health-system-cyberattacks-data-breaches-so-far-in-2020.html
Search...
28 health system cyberattack... ×
File Edit View Favorites Tools Help
9:01 PM

3. Parkview Medical Center in Pueblo, Colo., reported it experienced a cyberattack on April 21 that left its computer network down for at least a week.

4. Beaumont Health in Royal Oak, Mich., reported a hacking incident on April 17 that affected 112,211 patients through an email breach.

5. Houston Methodist Hospital reported 1,987 individuals were affected by the theft of a portable electronic device in April.

6. Advocate Aurora Health in Milwaukee reported on April 16 that 23,137 individuals were affected in a hacking incident related to their email and network server.

7. Hartfod (Conn.) HealthCare reported a hacking incident on April 13 that exposed 2,651 patients' records.

8. Doctors Community Medical Center in Lanham, Md., reported on April 13 that 18,481 patients' records were exposed in an email hacking incident.

9. Corpus Christi (Texas) Rehabilitation Hospital reported in April that 507 individuals were affected by an email hacking incident.

10. UPMC Altoona (Pa.) Regional Health Services reported on April 10 an email hacking incident that affected 13,911 patients' records.

11. The University of Utah in Salt Lake City reported on April 3 and email hacking incident exposed 5,000 patient records.

12. Washington University School of Medicine in St. Louis reported on March 31 an email hacking incident

team collaboration

○ More robotics and virtual communication capabilities from within the hospital

○ Better population health analyti to detect and deploy resources in future

○ More advanced clinical data ar analytics

○ Other

Email*

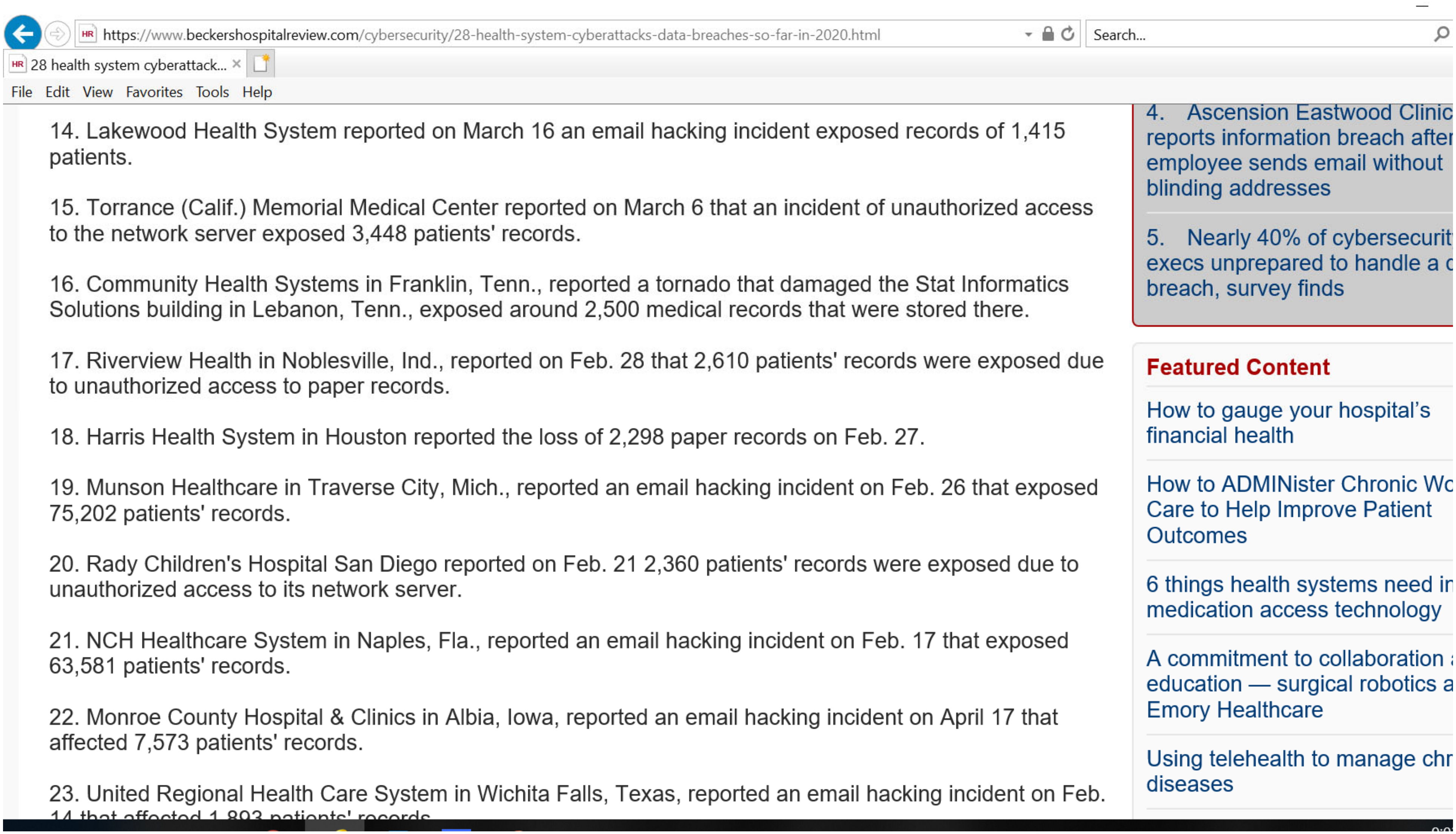
Submit

Related Articles

1. Becker's Women's Leadershi E-Newsletter

2. Thousands of medical records from CHS hospitals exposed after

Cybersecurity Threats


https://www.beckershospitalreview.com/cybersecurity/28-health-system-cyberattacks-data-breaches-so-far-in-2020.html
Search...
28 health system cyberattack...
File Edit View Favorites Tools Help

14. Lakewood Health System reported on March 16 an email hacking incident exposed records of 1,415 patients.

15. Torrance (Calif.) Memorial Medical Center reported on March 6 that an incident of unauthorized access to the network server exposed 3,448 patients' records.

16. Community Health Systems in Franklin, Tenn., reported a tornado that damaged the Stat Informatics Solutions building in Lebanon, Tenn., exposed around 2,500 medical records that were stored there.

17. Riverview Health in Noblesville, Ind., reported on Feb. 28 that 2,610 patients' records were exposed due to unauthorized access to paper records.

18. Harris Health System in Houston reported the loss of 2,298 paper records on Feb. 27.

19. Munson Healthcare in Traverse City, Mich., reported an email hacking incident on Feb. 26 that exposed 75,202 patients' records.

20. Rady Children's Hospital San Diego reported on Feb. 21 2,360 patients' records were exposed due to unauthorized access to its network server.

21. NCH Healthcare System in Naples, Fla., reported an email hacking incident on Feb. 17 that exposed 63,581 patients' records.

22. Monroe County Hospital & Clinics in Albia, Iowa, reported an email hacking incident on April 17 that affected 7,573 patients' records.

23. United Regional Health Care System in Wichita Falls, Texas, reported an email hacking incident on Feb. 14 that affected 1,893 patients' records.

4. Ascension Eastwood Clinic reports information breach afte employee sends email without blinding addresses

5. Nearly 40% of cybersecurit execs unprepared to handle a c breach, survey finds

Featured Content

How to gauge your hospital's financial health

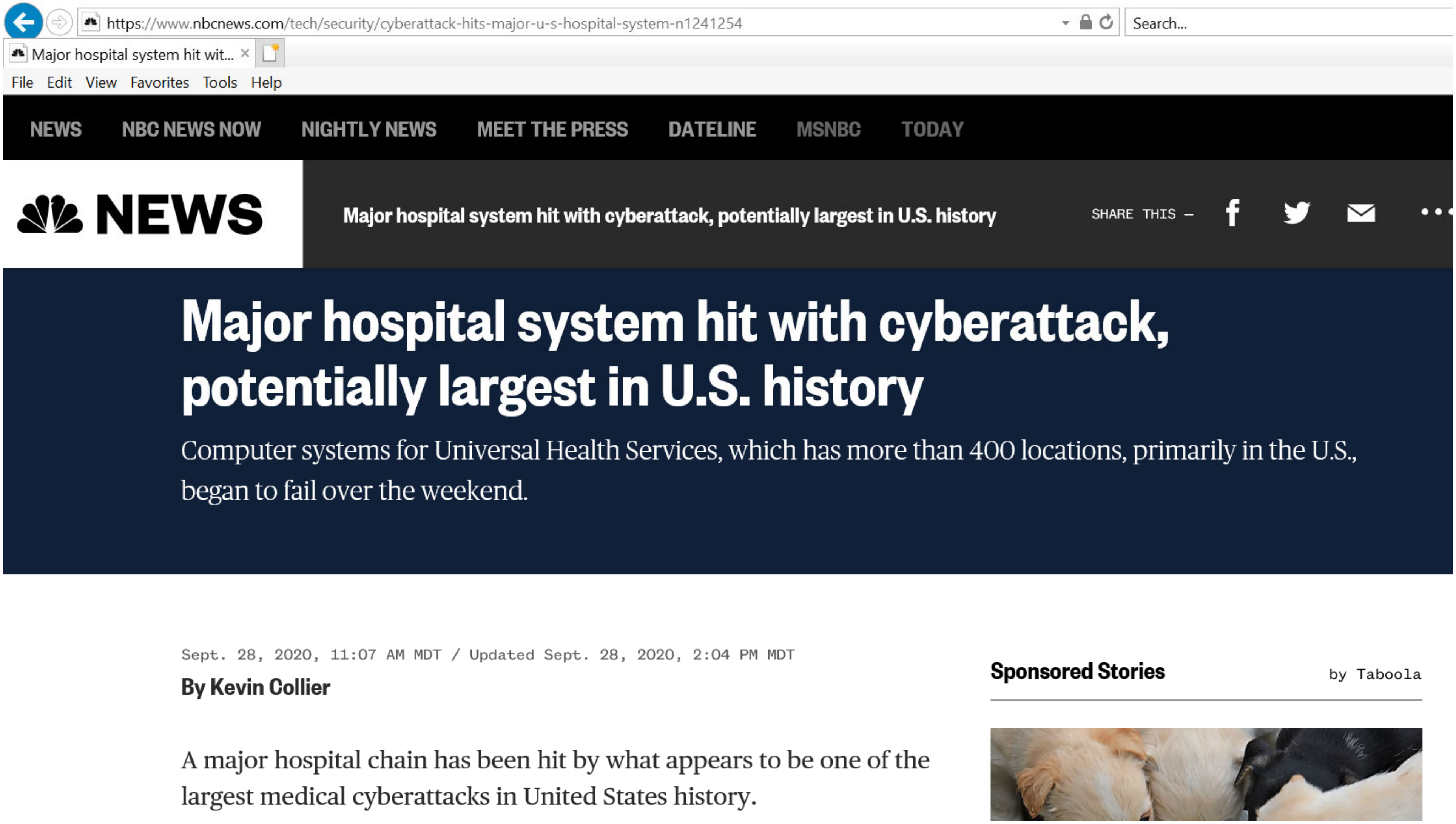
How to ADMINister Chronic Wo Care to Help Improve Patient Outcomes

6 things health systems need in medication access technology

A commitment to collaboration a education — surgical robotics a Emory Healthcare

Using telehealth to manage chr diseases

Cybersecurity Threats


https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254
Search...
Major hospital system hit wit...
File Edit View Favorites Tools Help
NEWS NBC NEWS NOW NIGHTLY NEWS MEET THE PRESS DATELINE MSNBC TODAY
NEWS
Major hospital system hit with cyberattack, potentially largest in U.S. history
SHARE THIS –
Sponsored Stories
by Taboola

Major hospital system hit with cyberattack, potentially largest in U.S. history

Computer systems for Universal Health Services, which has more than 400 locations, primarily in the U.S., began to fail over the weekend.

Sept. 28, 2020, 11:07 AM MDT / Updated Sept. 28, 2020, 2:04 PM MDT

By Kevin Collier

A major hospital chain has been hit by what appears to be one of the largest medical cyberattacks in United States history.

Cybersecurity in Healthcare

- Ransomware encrypts your IT system so that you may not access it, including:
  - Patient records
  - Financial records
  - Employment records
- Hacker accesses data on your system
- Hacker manipulates or corrupts data on medical devices
- Employee error leads to access to hundreds of patient records

What are the consequences to your organization?

Cybersecurity in Healthcare

- Ransomware encrypts your IT system so that you may not access it, including:
  - Patient records
  - Financial records
  - Employment records
- Hacker accesses data on your system
- Hacker manipulates or corrupts data on medical devices
- Employee error leads to access to thousands of patient records

- Harm to patients
- Inability to access data
- Corruption of data
- Forced to transfer patients
- Disruption of operations
- Lost revenue
- Cost of response
- Loss or damage to equipment
- Bad public relations
- Fines and penalties
- Lawsuits
- Others?

Cybersecurity Laws

Cyberliability Laws

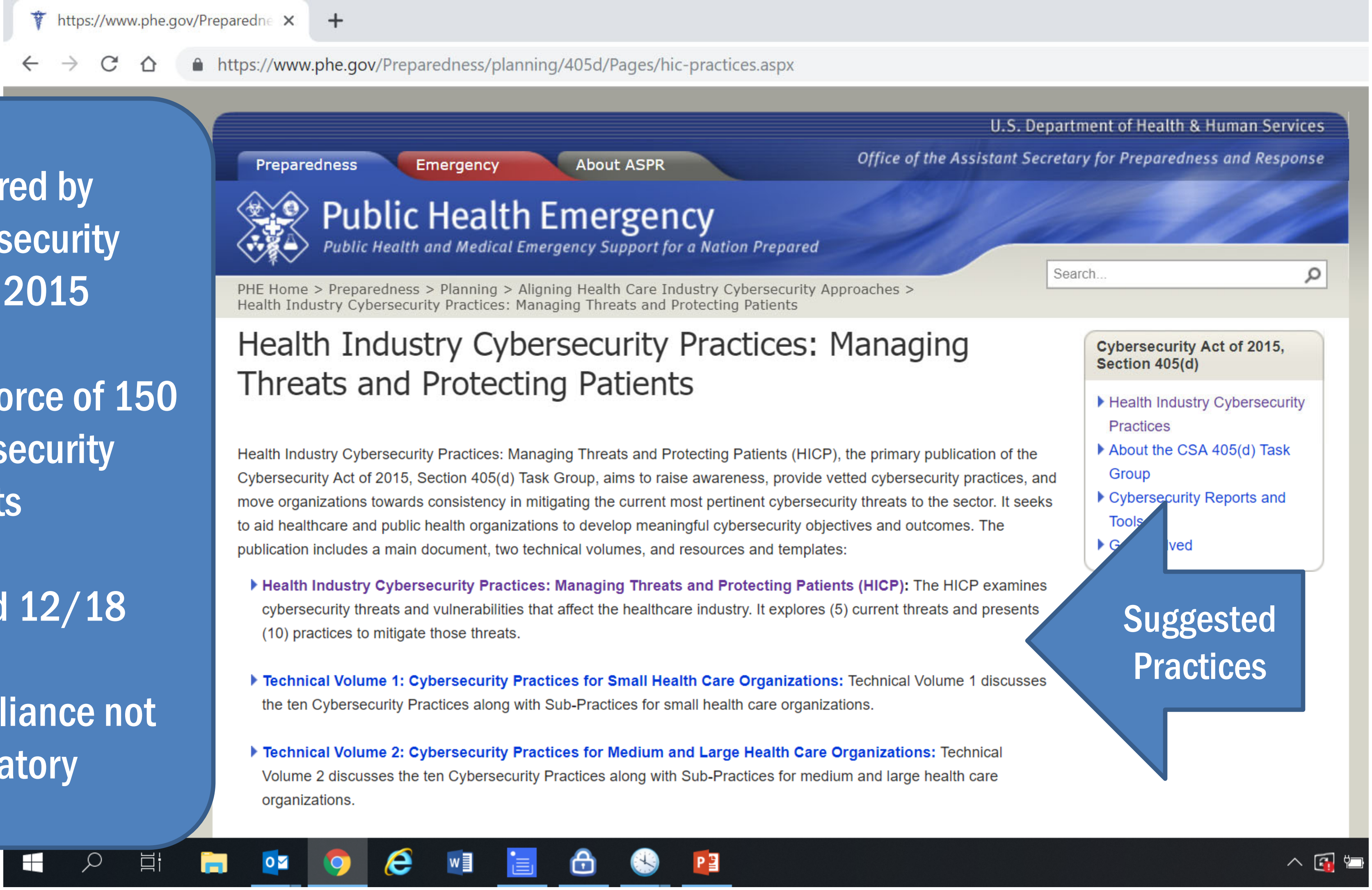
- Health Insurance Portability and Accountability Act ("HIPAA"), 45 CFR part 164
  - Privacy Rule.
  - Security Rule
    - Perform periodic risk assessment.
    - Implement administrative, technical and physical safeguards.
      - Policies and procedures
      - Technical solutions
      - Encryption
    - Execute business associate agreements.
  - Breach Notification Rule

Cyberliability Laws

- Federal Trade Comm'n Act ("FTCA") § 5 (15 USC 45(a))
  - Prohibits unfair or deceptive acts affecting commerce.
    - Deceipt = misrepresentations re privacy policy
    - Unfair = inadequate security measures
  - FTC has authority to regulate a company's cybersecurity efforts. *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015)
  - FTC has filed 50+ complaints against entities based on failure to safeguard personal info.

https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

- Required by Cybersecurity Act of 2015
- Task force of 150
- cybersecurity experts
- Issued 12/18
- Compliance not mandatory



https://www.phe.gov/Preparedne ✕
https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
U.S. Department of Health & Human Services
Office of the Assistant Secretary for Preparedness and Response
Preparedness
Emergency
About ASPR
Public Health Emergency
Public Health and Medical Emergency Support for a Nation Prepared
Search...

PHE Home > Preparedness > Planning > Aligning Health Care Industry Cybersecurity Approaches > Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group, aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes. The publication includes a main document, two technical volumes, and resources and templates:

- **Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP):** The HICP examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores (5) current threats and presents (10) practices to mitigate those threats.
- **Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations:** Technical Volume 1 discusses the ten Cybersecurity Practices along with Sub-Practices for small health care organizations.
- **Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations:** Technical Volume 2 discusses the ten Cybersecurity Practices along with Sub-Practices for medium and large health care organizations.

