CYBERSECURITY AND HIPAA

Wyoming HFMA

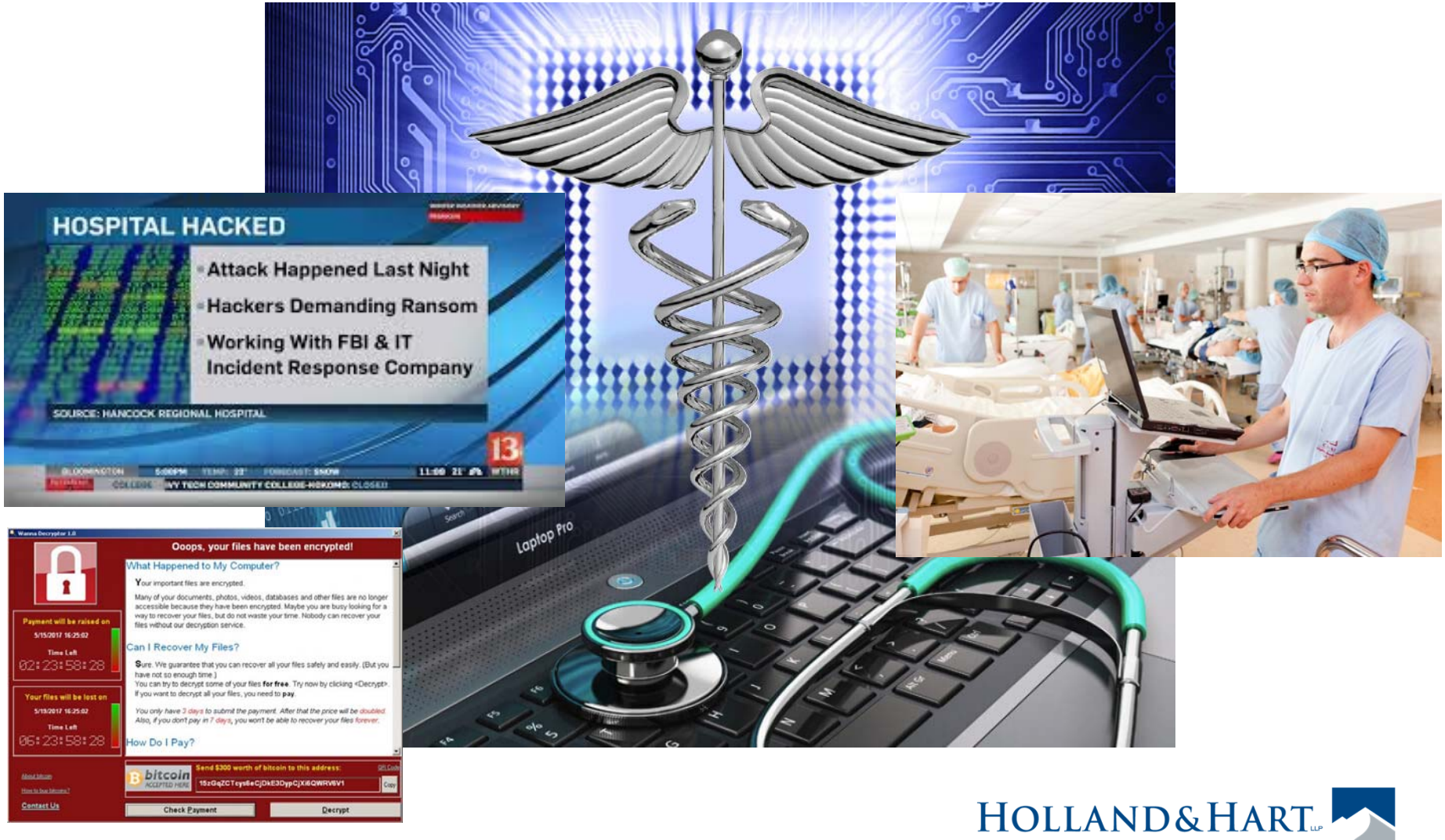
Kim C. Stanger

(5-19)

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.