Cybersecurity Act of 2015, Section 405(d)

- Health Industry Cybersecurity Practices
- About the CSA 405(d) Task Group
- Cybersecurity Reports and Tools
- G ved

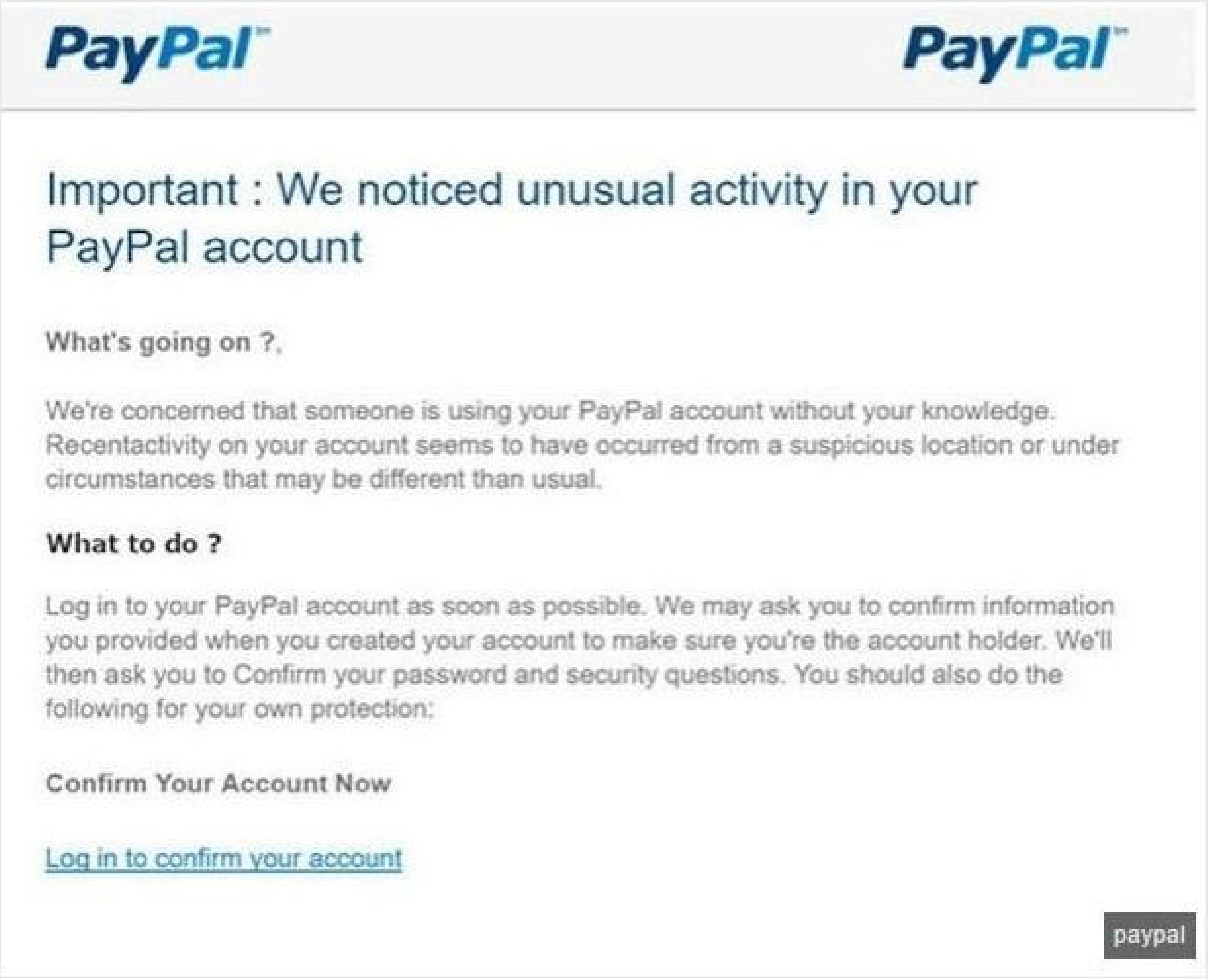
Suggested Practices

Top Cyber Threats in Healthcare

1. E-mail phishing attacks
2. Ransomware attacks
3. Loss or theft of equipment or data
4. Insider, accidental or intentional data loss
5. Attacks against connected medical devices that may affect patient safety

1. E-mail Phishing Attacks

- Cybercriminal attempts to trick you into:
  - Giving access to system by entering passwords, or
  - Downloading malicious software.
- Cybercriminal may:
  - Obtain your e-mail from publicly available sources.
  - Identify contacts through publicly available sources or social media.
  - Send you e-mail that appears to be from a known contact.
- E-mail usually contains an active link that:
  - Solicits sensitive information, or
  - Downloads malicious software.
- Some attacks are very convincing…



Important : We noticed unusual activity in your PayPal account

What's going on ?.

We're concerned that someone is using your PayPal account without your knowledge. Recentactivity on your account seems to have occurred from a suspicious location or under circumstances that may be different than usual.

What to do ?

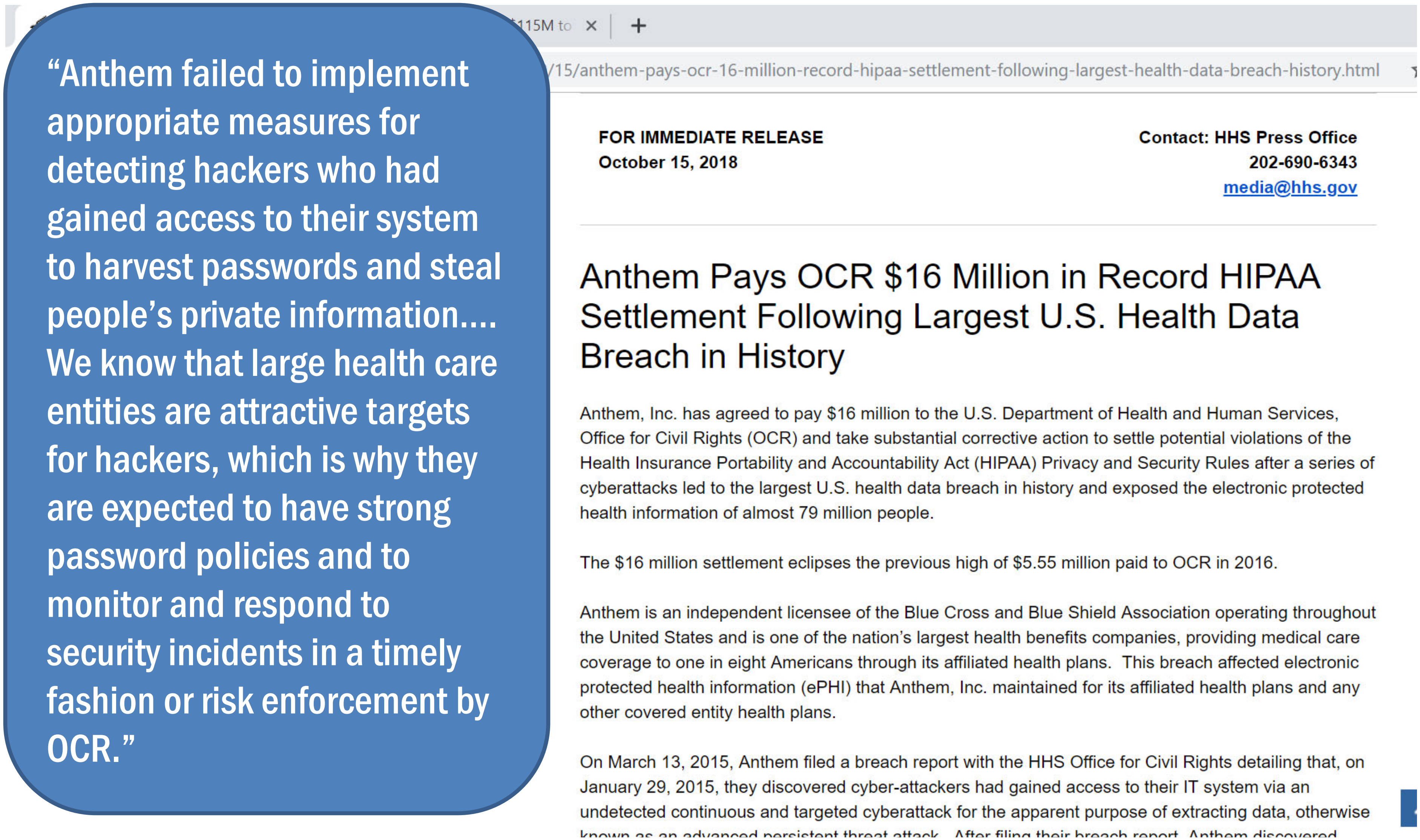
Log in to your PayPal account as soon as possible. We may ask you to confirm information you provided when you created your account to make sure you're the account holder. We'll then ask you to Confirm your password and security questions. You should also do the following for your own protection:

Confirm Your Account Now

Log in to confirm your account

E-mail Phishing Attacks

"Anthem failed to implement appropriate measures for detecting hackers who had gained access to their system to harvest passwords and steal people's private information.... We know that large health care entities are attractive targets for hackers, which is why they are expected to have strong password policies and to monitor and respond to security incidents in a timely fashion or risk enforcement by OCR."


$115M to ×
+
/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html

FOR IMMEDIATE RELEASE
October 15, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

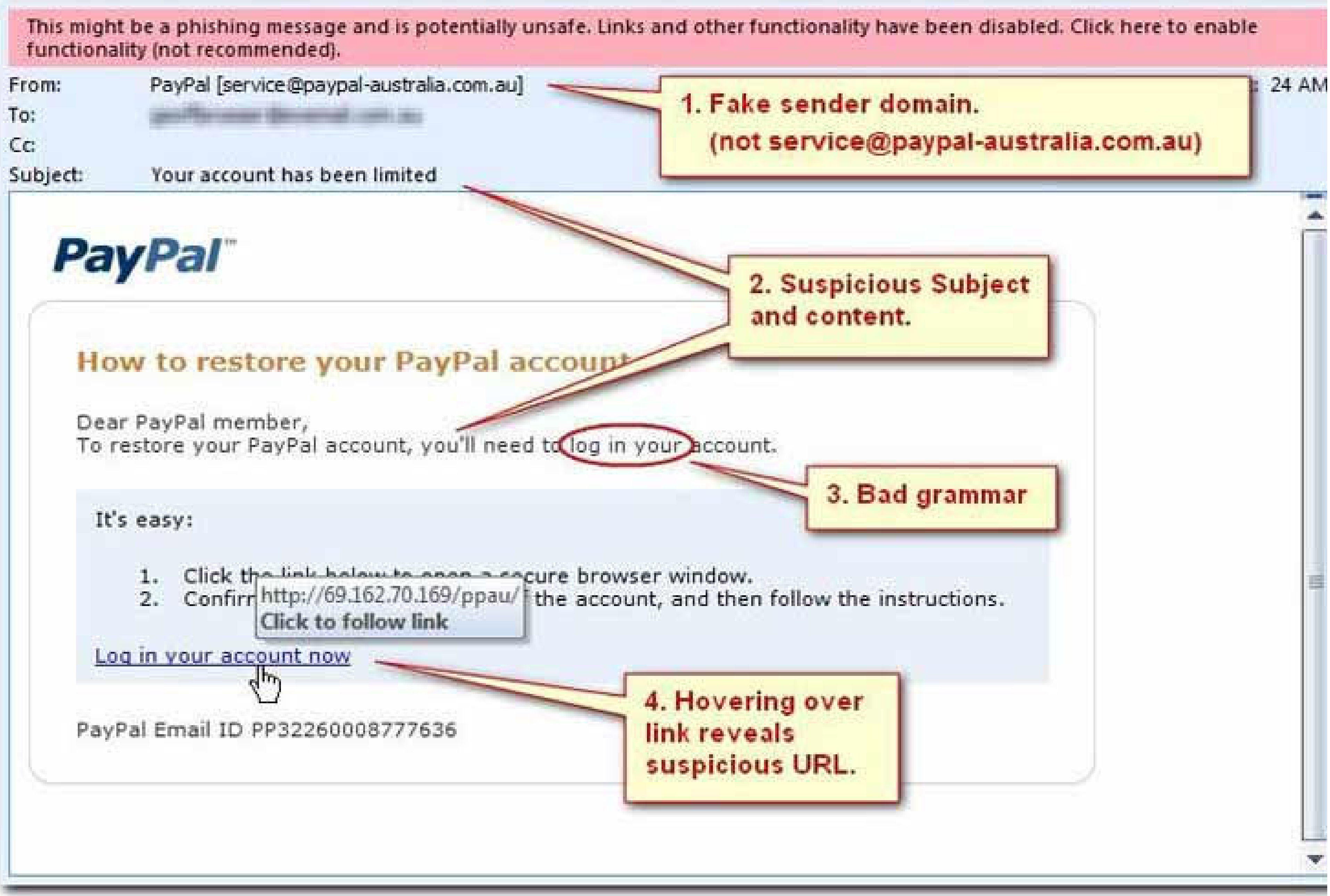
Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History

Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules after a series of cyberattacks led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people.

The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016.

Anthem is an independent licensee of the Blue Cross and Blue Shield Association operating throughout the United States and is one of the nation's largest health benefits companies, providing medical care coverage to one in eight Americans through its affiliated health plans. This breach affected electronic protected health information (ePHI) that Anthem, Inc. maintained for its affiliated health plans and any other covered entity health plans.

On March 13, 2015, Anthem filed a breach report with the HHS Office for Civil Rights detailing that, on January 29, 2015, they discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data, otherwise known as an advanced persistent threat attack. After filing their breach report, Anthem discovered



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).

From: PayPal [service@paypal-australia.com.au] 24 AM

To: [redacted]

Cc:

Subject: Your account has been limited

PayPal™

How to restore your PayPal account

Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.

It's easy:

1. Click the link below to open a secure browser window.
2. Confirr the account, and then follow the instructions.

http://69.162.70.169/ppau/
Click to follow link

Log in your account now

PayPal Email ID PP32260008777636

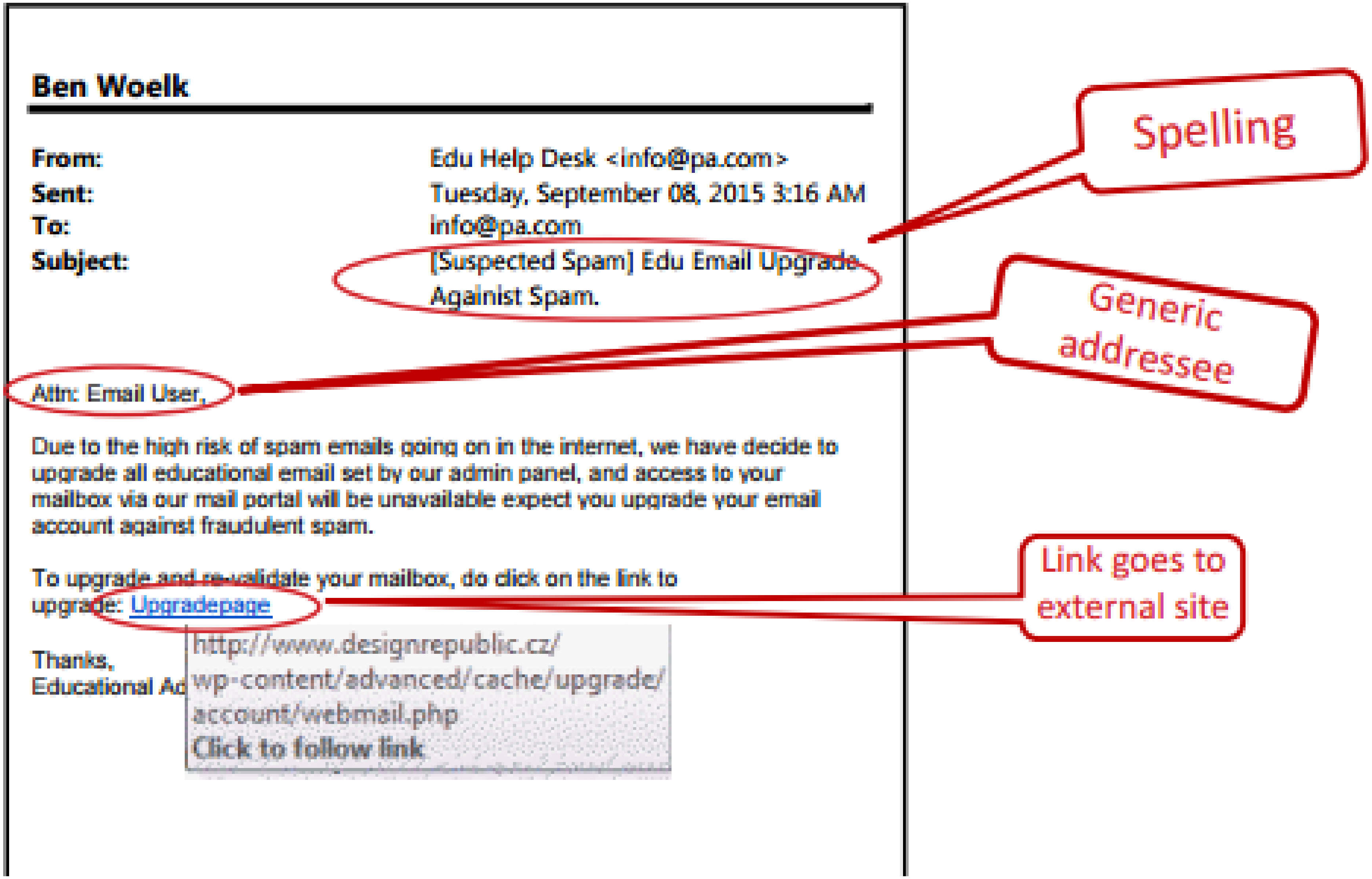
1. Fake sender domain.
(not service@paypal-australia.com.au)

2. Suspicious Subject and content.

3. Bad grammar

4. Hovering over link reveals suspicious URL.

May also appear to be internal e-mails



Ben Woelk

From: Edu Help Desk <info@pa.com>
Sent: Tuesday, September 08, 2015 3:16 AM
To: info@pa.com
Subject: [Suspected Spam] Edu Email Upgrade Againist Spam.

Attn: Email User,

Due to the high risk of spam emails going on in the internet, we have decide to upgrade all educational email set by our admin panel, and access to your mailbox via our mail portal will be unavailable expect you upgrade your email account against fraudulent spam.

To upgrade and re-validate your mailbox, do click on the link to upgrade: Upgradepage

http://www.designrepublic.cz/wp-content/advanced/cache/upgrade/account/webmail.php
Click to follow link

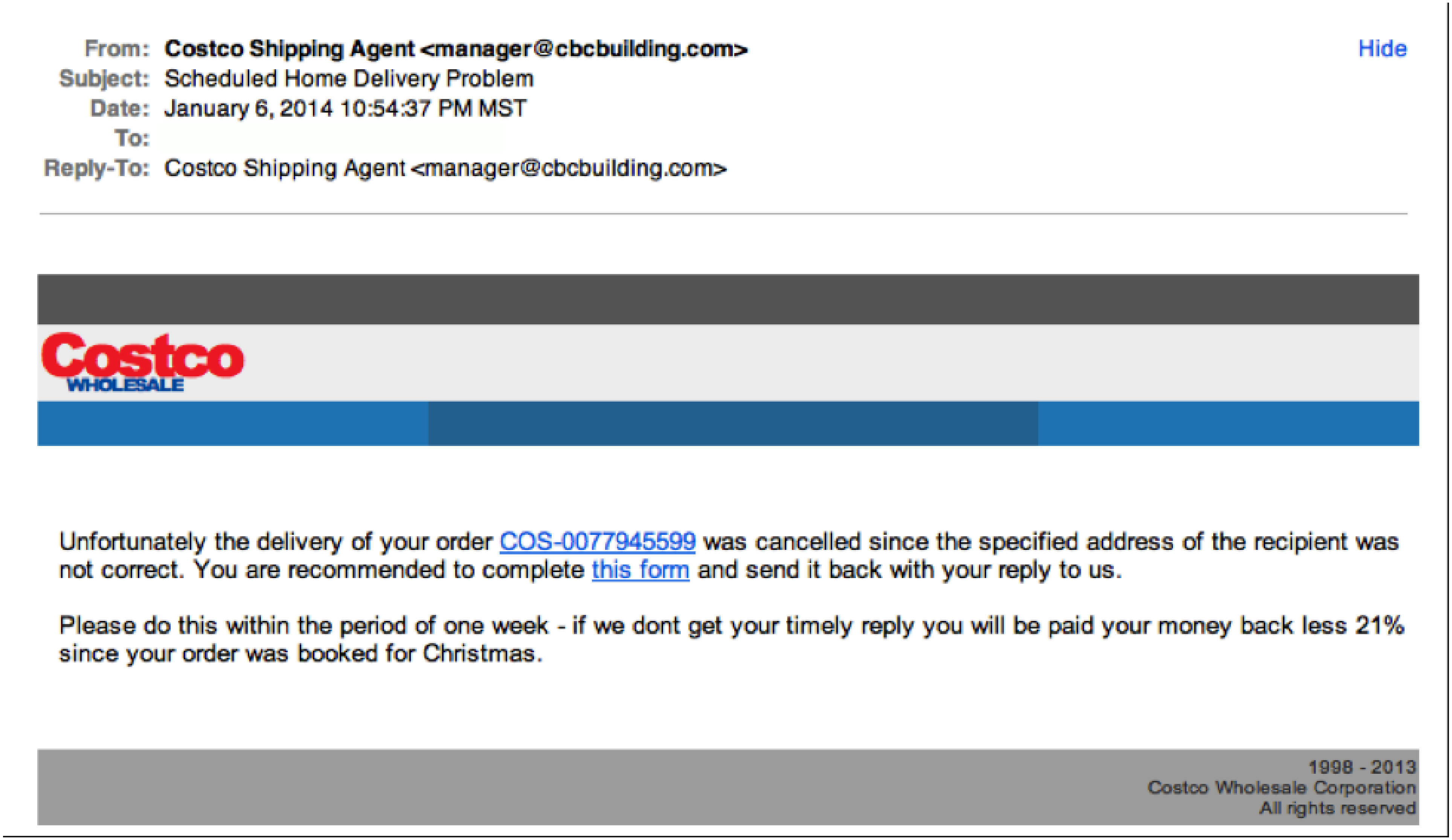
Thanks,
Educational Ad

Spelling

Generic addressee

Link goes to external site

E-mail Phishing Attack



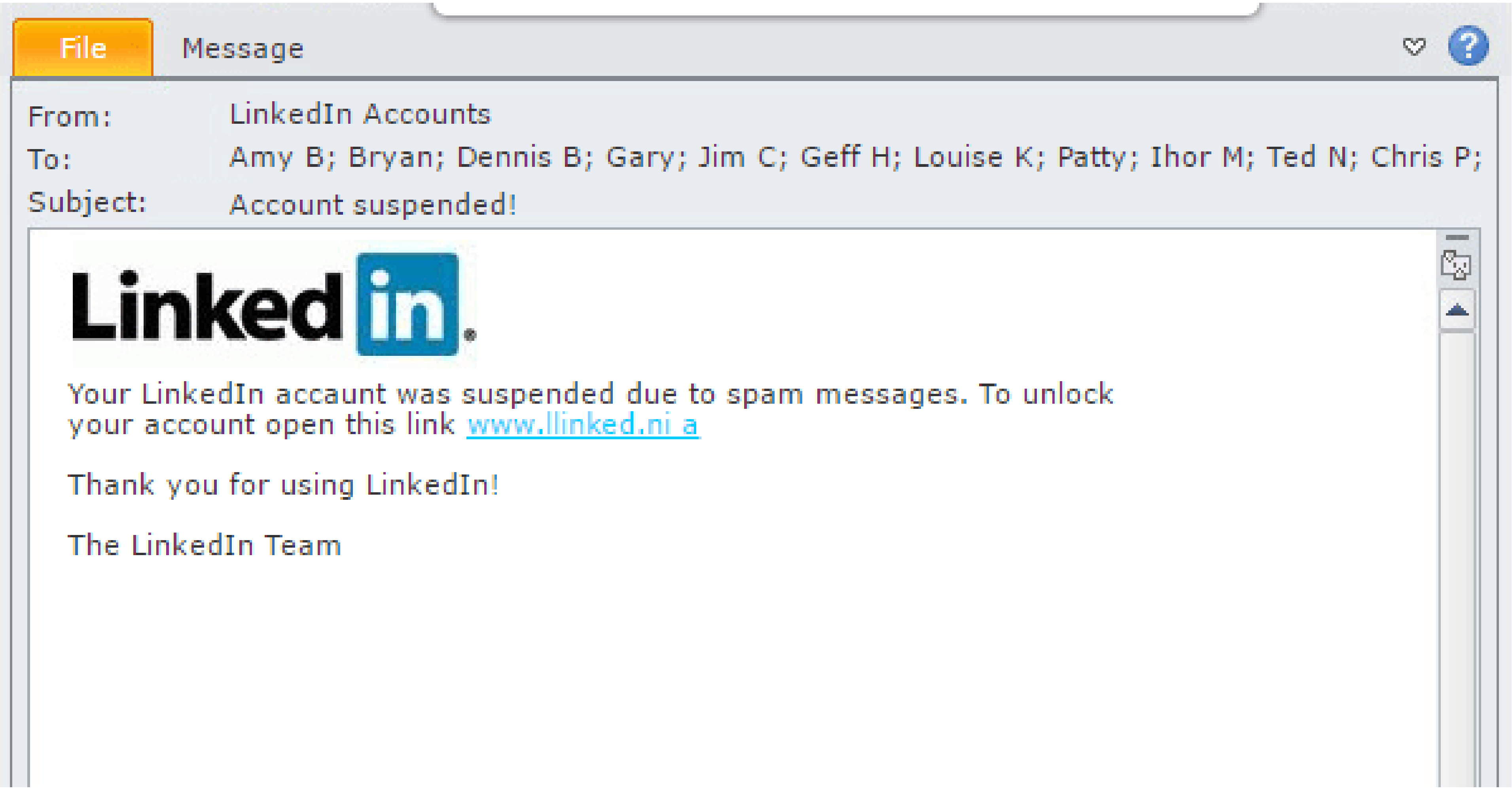
From: **Costco Shipping Agent <manager@cbcbuilding.com>**
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

1998 - 2013
Costco Wholesale Corporation
All rights reserved

E-mail Phishing Attacks



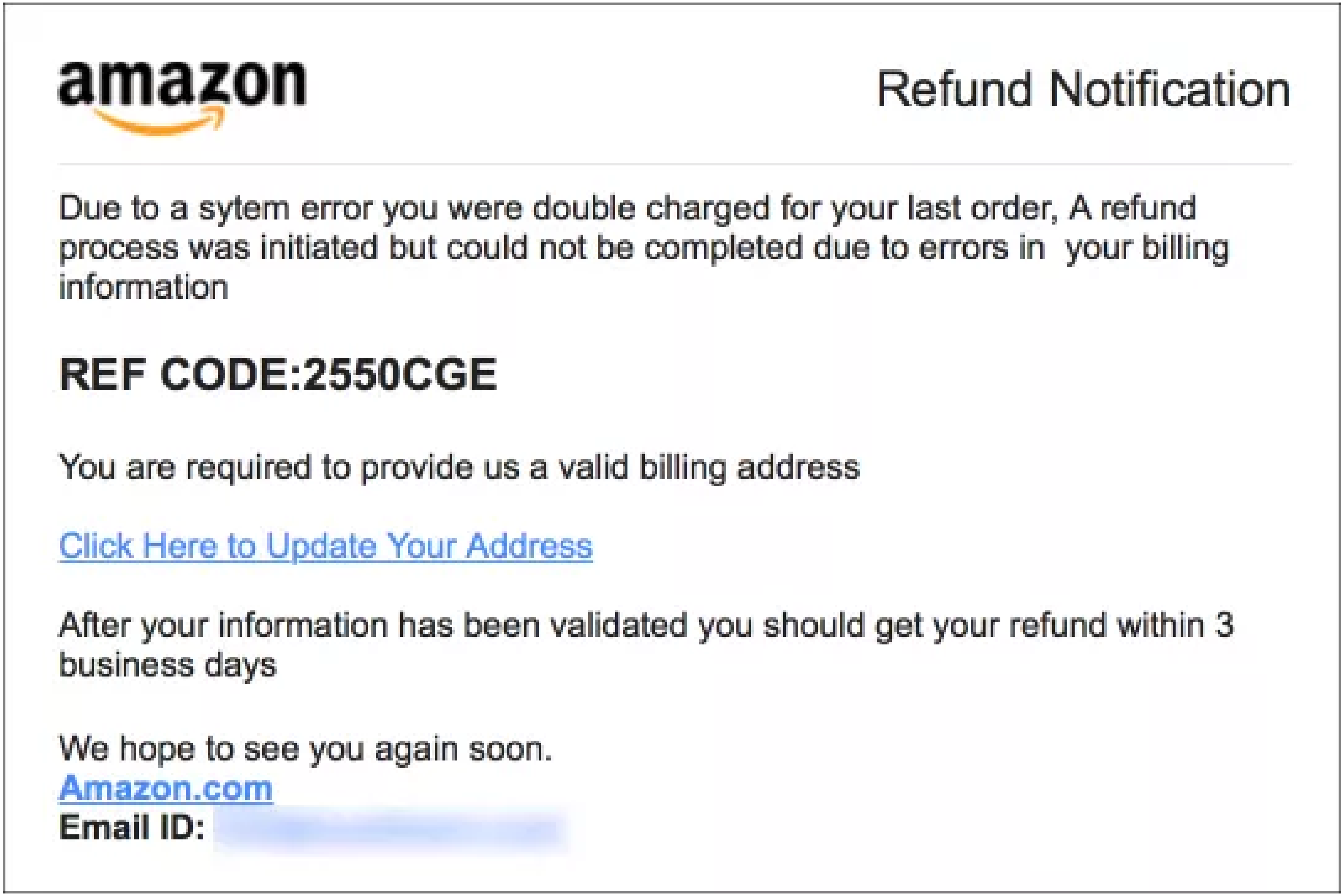
From: LinkedIn Accounts
To: Amy B; Bryan; Dennis B; Gary; Jim C; Geff H; Louise K; Patty; Ihor M; Ted N; Chris P;
Subject: Account suspended!

Linked in

Your LinkedIn accaunt was suspended due to spam messages. To unlock your account open this link www.llinked.ni a

Thank you for using LinkedIn!

The LinkedIn Team



Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID: [redacted]

E-mail Phishing Attacks

- Do you know the sender?
- Did you expect the e-mail?
- Is the subject generic, urgent, or suspicious?
- Are there spelling, grammar, or other indicators that the tone or style is off?
- Does the e-mail require you to take some action, e.g.,
  - Disclose confidential info
  - Click on link
  - Open attachment
- Did you hover over link to see the URL destination?

Do NOT

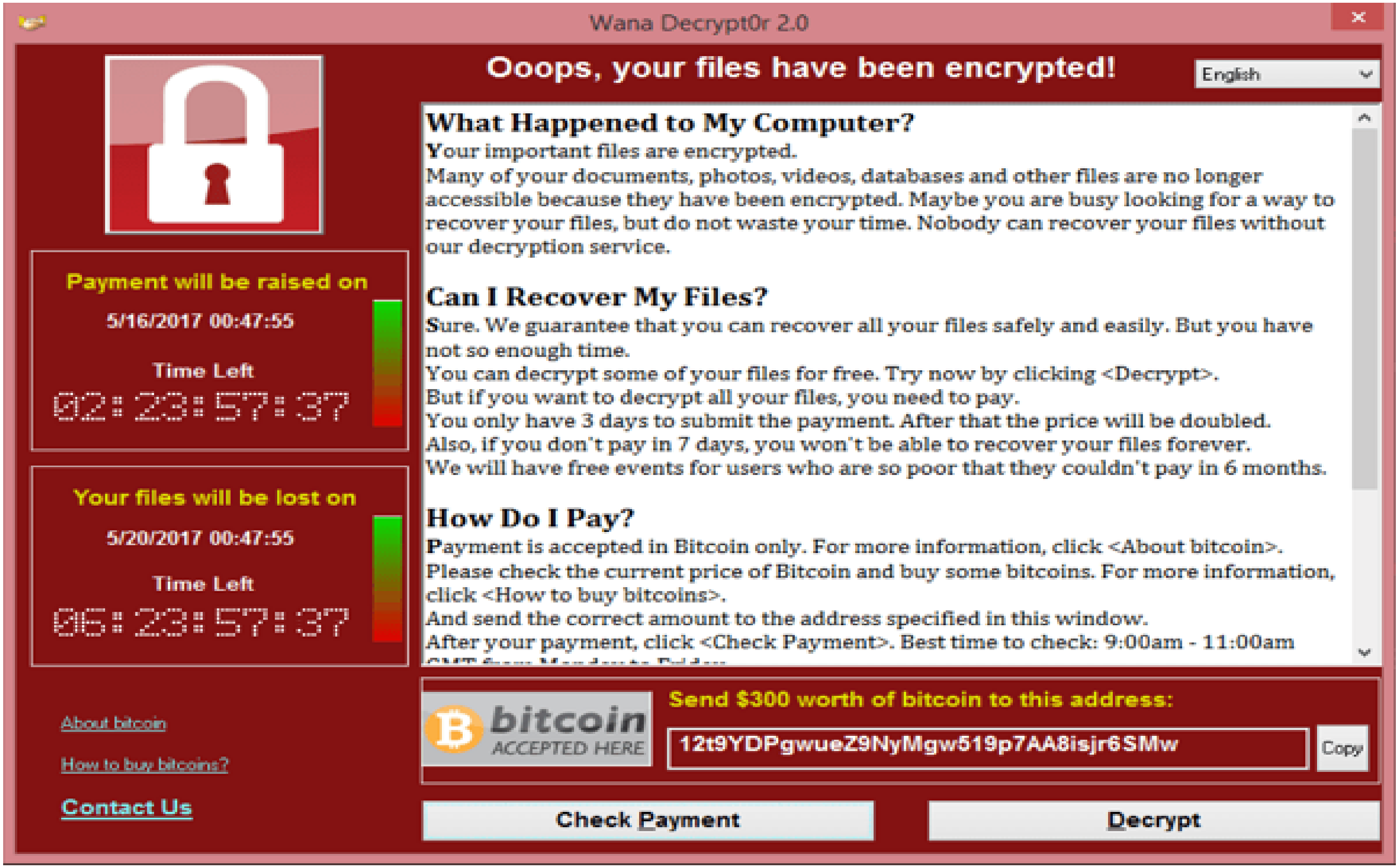
- ***Open attachment***
- ***Click on link***
- ***Input info***

E-mail Phishing Attacks

Practices to consider:

- Be suspicious of e-mails from unknown senders, re sensitive info, or call to action that stresses urgency or importance.
- Be suspicious of e-mails that appear to be from known senders that ask you to do something out of context or unexpected.
- Train staff to recognize suspicious e-mails and where to forward them.
- Never open attachments from unknown senders.
- Hover over links to identify URL.
- Tag external e-mails to make them recognizable to staff.
- Implement security measures to identify and limit phishing attacks.

2. Ransomware Attacks



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

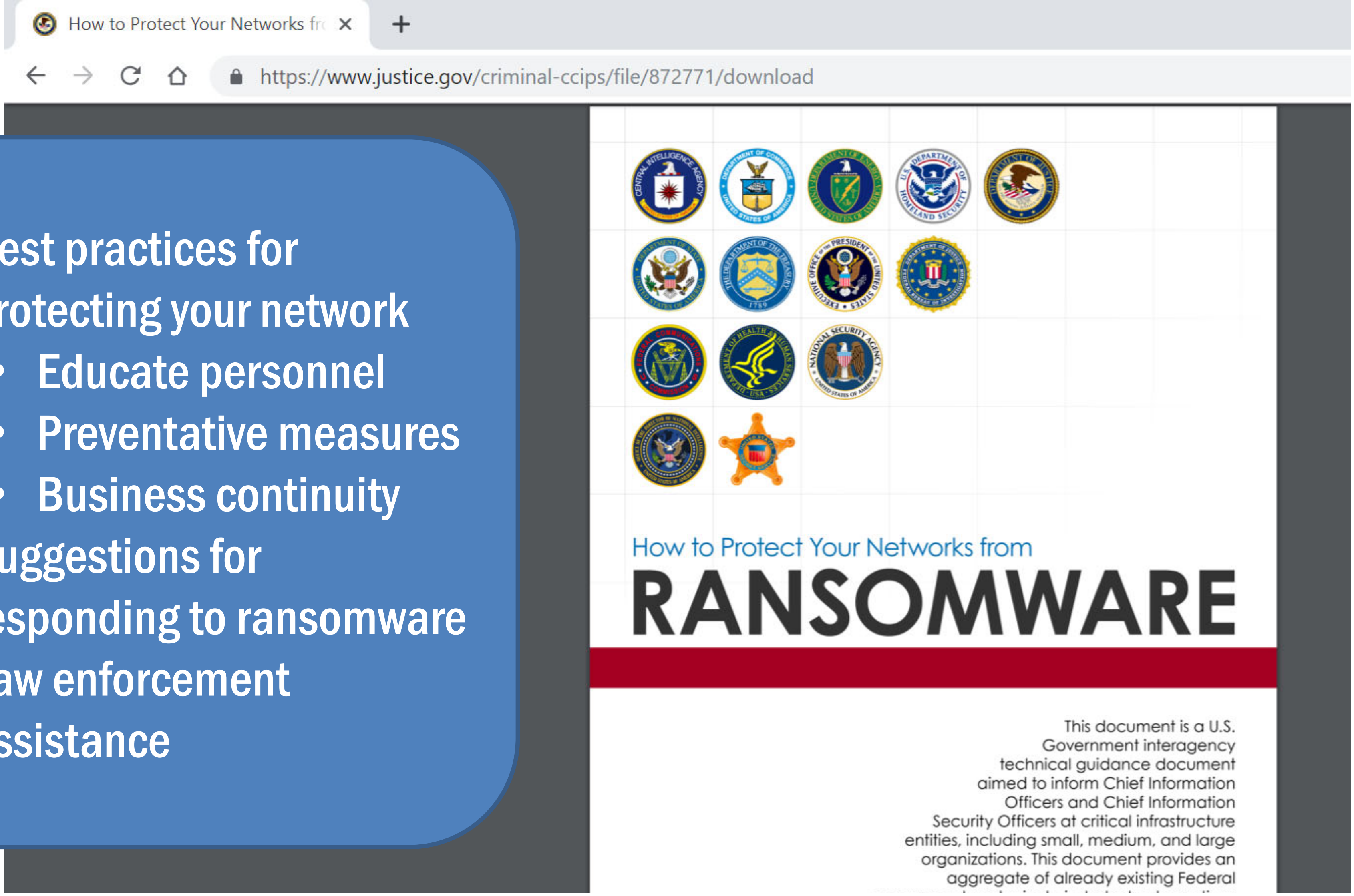
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Ransomware Attacks

- Cybercriminal infects system with malware through phishing or other attacks.
- Malware:
  - Encrypts data, thereby denying access until ransom is paid;
  - Destroys data; or
  - Exfiltrates data.
- No guarantee that paying ransom will allow you to recover data.

https://www.justice.gov/criminal-ccips/file/872771/download

1. Best practices for protecting your network
   - Educate personnel
   - Preventative measures
   - Business continuity
2. Suggestions for responding to ransomware
3. Law enforcement assistance


How to Protect Your Networks fr
https://www.justice.gov/criminal-ccips/file/872771/download

How to Protect Your Networks from

RANSOMWARE

This document is a U.S. Government interagency technical guidance document aimed to inform Chief Information Officers and Chief Information Security Officers at critical infrastructure entities, including small, medium, and large organizations. This document provides an aggregate of already existing Federal

Ransomware Attacks

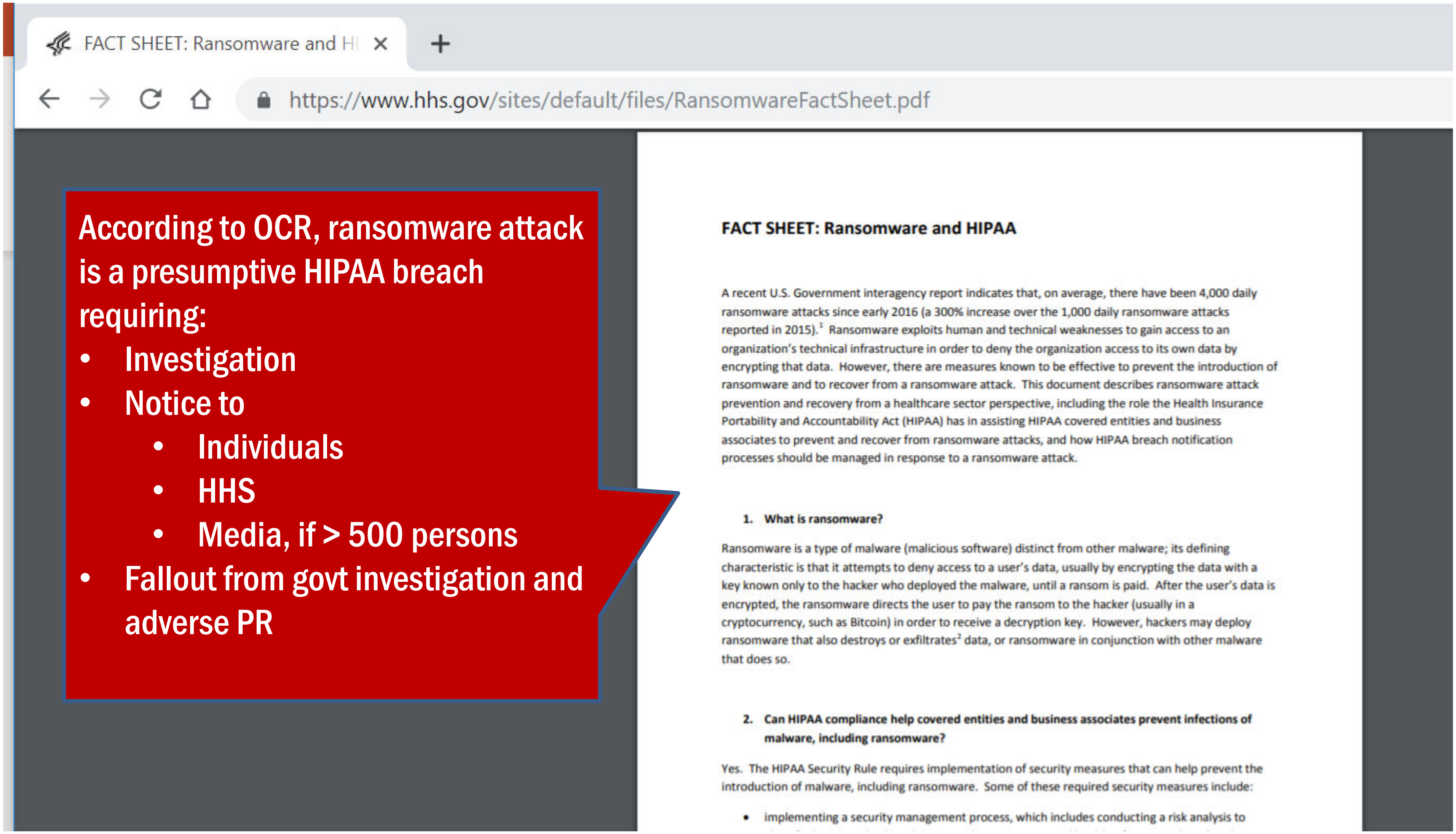
Practices to consider

- Train staff to recognize phishing and other security concerns.
- Warn staff of external e-mails.
- Establish a strong firewall.
- Deploy anti-malware detection and remediation tools.
- Patch software per authorized procedures.
- Use strong username and passwords with multi-facet authentication.
- Limit users who can log in from remote desktops.
- Limit rate of allowed authentication attempts.
- Separate critical and vulnerable systems.
- Determine which computers may access and store critical data.
- Maintain and protect data backups and recovery processes.
- Implement incident response procedures.

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

According to OCR, ransomware attack is a presumptive HIPAA breach requiring:

- Investigation
- Notice to
  - Individuals
  - HHS
  - Media, if > 500 persons
- Fallout from govt investigation and adverse PR


FACT SHEET: Ransomware and H
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. **What is ransomware?**

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. **Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?**

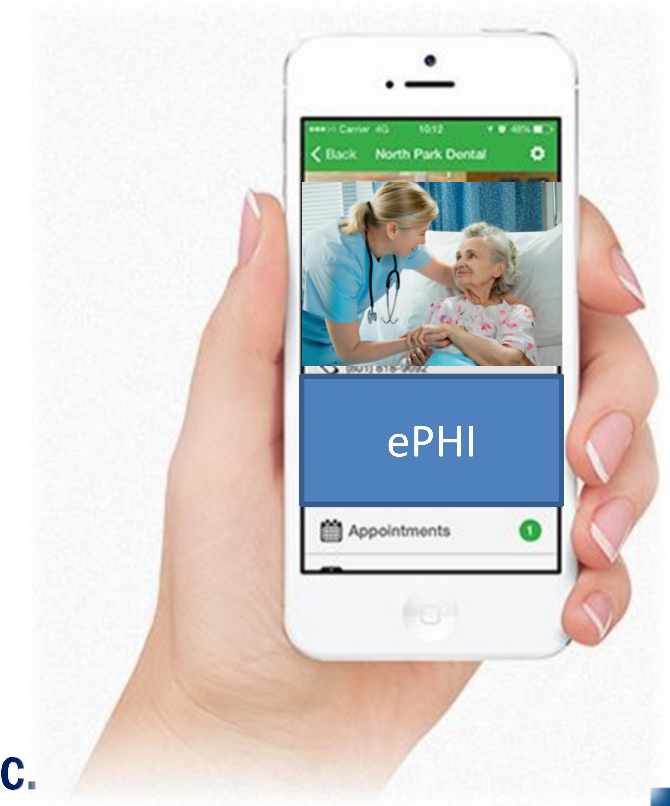
Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to

3. Loss or Theft of Equipment or Data

Loss or Theft of Equipment or Data

- Beware unsecured or unencrypted equipment, e.g.,
  - Equipment (e.g., desktop, copier, fax, medical device, etc.)
  - Laptops, tablets, smart phones
  - USBs/thumb drives
- May contain e-PHI, e.g.,
  - Medical records
  - E-mails or texts
  - Photos or images
  - Videos
  - Voice messages
  - Other?
- May allow access to system, e.g.,
  - Passwords, connections, emails, etc.



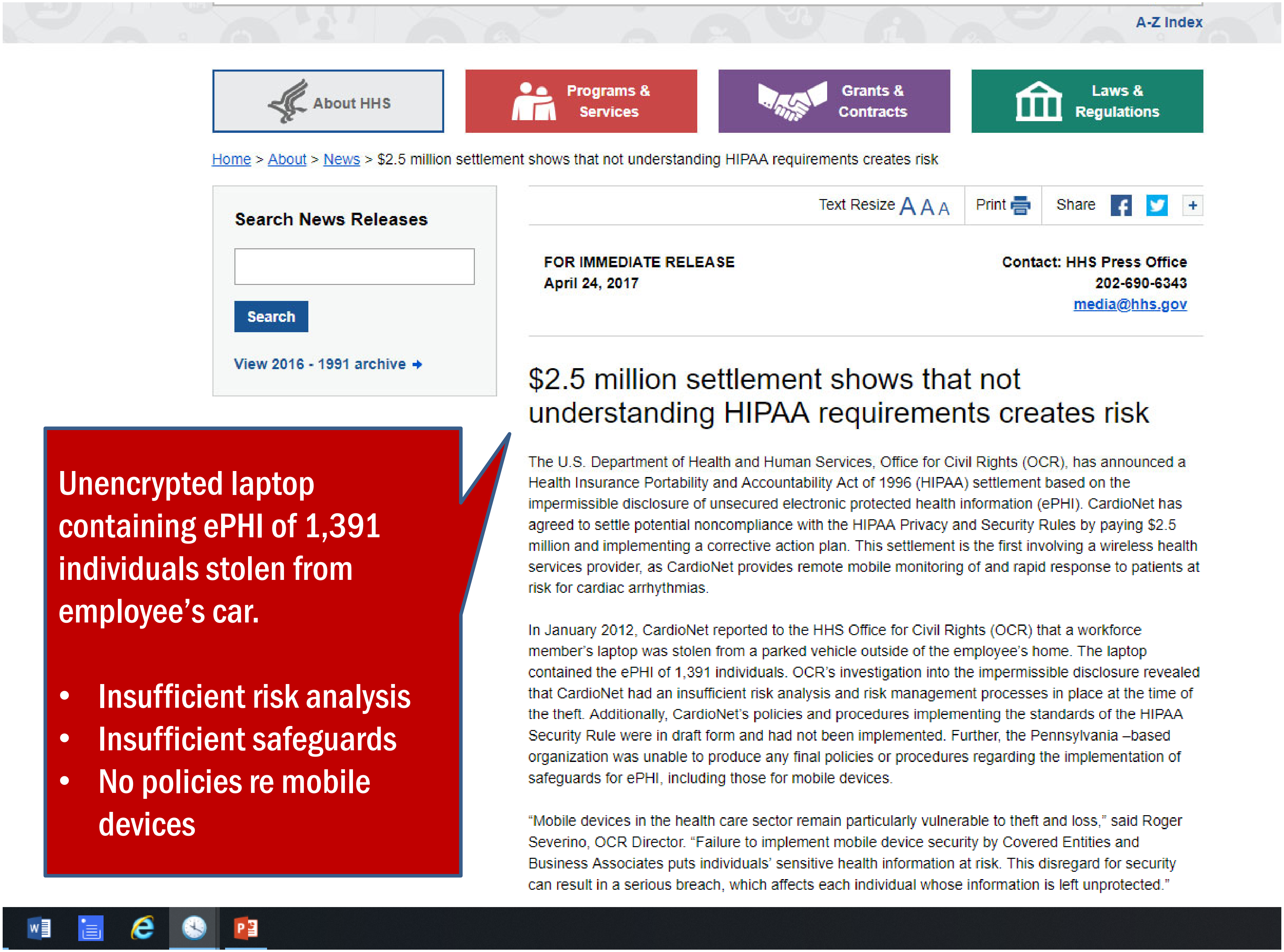
Loss or Theft of Equipment or Data

"[I]n cases where a lost laptop [,USB, phone, or other device containing e-PHI] is recovered, the fact that a forensic analysis of the computer shows that its information was not accessed is a relevant consideration for the risk assessment, and entities in such situations may be able to demonstrate a low probability that the information has been compromised.... [I]f a computer is lost or stolen, we do not consider it reasonable to delay breach notification based on the hope that the computer will be recovered."

(HHS commentary to the HIPAA omnibus rule, 78 FR 5646)

The corollary:

Loss of unencrypted device containing e-PHI is presumptively a reportable HIPAA breach.



FOR IMMEDIATE RELEASE
April 24, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

$2.5 million settlement shows that not understanding HIPAA requirements creates risk

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the impermissible disclosure of unsecured electronic protected health information (ePHI). CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan. This settlement is the first involving a wireless health services provider, as CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January 2012, CardioNet reported to the HHS Office for Civil Rights (OCR) that a workforce member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management processes in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania –based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

"Mobile devices in the health care sector remain particularly vulnerable to theft and loss," said Roger Severino, OCR Director. "Failure to implement mobile device security by Covered Entities and Business Associates puts individuals' sensitive health information at risk. This disregard for security can result in a serious breach, which affects each individual whose information is left unprotected."

Unencrypted laptop containing ePHI of 1,391 individuals stolen from employee's car.

- Insufficient risk analysis
- Insufficient safeguards
- No policies re mobile devices

Loss or Theft of Equipment or Data

HHS Examples

“A covered entity disposed of several hard drives containing electronic protected health information in an unsecured dumpster, in violation of [HIPAA]. HHS’s investigation reveals that the covered entity had failed to implement any policies and procedures to reasonably and appropriately safeguard protected health information during the disposal process.”

“A covered entity’s employee lost an unencrypted laptop that contained unsecured protected health information. HHS’s investigation reveals the covered entity feared its reputation would be harmed if information about the incident became public and, therefore, decided not to provide notification as required by § 164.400 et seq.”

(HHS commentary to breach notification rule, 75 FR 40879)

Consequences

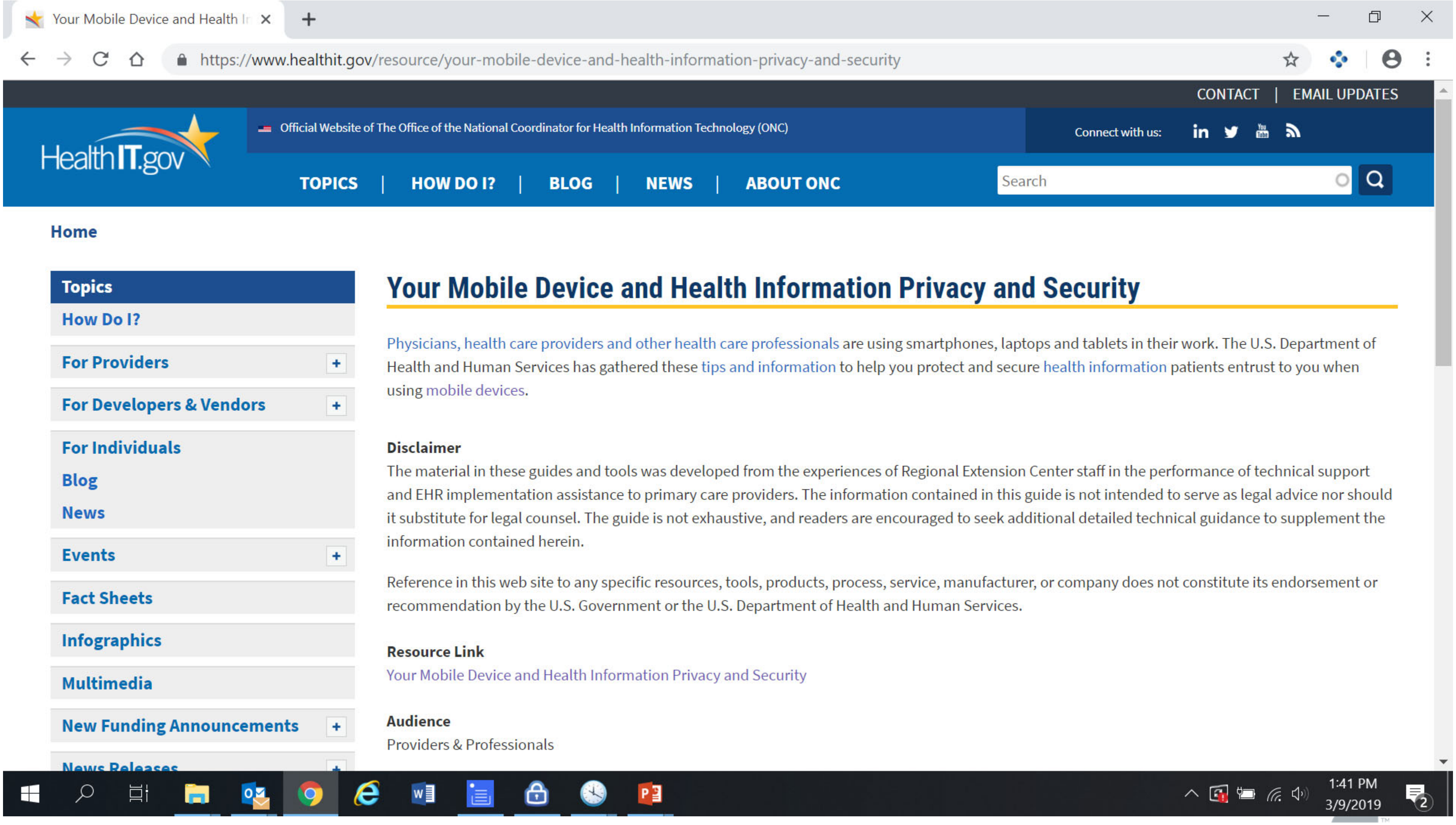
- Willful neglect.
- Mandatory penalties of:
  - If correct w/in 30 days:
    - $11,182 to $57,051 per violation
    - Max $114,102 per type per year.
  - At least $57,051 per violation if don’t correct w/in 30 days
    - $57,051 per violation
    - Max $1,711,533 per type per year

HOLLAND&HART LLP

Loss or Theft of Equipment or Data

- Practices to consider:
  - Train personnel.
  - Encrypt sensitive data.
  - Use secure server.
  - Implement proven backup and restoration processes.
  - Acquire and use data loss prevention tools.
  - Implement safeguard policy for mobile devices.
  - Maintain accurate asset inventory.
  - Implement process to remove sensitive info from all devices before retired.

Beware Mobile Devices


Your Mobile Device and Health In
https://www.healthit.gov/resource/your-mobile-device-and-health-information-privacy-and-security
CONTACT | EMAIL UPDATES
HealthIT.gov
Official Website of The Office of the National Coordinator for Health Information Technology (ONC)
Connect with us:
TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC
Search
Home
Topics
How Do I?
For Providers +
For Developers & Vendors +
For Individuals
Blog
News
Events +
Fact Sheets
Infographics
Multimedia
New Funding Announcements +
News Releases +
1:41 PM
3/9/2019

Your Mobile Device and Health Information Privacy and Security

Physicians, health care providers and other health care professionals are using smartphones, laptops and tablets in their work. The U.S. Department of Health and Human Services has gathered these tips and information to help you protect and secure health information patients entrust to you when using mobile devices.

Disclaimer
The material in these guides and tools was developed from the experiences of Regional Extension Center staff in the performance of technical support and EHR implementation assistance to primary care providers. The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Reference in this web site to any specific resources, tools, products, process, service, manufacturer, or company does not constitute its endorsement or recommendation by the U.S. Government or the U.S. Department of Health and Human Services.

Resource Link
Your Mobile Device and Health Information Privacy and Security

Audience
Providers & Professionals

Mobile Devices: Tips to Protect and Secure Health Information

- Use a password or other user authentication.
- Install and enable encryption.
- Install and activate wiping and/or remote disabling.
- Disable and do not install file- sharing applications.
- Install and enable a firewall.
- Install and enable security software.
- Keep security software up to date.
- Research mobile applications (apps) before downloading.
- Maintain physical control of your mobile device.
- Use adequate security to send or receive health information over public Wi-Fi networks.
- Delete all stored health information before discarding or reusing the mobile device.

Loss or Theft of Equipment or Data

Questions to consider:

- Does my equipment contain confidential or sensitive information?
- Is the device secured through, e.g., strong password protection?
- Is the information encrypted?
- May I or do I need to take the equipment with me?
- Is there a secure virtual private network (VPN) that I can use?

4. Insider Accidental or Intentional Data Loss

Insider Accidental or Intentional Data Loss

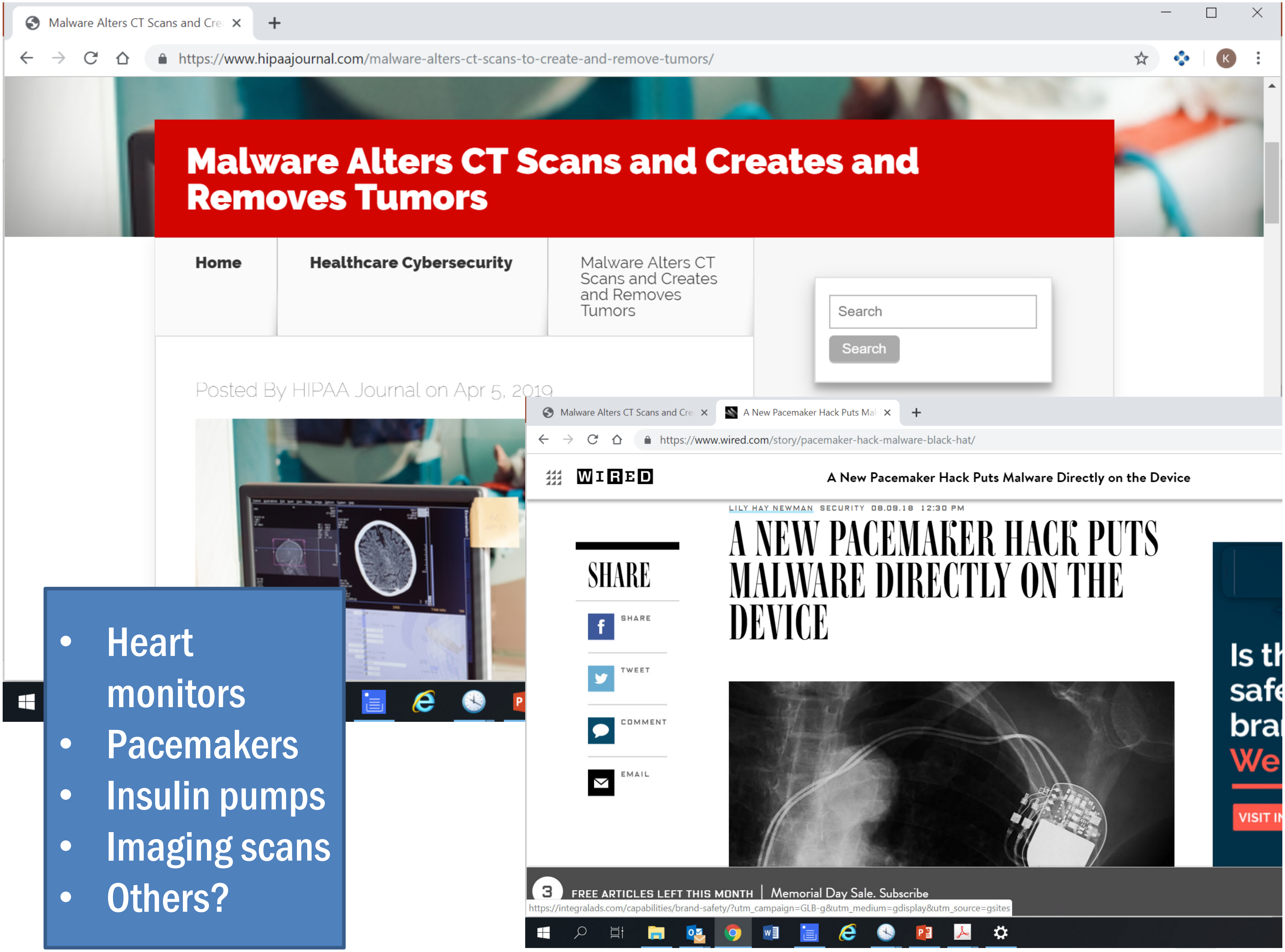
Common vulnerabilities

- Files e-mailed to wrong address
- Inadequate monitoring, tracking and auditing
  - Access to e-mail and file storage
  - E-mailing and uploading data outside organization
- Inadequate physical access control
- Inadequate training

Practices to consider

- Train personnel
- Workforce access limits and audits
- Implement privileged access management tools
- Implement and use data loss prevention tools.
- Backup

5. Attacks Against Connected Medical Devices



Malware Alters CT Scans and Cre

https://www.hipaajournal.com/malware-alters-ct-scans-to-create-and-remove-tumors/

Malware Alters CT Scans and Creates and Removes Tumors

Home
Healthcare Cybersecurity
Malware Alters CT Scans and Creates and Removes Tumors
Search
Search

Posted By HIPAA Journal on Apr 5, 2019

Malware Alters CT Scans and Cre
A New Pacemaker Hack Puts Mal

https://www.wired.com/story/pacemaker-hack-malware-black-hat/

WIRED
A New Pacemaker Hack Puts Malware Directly on the Device

LILY HAY NEWMAN SECURITY 08.09.18 12:30 PM

A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE

SHARE
SHARE
TWEET
COMMENT
EMAIL
Is th
safe
bra
We
VISIT I

3 FREE ARTICLES LEFT THIS MONTH | Memorial Day Sale. Subscribe

https://integralads.com/capabilities/brand-safety/?utm_campaign=GLB-g&utm_medium=gdisplay&utm_source=gsites

- Heart monitors
- Pacemakers
- Insulin pumps
- Imaging scans
- Others?

Attacks Against Connected Medical Devices

Common vulnerabilities

- Patches not implemented
- Outdated equipment
- Most devices cannot be monitored by intrusion detection system
- Cybersecurity profile info may be unavailable
- Wide variance in devices

Practices to consider

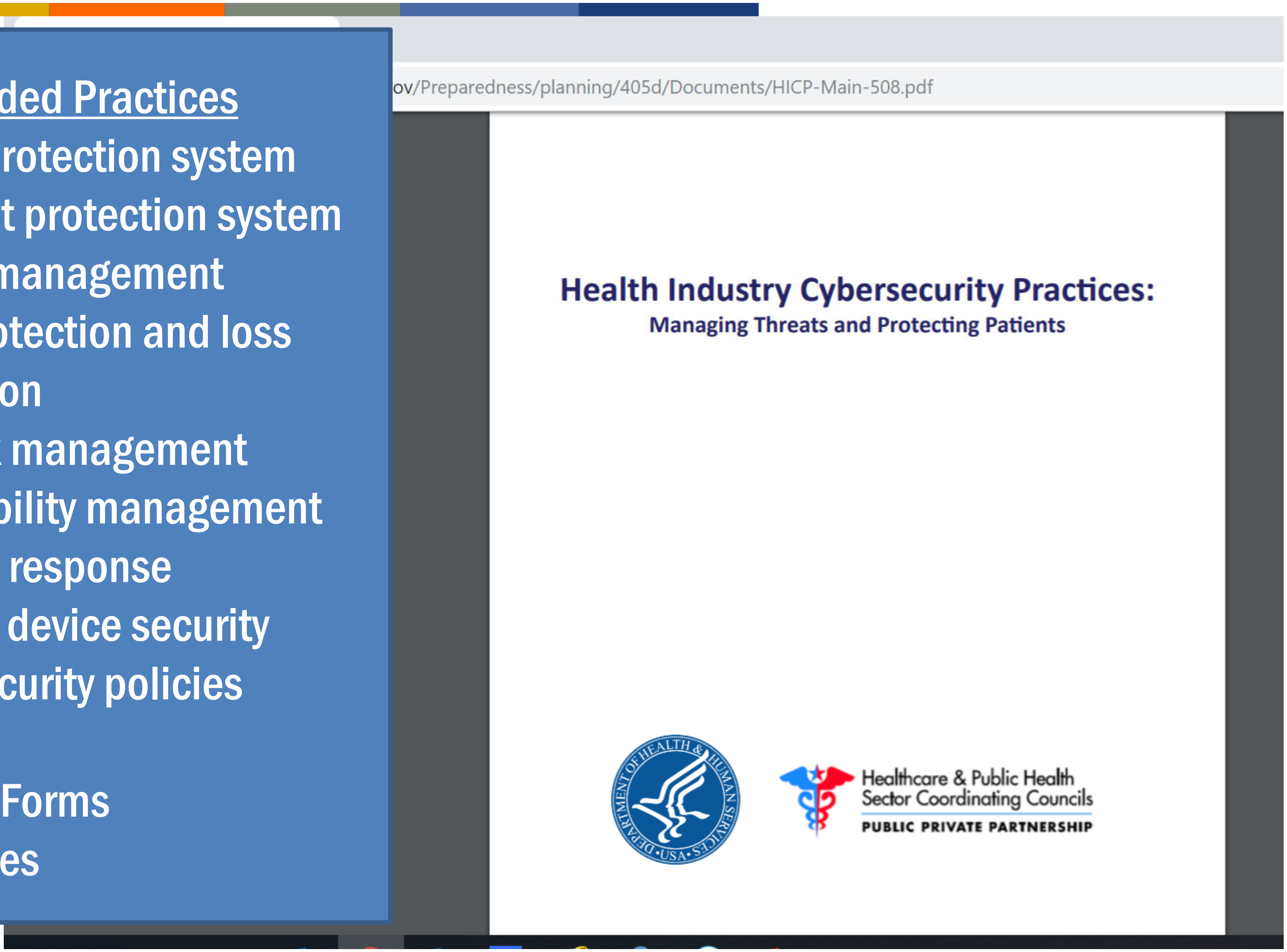
- Communicate with device mfr
- Follow mfr instructions
- Patch devices after patch has been validated and tested
- Assess security on networked devices
- Assess devices risks
- Contract carefully
- Access controls for outsiders

https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Recommended Practices

1. E-mail protection system
2. Endpoint protection system
3. Access management
4. Data protection and loss prevention
5. Network management
6. Vulnerability management
7. Incident response
8. Medical device security
9. Cybersecurity policies

- Sample Forms
- Resources



ov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

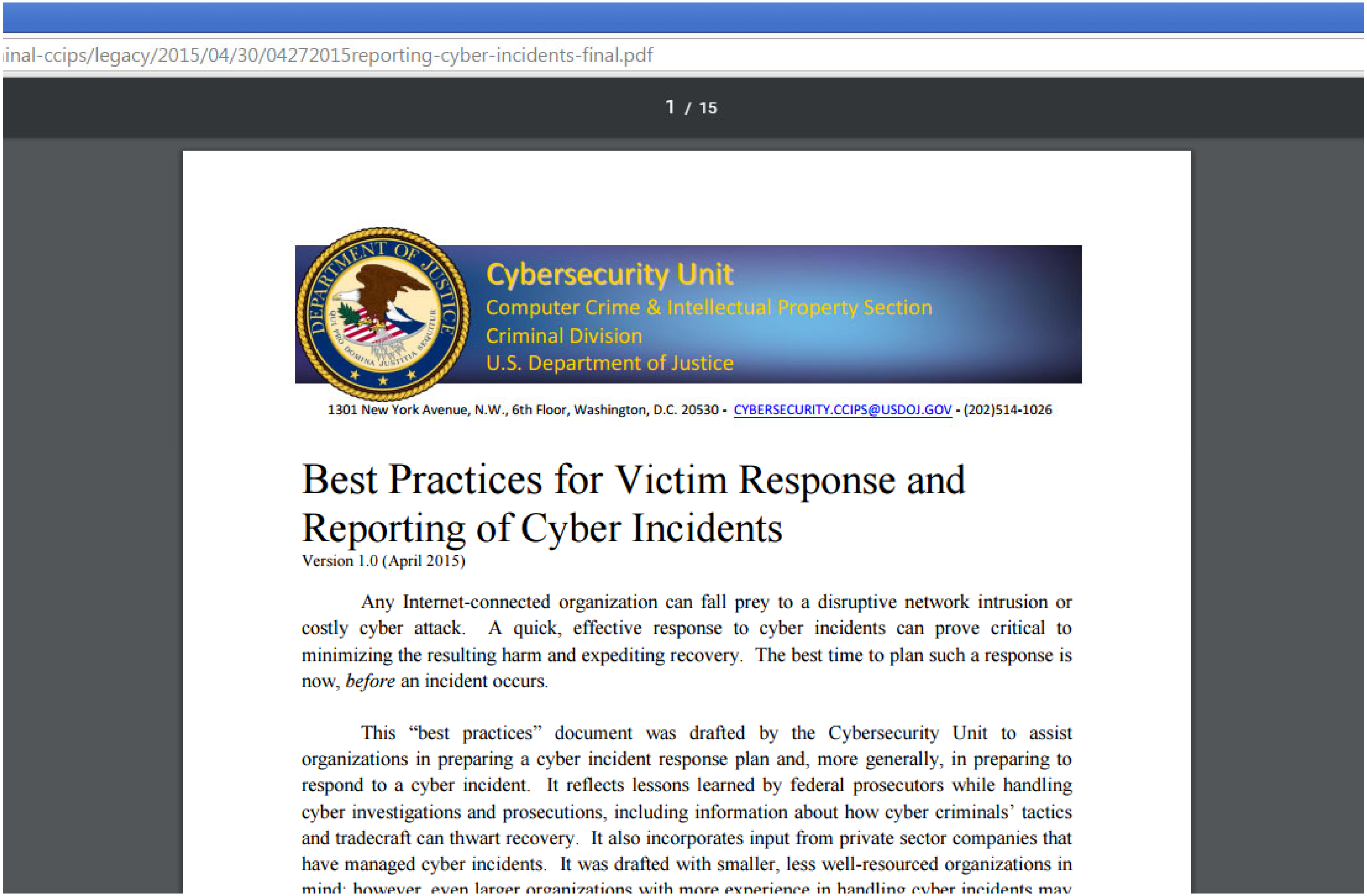
Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP

www.justice.gov/sites/default/files/criminal- ccips/legacy/
2015/04/30/04272015reporting-cyber-incidents-final.pdf


inal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf
1 / 15

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents

Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* an incident occurs.

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may

Health Insurance Portability and Accountability Act ("HIPAA")

- 45 CFR 164
  - .500: Privacy Rule
  - .300: Security Rule
  - .400: Breach Notification Rule
- HITECH Act
  - Modified HIPAA
  - Implemented by HIPAA Omnibus Rule

HOLLAND&HART LLP

HIPAA Security Rule

- Risk assessment
- Implement safeguards.
  - Administrative
  - Technical, including encryption
  - Physical
- Execute business associate agreements.

(45 CFR 164.301 et seq.; *see* WSA 35-2-615)

Protect ePHI:

- Confidentiality
- Integrity
- Availability

Risk Assessment

Requirement

- Must conduct and document an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

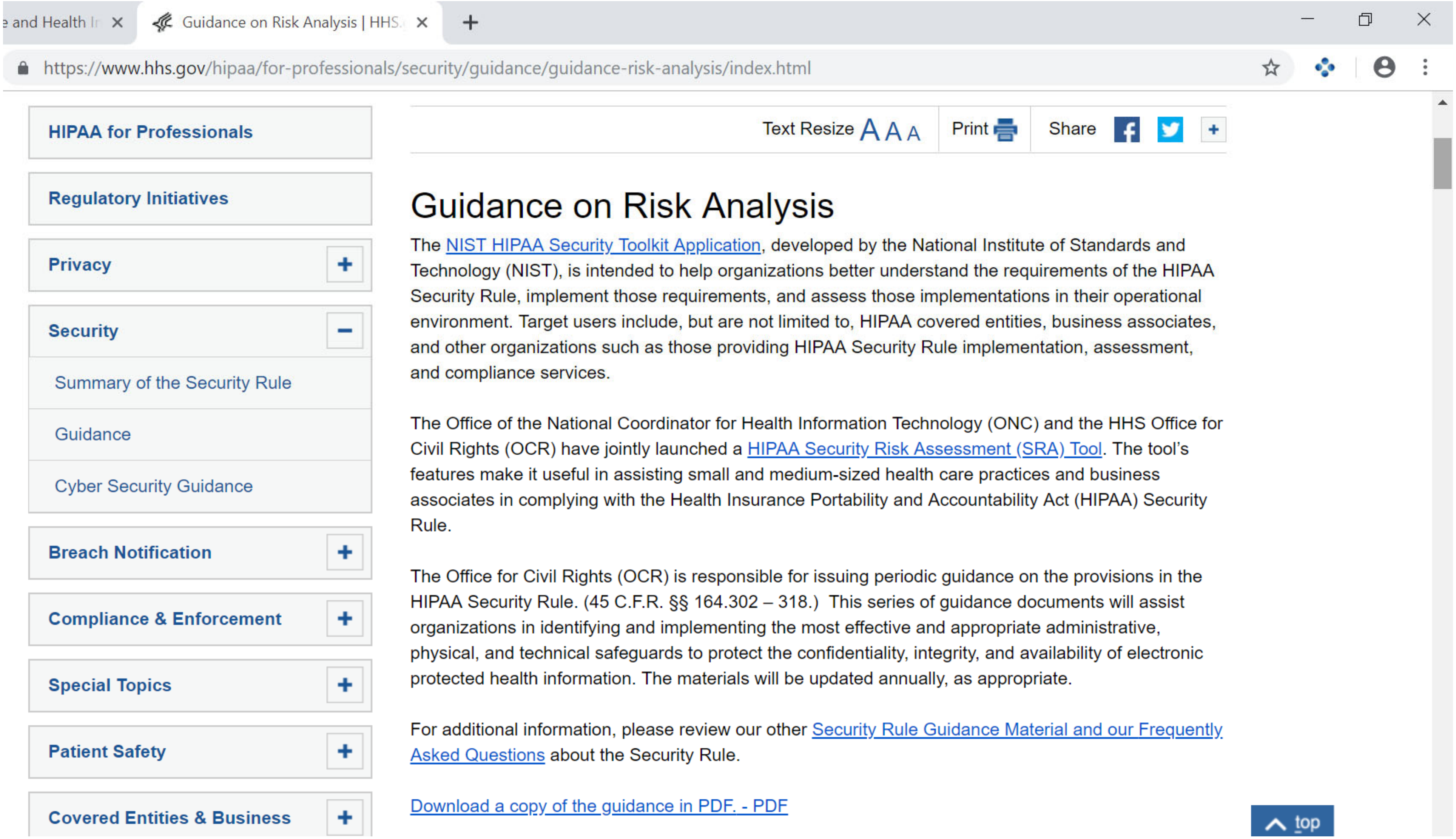
(45 CFR 164.308(a)(1))

- Ongoing process.

Elements

- Scope includes all ePHI in any format, including hard drives, portable media, mobile devices, servers, transmission, storage, networks, etc.
- Track flow of ePHI
- Identify threats and vulnerabilities
- Asses current security measures
- Assess likelihood of threat
- Determine level of risk
- Confirm and implement plan

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html


e and Health In ×
Guidance on Risk Analysis | HHS. ×
+
https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html
HIPAA for Professionals
Regulatory Initiatives
Privacy +
Security −
Summary of the Security Rule
Guidance
Cyber Security Guidance
Breach Notification +
Compliance & Enforcement +
Special Topics +
Patient Safety +
Covered Entities & Business +
Text Resize A A A
Print
Share
+
top

Guidance on Risk Analysis

The NIST HIPAA Security Toolkit Application, developed by the National Institute of Standards and Technology (NIST), is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services.

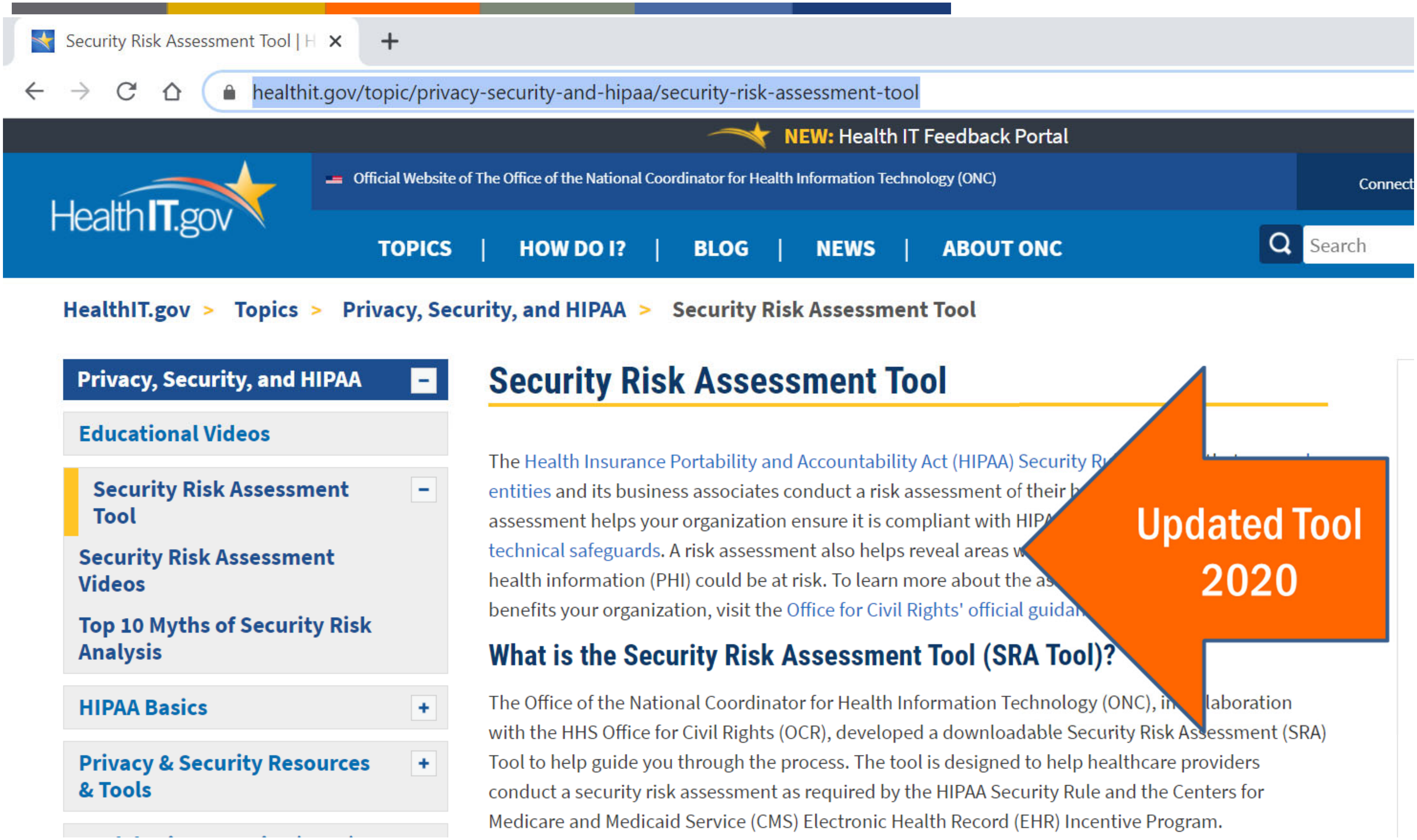
The Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) have jointly launched a HIPAA Security Risk Assessment (SRA) Tool. The tool's features make it useful in assisting small and medium-sized health care practices and business associates in complying with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The Office for Civil Rights (OCR) is responsible for issuing periodic guidance on the provisions in the HIPAA Security Rule. (45 C.F.R. §§ 164.302 – 318.) This series of guidance documents will assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. The materials will be updated annually, as appropriate.

For additional information, please review our other Security Rule Guidance Material and our Frequently Asked Questions about the Security Rule.

Download a copy of the guidance in PDF. - PDF

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool


Security Risk Assessment Tool | H
healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
NEW: Health IT Feedback Portal
HealthIT.gov
Official Website of The Office of the National Coordinator for Health Information Technology (ONC)
Connect
TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC
Search

HealthIT.gov > Topics > Privacy, Security, and HIPAA > Security Risk Assessment Tool

Privacy, Security, and HIPAA −
Educational Videos
Security Risk Assessment Tool −
Security Risk Assessment Videos
Top 10 Myths of Security Risk Analysis
HIPAA Basics +
Privacy & Security Resources & Tools +

Security Risk Assessment Tool

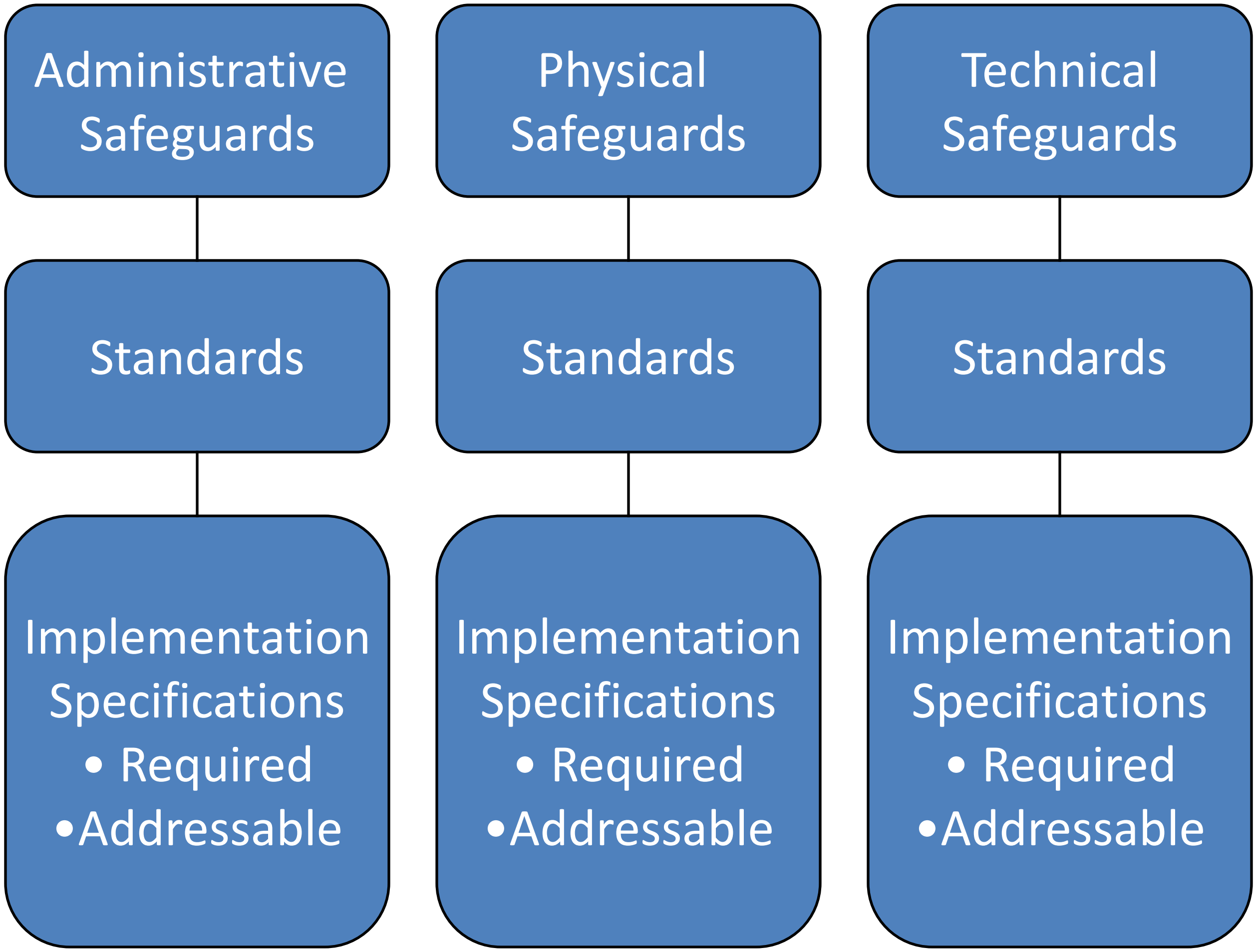
The Health Insurance Portability and Accountability Act (HIPAA) Security R
entities and its business associates conduct a risk assessment of their h
assessment helps your organization ensure it is compliant with HIPA
technical safeguards. A risk assessment also helps reveal areas w
health information (PHI) could be at risk. To learn more about the as
benefits your organization, visit the Office for Civil Rights' official guida

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in laboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program.

Updated Tool 2020

Safeguards



Administrative Safeguards

Standards

Implementation Specifications
- Required
- Addressable

Physical Safeguards

Standards

Implementation Specifications
- Required
- Addressable

Technical Safeguards

Standards

Implementation Specifications
- Required
- Addressable

Security Rule: Administrative Safeguards

- Assign security officer.
- Implement policies, procedures and safeguards to minimize risks.
- Sanction workforce members who violate policies.
- Process for authorizing or terminating access to e-PHI.
- Train workforce members on security requirements.
- Process for responding to security incidents.
- Review or audit information system activity.
- Establish backup plans, disaster recovery plans, etc.
- Periodically evaluate security measures.

(45 CFR 164.308)

Security Rule:
Physical Safeguards

- Limit access to physical facilities and devices containing e-PHI.
- Document repairs and modifications to facilities.
- Secure workstations.
- Implement policies concerning proper use of workstations.
- Implement policies concerning the flow of e-PHI into and out of the facility.
- Implement policies for disposal of e-PHI.
- Create a backup copy of e-PHI.

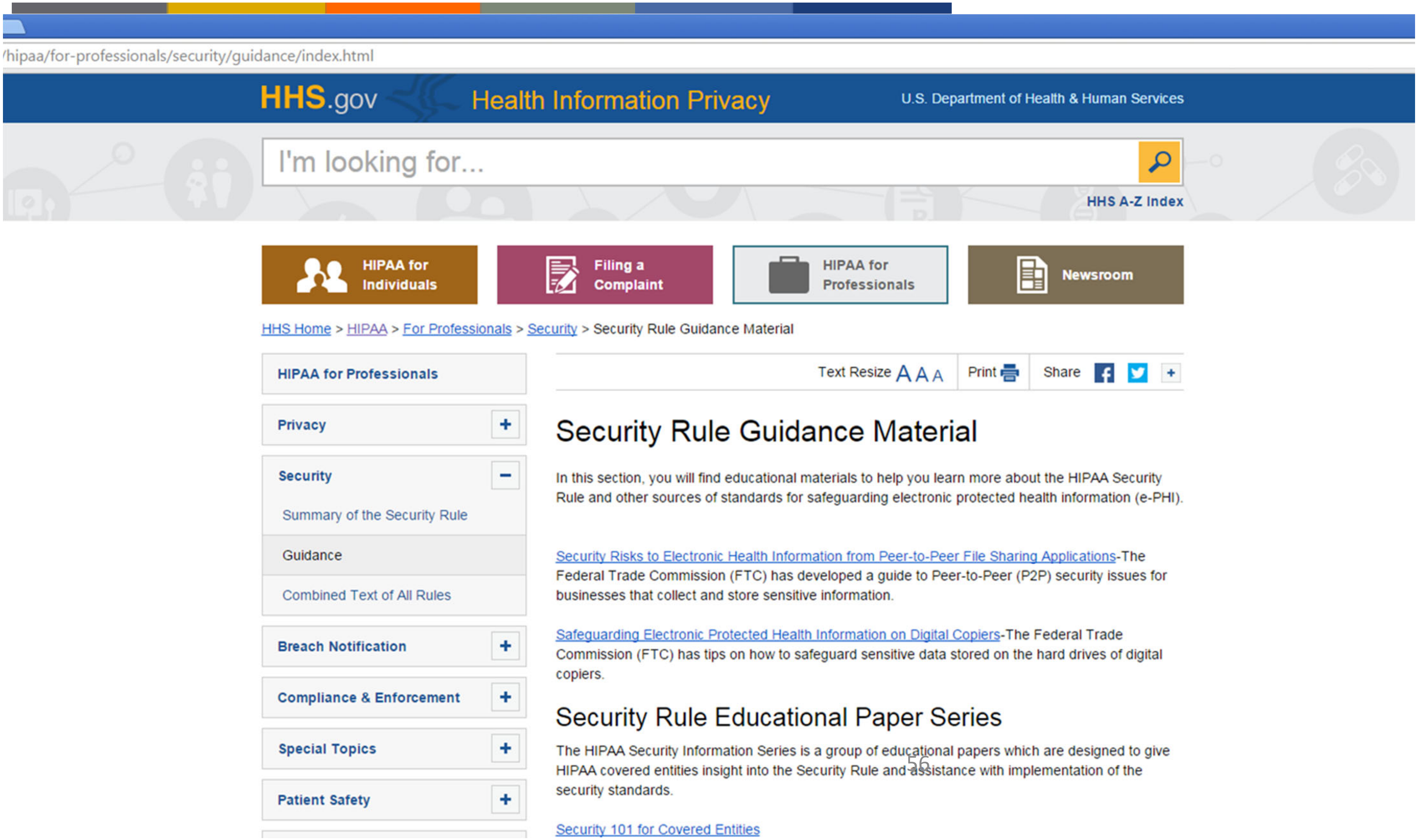
(45 CFR 164.310)

Security Rule: Technical Safeguards

- Assign unique names or numbers to track users.
- Implement automatic logoff process.
- Use encryption and decryption, where appropriate.
- Implement systems to audit use of e-PHI.
- Implement safeguards to protect e-PHI from alteration or destruction.
- Implement methods to ensure e-PHI has not been altered or destroyed.
- Implement verification process.
- Protect data during transmission.

(45 CFR 164.312)

https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html


/hipaa/for-professionals/security/guidance/index.html
HHS.gov
Health Information Privacy
U.S. Department of Health & Human Services
I'm looking for...
HHS A-Z Index
HIPAA for Individuals
Filing a Complaint
HIPAA for Professionals
Newsroom
HHS Home > HIPAA > For Professionals > Security > Security Rule Guidance Material
HIPAA for Professionals
Privacy +
Security −
Summary of the Security Rule
Guidance
Combined Text of All Rules
Breach Notification +
Compliance & Enforcement +
Special Topics +
Patient Safety +
Text Resize A A A
Print
Share
+

Security Rule Guidance Material

In this section, you will find educational materials to help you learn more about the HIPAA Security Rule and other sources of standards for safeguarding electronic protected health information (e-PHI).

Security Risks to Electronic Health Information from Peer-to-Peer File Sharing Applications-The Federal Trade Commission (FTC) has developed a guide to Peer-to-Peer (P2P) security issues for businesses that collect and store sensitive information.

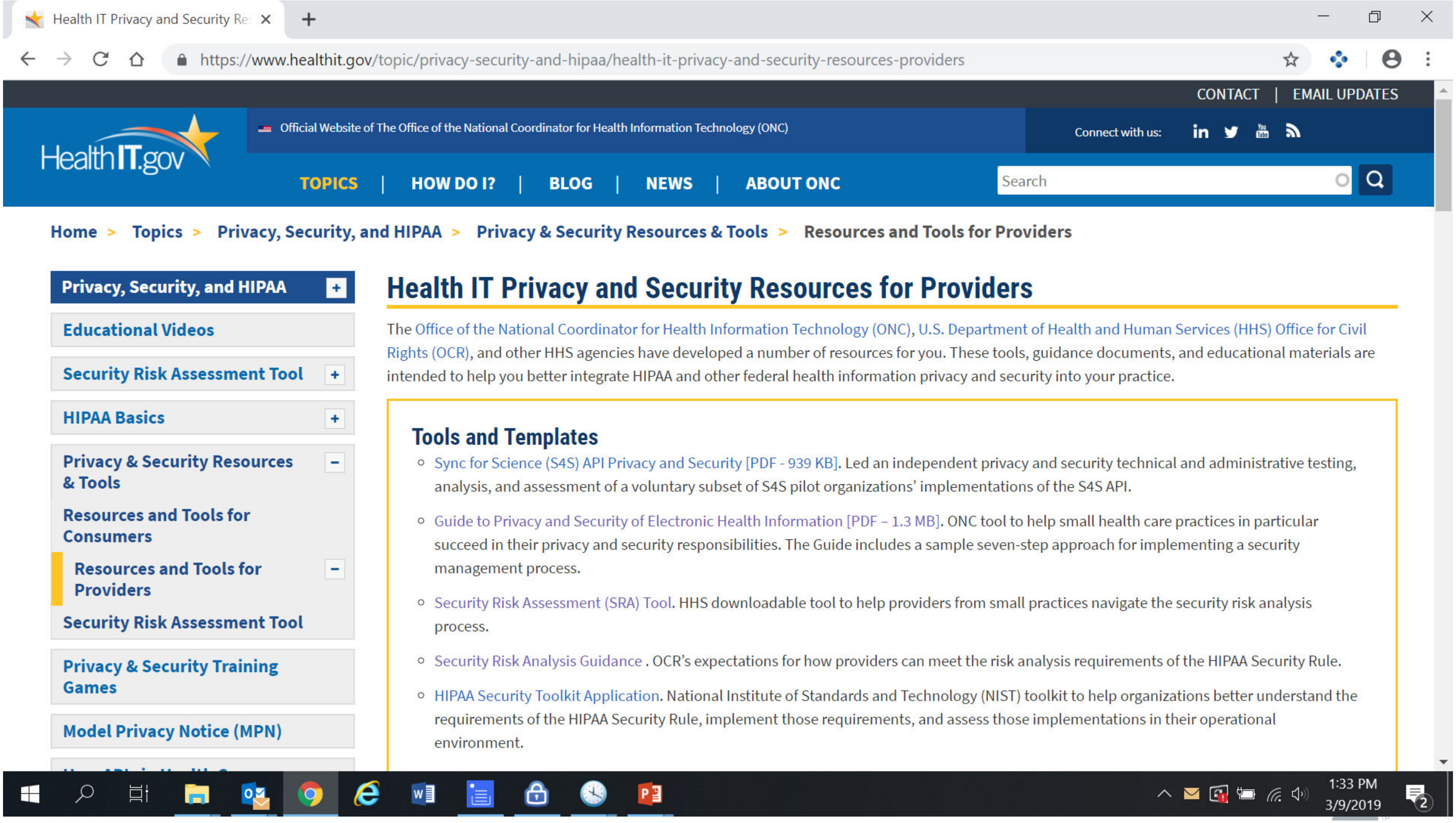
Safeguarding Electronic Protected Health Information on Digital Copiers-The Federal Trade Commission (FTC) has tips on how to safeguard sensitive data stored on the hard drives of digital copiers.

Security Rule Educational Paper Series

The HIPAA Security Information Series is a group of educational papers which are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards.

Security 101 for Covered Entities

https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers


Health IT Privacy and Security Re ×
https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers
CONTACT | EMAIL UPDATES
HealthIT.gov
Official Website of The Office of the National Coordinator for Health Information Technology (ONC)
Connect with us:
TOPICS | HOW DO I? | BLOG | NEWS | ABOUT ONC
Search
Home > Topics > Privacy, Security, and HIPAA > Privacy & Security Resources & Tools > Resources and Tools for Providers
Privacy, Security, and HIPAA +
Educational Videos
Security Risk Assessment Tool +
HIPAA Basics +
Privacy & Security Resources & Tools −
Resources and Tools for Consumers
Resources and Tools for Providers −
Security Risk Assessment Tool
Privacy & Security Training Games
Model Privacy Notice (MPN)
1:33 PM
3/9/2019

Health IT Privacy and Security Resources for Providers

The Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and other HHS agencies have developed a number of resources for you. These tools, guidance documents, and educational materials are intended to help you better integrate HIPAA and other federal health information privacy and security into your practice.

Tools and Templates

- Sync for Science (S4S) API Privacy and Security [PDF - 939 KB]. Led an independent privacy and security technical and administrative testing, analysis, and assessment of a voluntary subset of S4S pilot organizations' implementations of the S4S API.
- Guide to Privacy and Security of Electronic Health Information [PDF – 1.3 MB]. ONC tool to help small health care practices in particular succeed in their privacy and security responsibilities. The Guide includes a sample seven-step approach for implementing a security management process.
- Security Risk Assessment (SRA) Tool. HHS downloadable tool to help providers from small practices navigate the security risk analysis process.
- Security Risk Analysis Guidance . OCR's expectations for how providers can meet the risk analysis requirements of the HIPAA Security Rule.
- HIPAA Security Toolkit Application. National Institute of Standards and Technology (NIST) toolkit to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.

Encryption

- Encryption is an addressable standard per 45 CFR 164.312:

  (e)(1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.

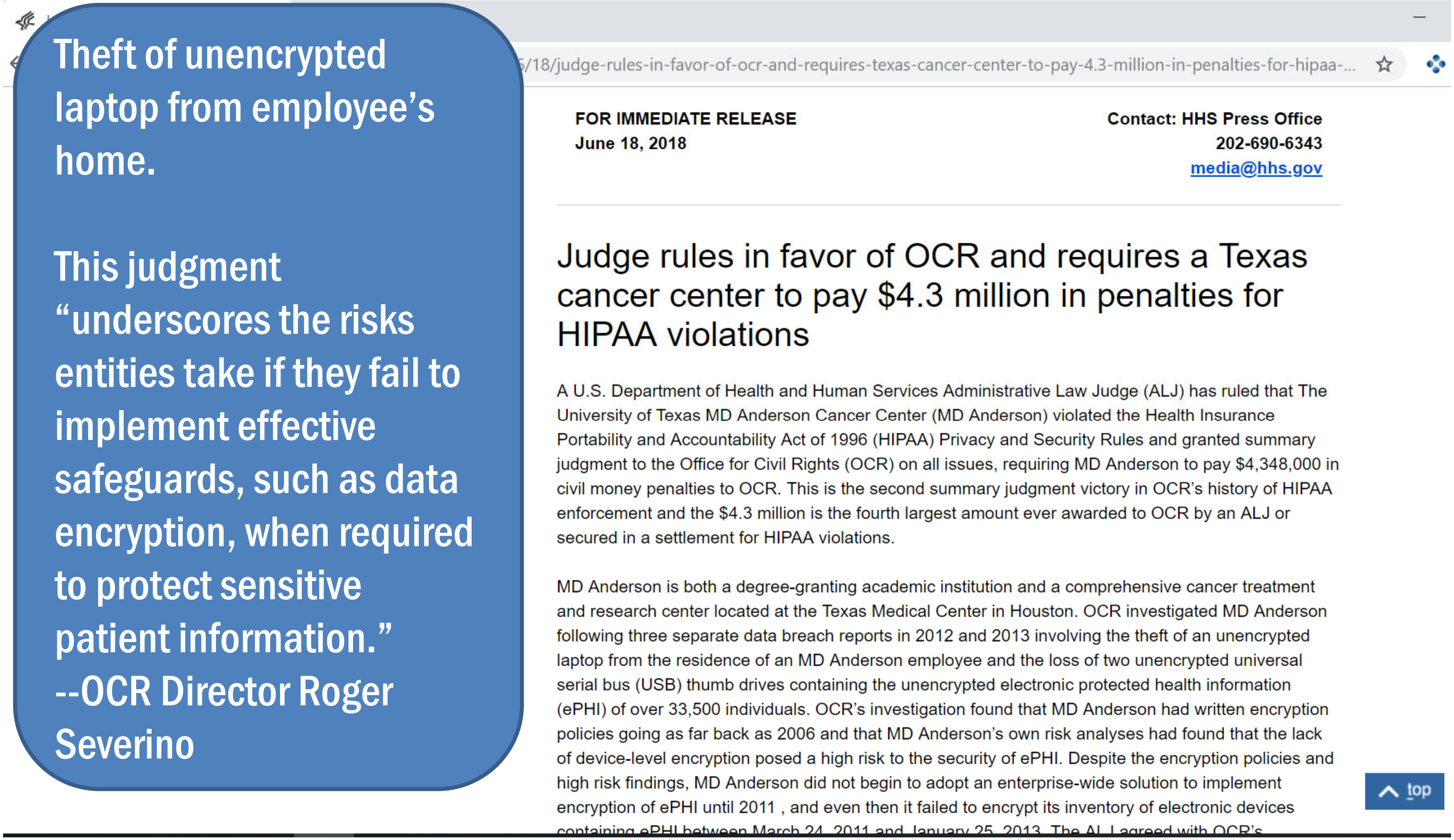
  (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

- ePHI that is properly encrypted is "secured".
  - Not subject to breach reporting.
- OCR presumes that loss of unencrypted laptop, USB, mobile device is reportable "breach."

Encryption

Theft of unencrypted laptop from employee’s home.

This judgment “underscores the risks entities take if they fail to implement effective safeguards, such as data encryption, when required to protect sensitive patient information.” --OCR Director Roger Severino



5/18/judge-rules-in-favor-of-ocr-and-requires-texas-cancer-center-to-pay-4.3-million-in-penalties-for-hipaa-...
top

FOR IMMEDIATE RELEASE
June 18, 2018

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Judge rules in favor of OCR and requires a Texas cancer center to pay $4.3 million in penalties for HIPAA violations

A U.S. Department of Health and Human Services Administrative Law Judge (ALJ) has ruled that The University of Texas MD Anderson Cancer Center (MD Anderson) violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and granted summary judgment to the Office for Civil Rights (OCR) on all issues, requiring MD Anderson to pay $4,348,000 in civil money penalties to OCR. This is the second summary judgment victory in OCR’s history of HIPAA enforcement and the $4.3 million is the fourth largest amount ever awarded to OCR by an ALJ or secured in a settlement for HIPAA violations.

MD Anderson is both a degree-granting academic institution and a comprehensive cancer treatment and research center located at the Texas Medical Center in Houston. OCR investigated MD Anderson following three separate data breach reports in 2012 and 2013 involving the theft of an unencrypted laptop from the residence of an MD Anderson employee and the loss of two unencrypted universal serial bus (USB) thumb drives containing the unencrypted electronic protected health information (ePHI) of over 33,500 individuals. OCR’s investigation found that MD Anderson had written encryption policies going as far back as 2006 and that MD Anderson’s own risk analyses had found that the lack of device-level encryption posed a high risk to the security of ePHI. Despite the encryption policies and high risk findings, MD Anderson did not begin to adopt an enterprise-wide solution to implement encryption of ePHI until 2011 , and even then it failed to encrypt its inventory of electronic devices containing ePHI between March 24, 2011 and January 25, 2013. The ALJ agreed with OCR’s

Encryption

Is the use of encryption mandatory in the Security Rule?

Answer: No. The final Security Rule made the use of encryption an addressable implementation specification. See 45 CFR § 164.312(a)(2)(iv) and (e)(2)(ii).

The encryption implementation specification is addressable, and must therefore be implemented if, after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its risk management of the confidentiality, integrity and availability of e-PHI.

If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate. If the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure and document the rationale for this decision.

(OCR FAQ at https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html).

Communicating by E-mail or Text

- ➢ General rule: must be secure, i.e., encrypted.

- To patients: may communicate via unsecure e-mail or text if warned patient and they choose to receive unsecure.

(45 CFR 164.522(b); 78 FR 5634)

- To providers, staff or other third parties: must use secure platform.

(45 CFR 164.312; CMS letter dated 12/28/17)

- Orders: Medicare Conditions of Participation and Conditions for Coverage generally prohibit texting orders.

(CMS letter dated 12/28/17)

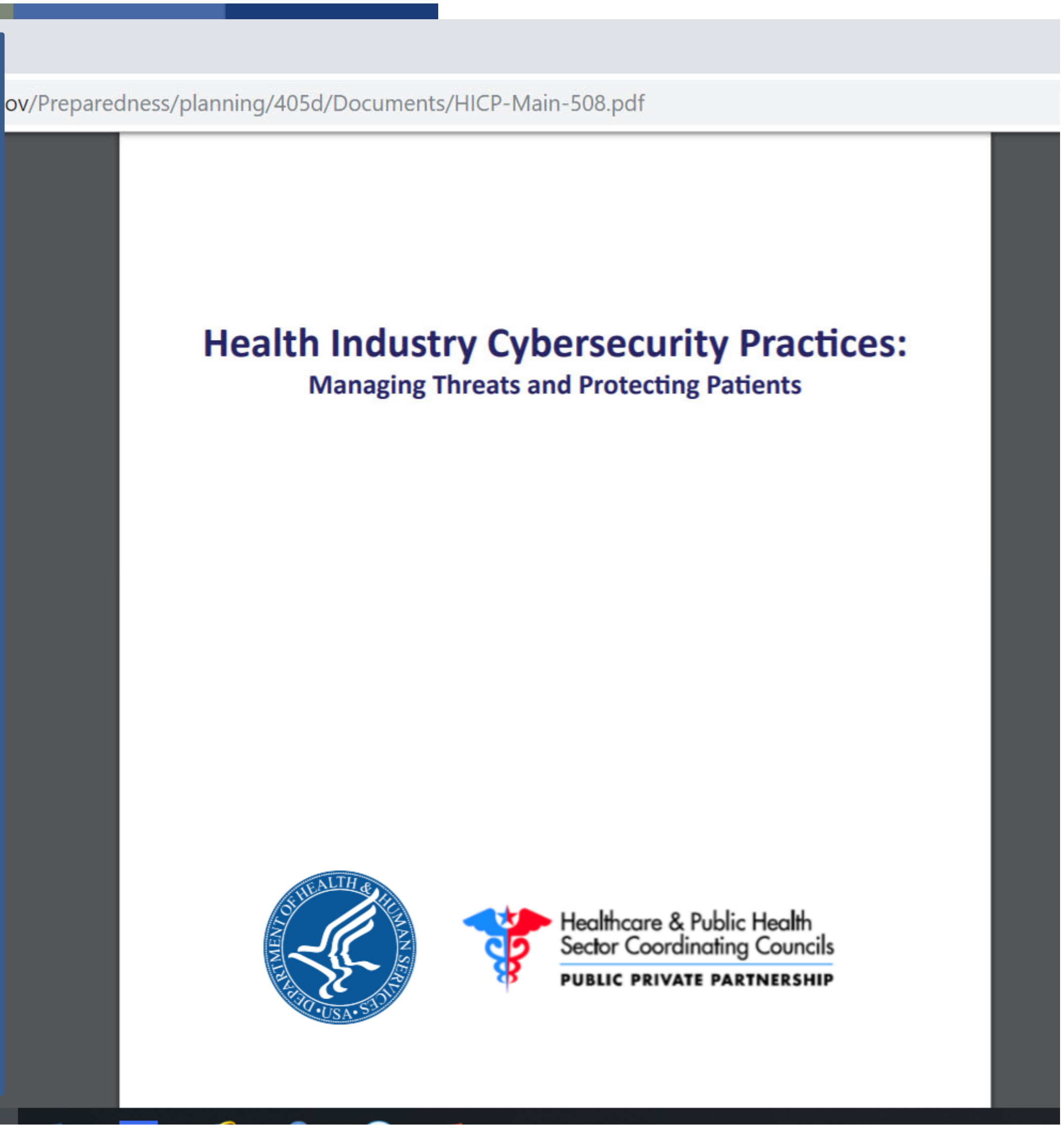
Additional Resources

https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Recommended Practices

1. E-mail protection system
2. Endpoint protection system
3. Access management
4. Data protection and loss prevention
5. Network management
6. Vulnerability management
7. Incident response
8. Medical device security
9. Cybersecurity policies

- Sample Forms
- Resources



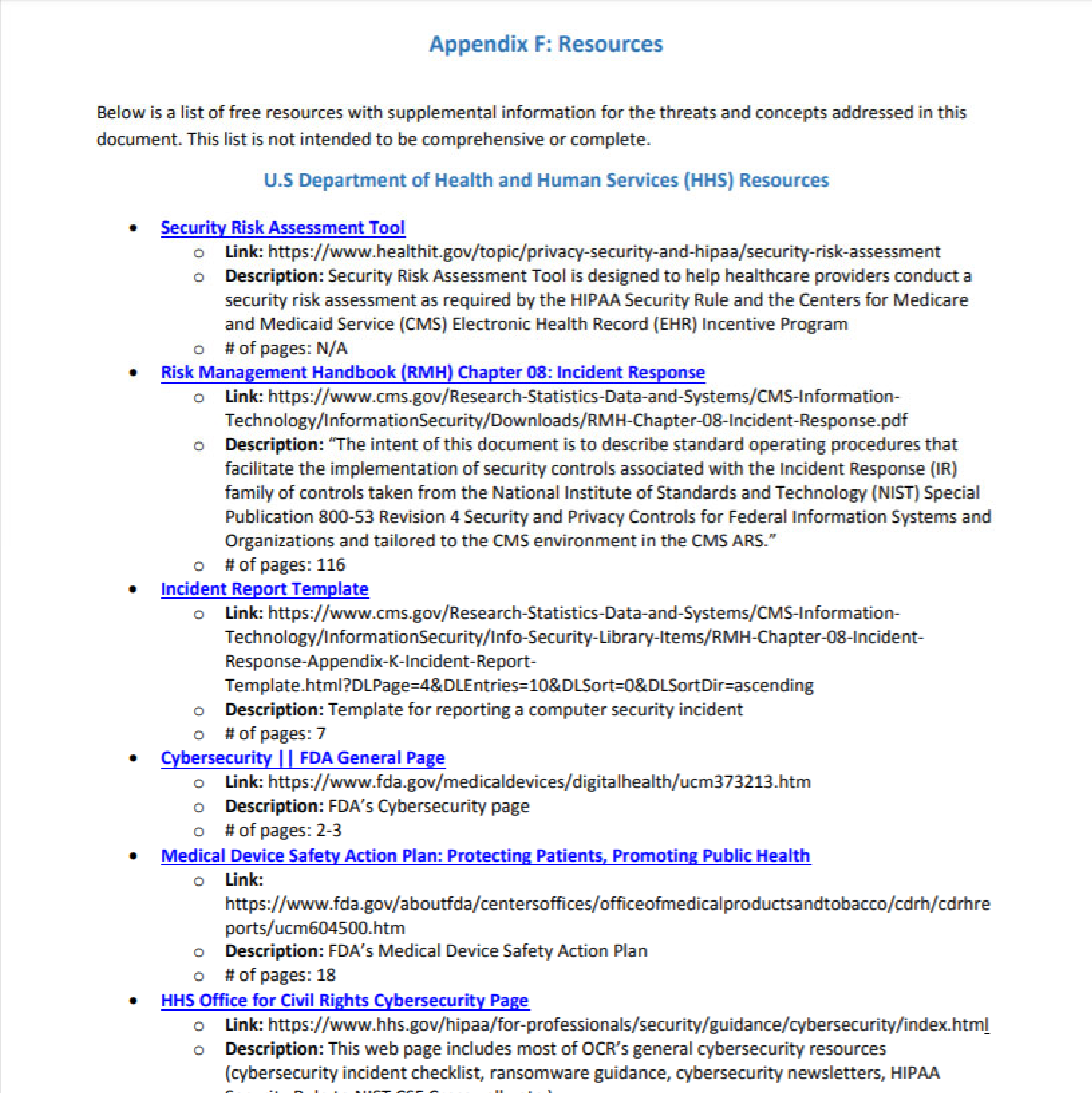
ov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

Health Industry Cybersecurity Practices:

Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Councils

PUBLIC PRIVATE PARTNERSHIP



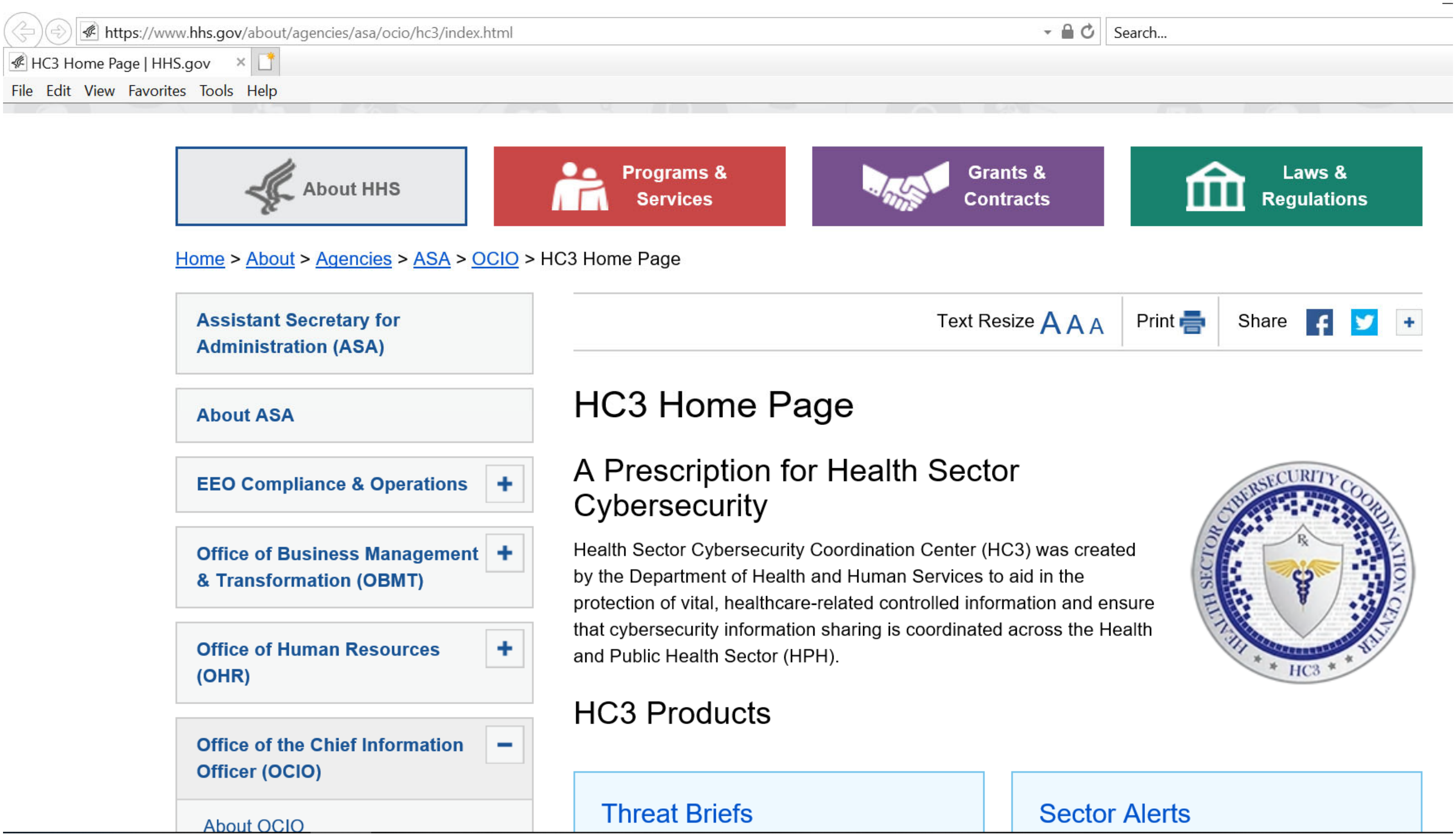
Appendix F: Resources

Below is a list of free resources with supplemental information for the threats and concepts addressed in this document. This list is not intended to be comprehensive or complete.

U.S Department of Health and Human Services (HHS) Resources

- Security Risk Assessment Tool
  - **Link:** https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
  - **Description:** Security Risk Assessment Tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program
  - # of pages: N/A
- Risk Management Handbook (RMH) Chapter 08: Incident Response
  - **Link:** https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH-Chapter-08-Incident-Response.pdf
  - **Description:** "The intent of this document is to describe standard operating procedures that facilitate the implementation of security controls associated with the Incident Response (IR) family of controls taken from the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations and tailored to the CMS environment in the CMS ARS."
  - # of pages: 116
- Incident Report Template
  - **Link:** https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/RMH-Chapter-08-Incident-Response-Appendix-K-Incident-Report-Template.html?DLPage=4&DLEntries=10&DLSort=0&DLSortDir=ascending
  - **Description:** Template for reporting a computer security incident
  - # of pages: 7
- Cybersecurity || FDA General Page
  - **Link:** https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm
  - **Description:** FDA's Cybersecurity page
  - # of pages: 2-3
- Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health
  - **Link:** https://www.fda.gov/aboutfda/centersoffices/officeofmedicalproductsandtobacco/cdrh/cdrhreports/ucm604500.htm
  - **Description:** FDA's Medical Device Safety Action Plan
  - # of pages: 18
- HHS Office for Civil Rights Cybersecurity Page
  - **Link:** https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
  - **Description:** This web page includes most of OCR's general cybersecurity resources (cybersecurity incident checklist, ransomware guidance, cybersecurity newsletters, HIPAA Security Rule to NIST CSF Crosswalk, etc.)

https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html



https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
Search...
HC3 Home Page | HHS.gov
File Edit View Favorites Tools Help
About HHS
Programs & Services
Grants & Contracts
Laws & Regulations

[Home](#) > [About](#) > [Agencies](#) > [ASA](#) > [OCIO](#) > HC3 Home Page

Assistant Secretary for Administration (ASA)
About ASA
EEO Compliance & Operations
Office of Business Management & Transformation (OBMT)
Office of Human Resources (OHR)
Office of the Chief Information Officer (OCIO)
About OCIO
Text Resize A A A
Print
Share

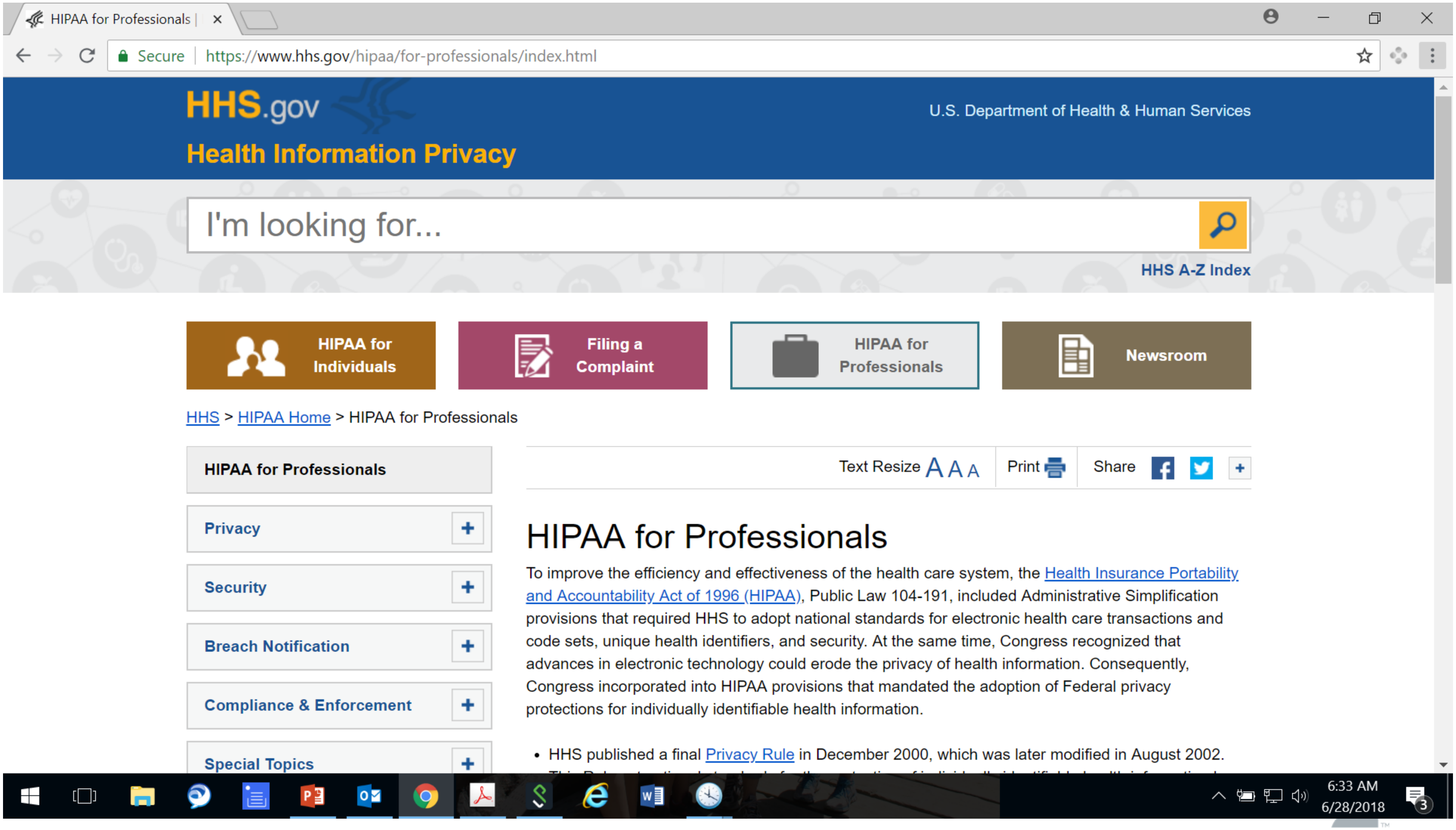
HC3 Home Page

A Prescription for Health Sector Cybersecurity

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).

HC3 Products

https://www.hhs.gov/hipaa/for-professionals/index.html



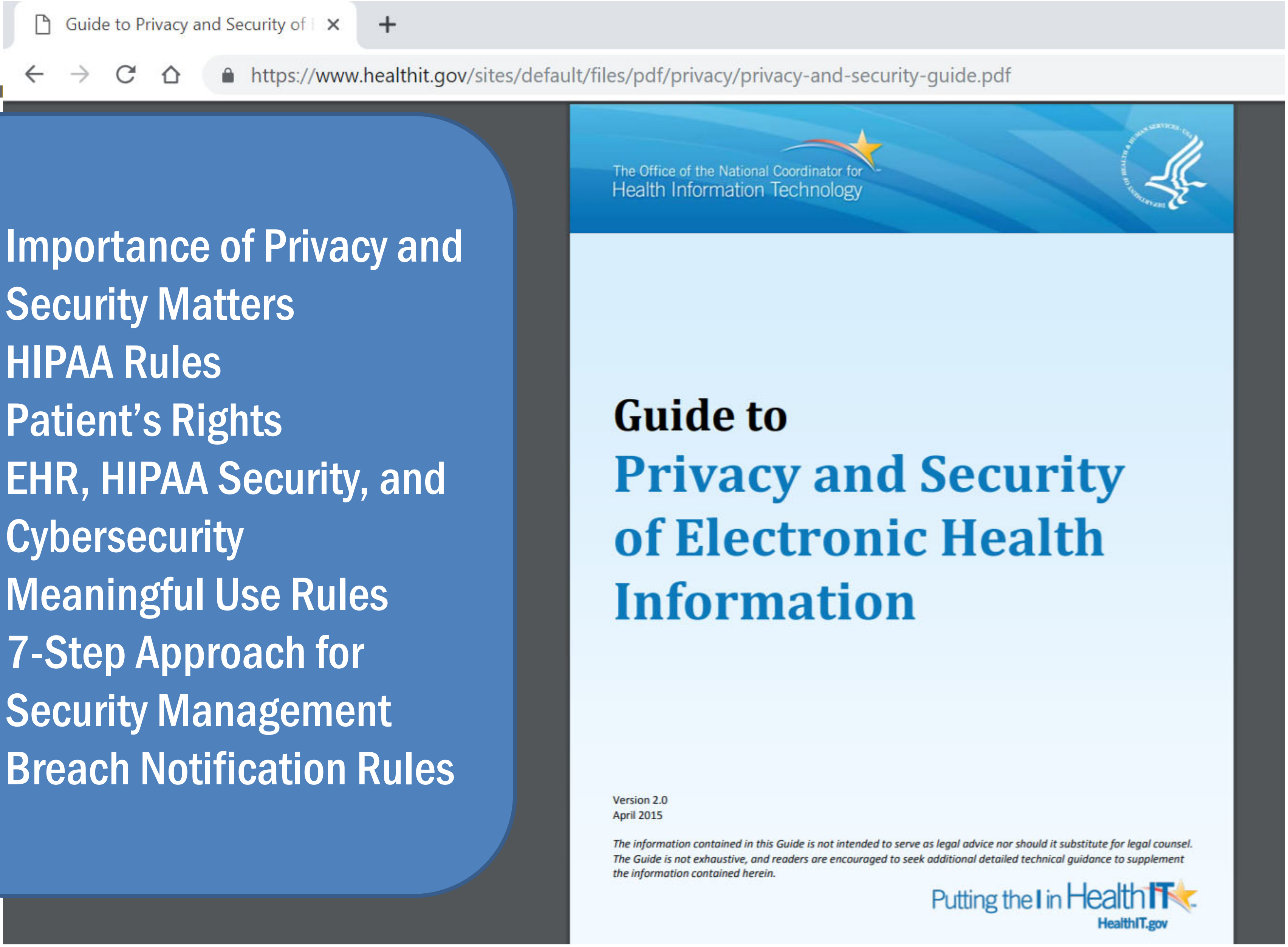
HIPAA for Professionals

To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, included Administrative Simplification provisions that required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

- HHS published a final Privacy Rule in December 2000, which was later modified in August 2002.

https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

1. Importance of Privacy and Security Matters
2. HIPAA Rules
3. Patient's Rights
4. EHR, HIPAA Security, and Cybersecurity
5. Meaningful Use Rules
6. 7-Step Approach for Security Management
7. Breach Notification Rules


Guide to Privacy and Security of
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

The Office of the National Coordinator for Health Information Technology

Guide to

Privacy and Security of Electronic Health Information

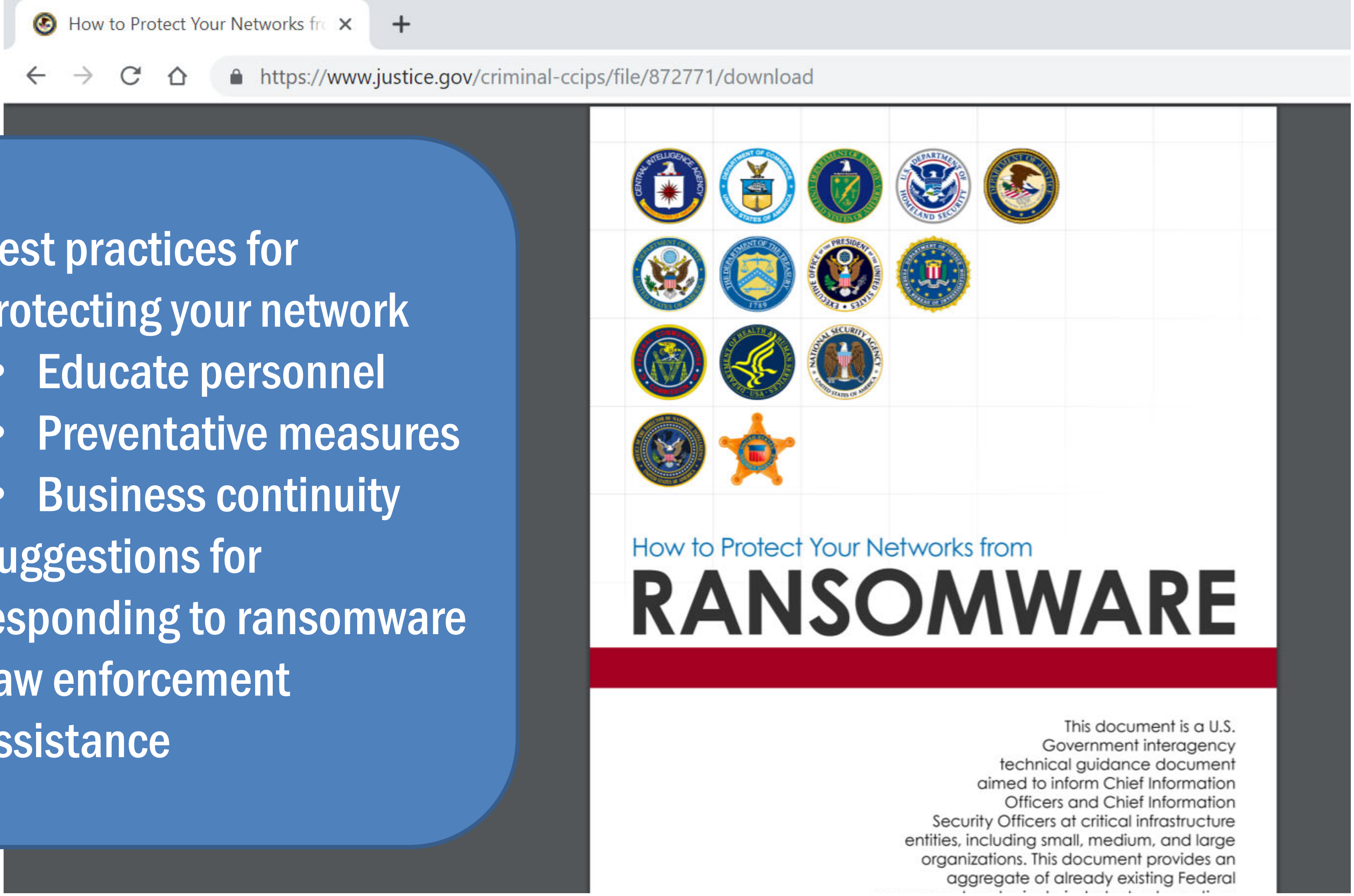
Version 2.0
April 2015

The information contained in this Guide is not intended to serve as legal advice nor should it substitute for legal counsel. The Guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

Putting the I in HealthIT
HealthIT.gov

https://www.justice.gov/criminal-ccips/file/872771/download

1. Best practices for protecting your network
   - Educate personnel
   - Preventative measures
   - Business continuity
2. Suggestions for responding to ransomware
3. Law enforcement assistance



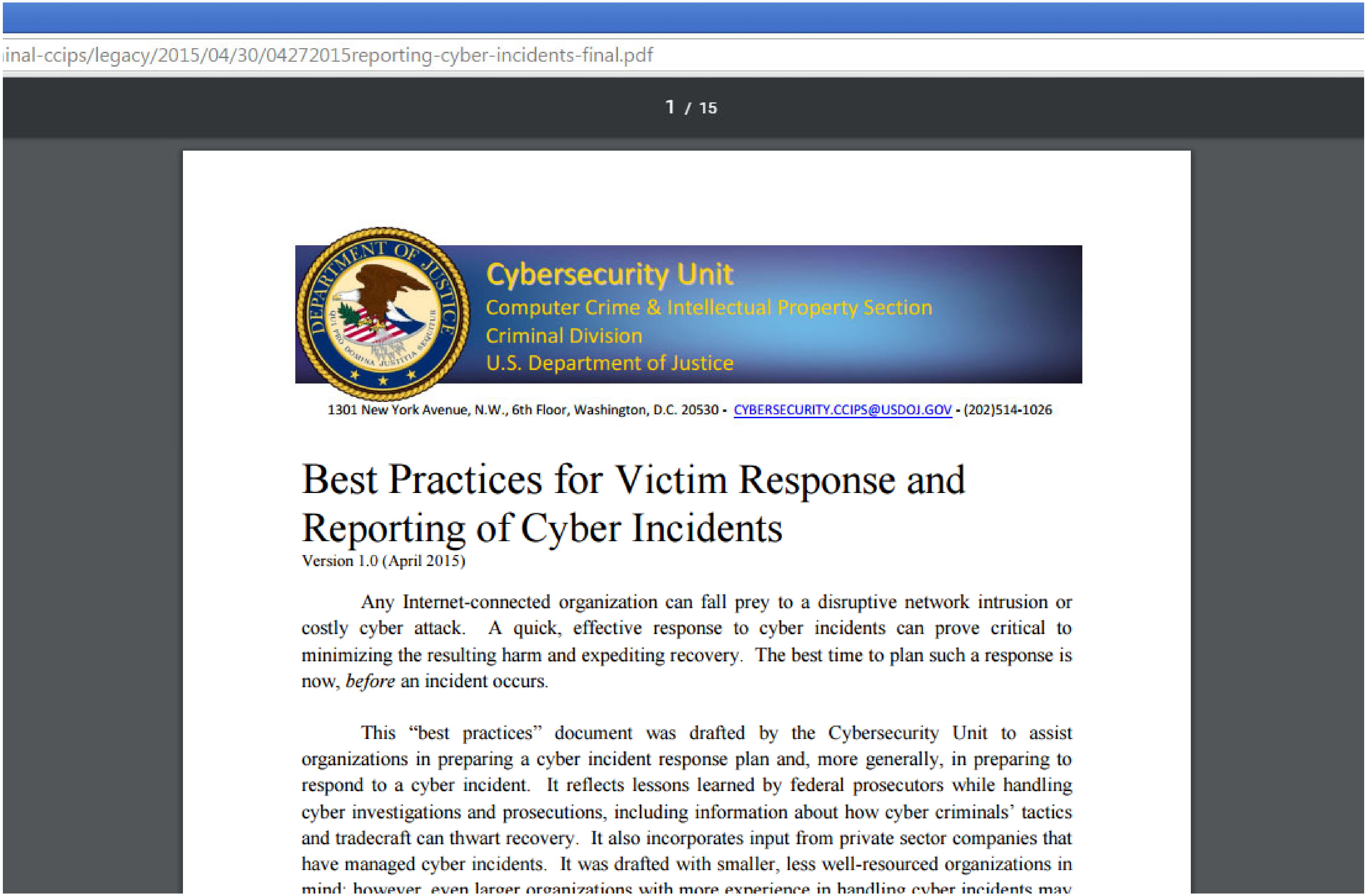
How to Protect Your Networks fr
https://www.justice.gov/criminal-ccips/file/872771/download

How to Protect Your Networks from

RANSOMWARE

This document is a U.S. Government interagency technical guidance document aimed to inform Chief Information Officers and Chief Information Security Officers at critical infrastructure entities, including small, medium, and large organizations. This document provides an aggregate of already existing Federal

www.justice.gov/sites/default/files/criminal- ccips/legacy/
2015/04/30/04272015reporting-cyber-incidents-final.pdf



inal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf

1 / 15

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

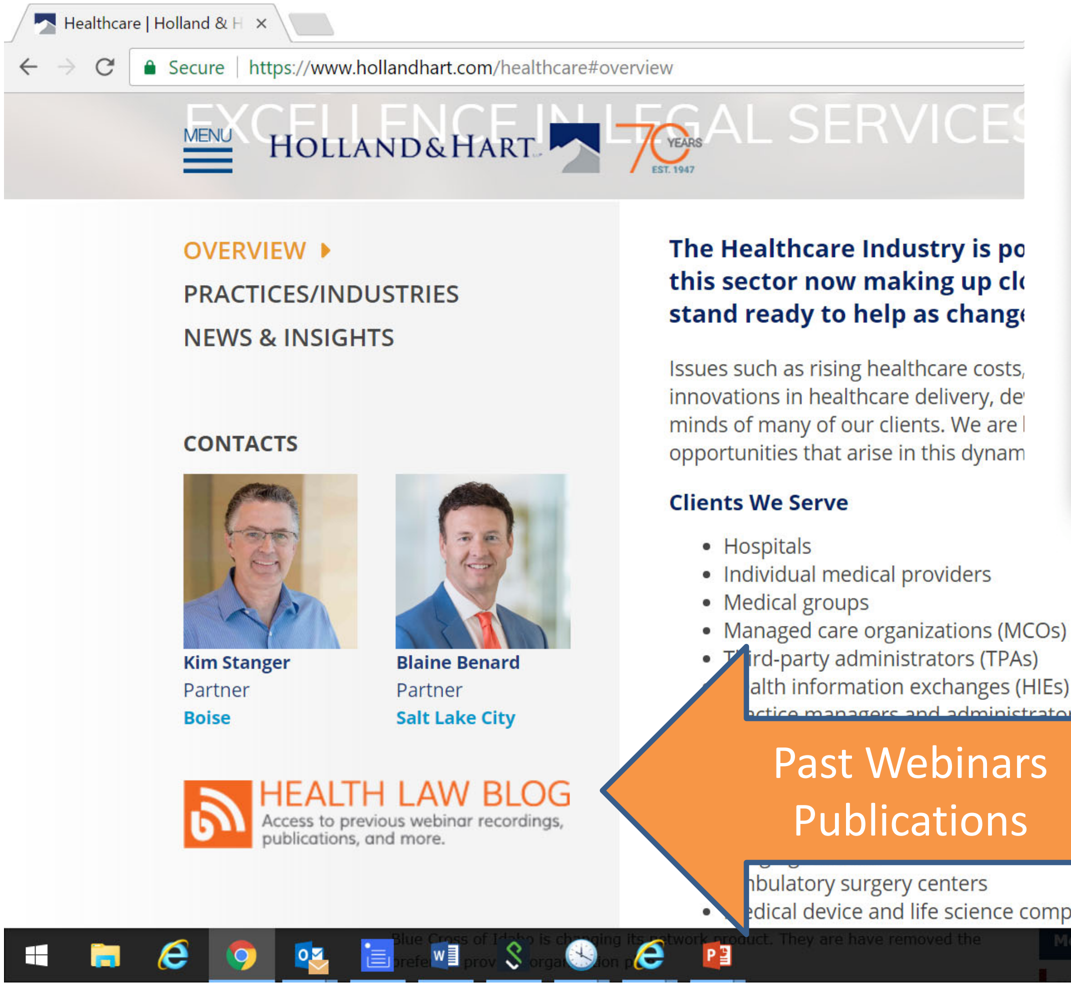
Best Practices for Victim Response and Reporting of Cyber Incidents

Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* an incident occurs.

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may

https://www.hollandhart.com/healthcare#overview



Healthcare | Holland & H ×
Secure
https://www.hollandhart.com/healthcare#overview
EXCELLENCE IN LEGAL SERVICES
MENU
HOLLAND&HART
70 YEARS EST. 1947

OVERVIEW ▸

PRACTICES/INDUSTRIES

NEWS & INSIGHTS

CONTACTS

Kim Stanger
Partner
Boise

Blaine Benard
Partner
Salt Lake City

HEALTH LAW BLOG
Access to previous webinar recordings, publications, and more.

**The Healthcare Industry is po
this sector now making up cl
stand ready to help as chang**

Issues such as rising healthcare costs,
innovations in healthcare delivery, de
minds of many of our clients. We are
opportunities that arise in this dynam

Clients We Serve

- Hospitals
- Individual medical providers
- Medical groups
- Managed care organizations (MCOs)
- Third-party administrators (TPAs)
- alth information exchanges (HIEs)
- actice managers and administrators
- nbulatory surgery centers
- dical device and life science companies

Past Webinars
Publications

Kim C. Stanger
Office: (208) 383-3913
Cell: (208) 409-7907
kcstanger@hollandhart.com

Andrew Shaxted
Cell: (773) 658-0241
Andrew.Shaxted@fticonsulting.com