The Threat of Cybersecurity



HOLLAND&HART LLP

NBC News (February 13, 2016)

- Healthcare related hacking up 11,000% since last year.
- 1/3 of Americans have had their health records compromised.
- Health records receive premium on "dark web"
  - ✓ Credit cards: $1 to $3
  - ✓ SSNs: $15
  - ✓ Complete health records: $60

NEWS
FEB 13 2016, 4:51 AM ET

Hacking of Health Care Records Skyrockets

by TOM COSTELLO

A man types on a computer keyboard in Warsaw in this February 28, 2013 illustration file picture. A barrage of damaging cyberattacks is shaking up the security industry, with some businesses and organisations no longer assuming they can keep hackers at bay, and instead turning to waging a guerrilla war from within their networks. KACPER PEMPEL / Reuters

For John Kuhn, a simple X-ray after a snowboarding accident turned into an accounting nightmare when the hospital billed him $20,000 for a surgery he never had.

Healthcare IT News

Headlines from July – October 2018

- 3 phishing attacks breach 20,000 Catawba Valley patient rec
- CMS responds to data breach affecting 75,000 in federal AC
- Two phishing attacks on Minnesota DHS breach 21,000 patie
- 3 Massachusetts hospitals fined nearly $1 million by OCR for
- Employee error exposed Blue Cross patient data for 3 months
- Ransomware attack breaches 40,800 patient records in Ha
- Phishing attack breaches 38,000 patient records at Legacy He
- 417,000 Augusta University Health patient records breached
- 1.4M records breached in UnityPoint Health phishing attack (7/31/18)
- Ransomware, malware attack breaches 45,000 patient record
- LabCorp's network breach puts millions of records at risk (7/1
- Hackers breach 1.5M Singapore patient records, including the
- Patient data exposed for months after phishing attack on Sunspir
- Phishing attacks breach Alive Hospice for 1 to 4 months (7/1 18)
- Ransomware attack on Cass Regional shuts down EHR (7/11/18)
- 270,000 patient records breached in Med Associates hack (6/20/18)

(https://www.healthcareitnews.com/projects/biggest-healthcare-dat

3 phishing attacks breach 20,000 Catawba Valley patient records (10/25/18)

Ransomware attack breaches 40,800 patient records in Hawaii (9/13/18)

Ransomware attack on Cass Regional shuts down EHR (7/11/18)

270,000 patient records breached in Med Associates hack (6/20/18

HOL

Modern Healthcare

Breaches Reported in April 2019

- Doctors Management Services, Inc. 206,695 people affected in a Hacking/IT Incident. Network Servers targeted. (4/22/19)
- Centrelake Medical Group, Inc., 197,661 people affected in a Hacking/IT Incident. Network Servers targeted. (4/16/19)
- Gulf Coast Pain Consultants, LLC. 35,000 people affected in a Unauthorized Access/Disclosure. Electronic Medical Records targeted. (4/5/19)
- EmCare, Inc. 31,236 people affected in a Hacking/IT Incident. Emails were targeted. (4/20/19)
- Kim P. Kornegay, DMD. 27,000 people affected in a Theft. Desktop Computer, Electronic Medical Record, Paper/Films targeted. (4/19/19)
- Pediatric Orthopedic Specialties, PA. 24,176 people affected in a Hacking/IT Incident. Network Servers targeted. (4/18/19)
- Health Recovery Services, Inc. 20,485 people affected in a Unauthorized Access/Disclosure. Network Servers targeted. (4/5/19)
- Baystate Health. 11,658 people affected in a Hacking/IT Incident. Emails targeted. (4/5/19)
- Riverplace Counseling Center, Inc. 11,639 people affected in a Hacking/IT Incident. Network Servers targeted. (4/11/19)
- Minnesota Dept of Human Services. 10,263 people affected in a Hacking/IT Incident. Emails targeted. (4/9/19)

(https://www.modernhealthcare.com/cybersecurity/healthcare-breaches-reported-february-exposed-data-2-million-people)

➢ Record 2M patients affected

HOLLAND&HART LLP

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

What are the consequences to your organization?

HOLLAND&HART LLP

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 move patients
- Disruption of operations
- Lost revenue
- Cost of response
- Loss or damage to equipment
- Bad public relations
- Fines and penalties
- Lawsuits
- Others?

HOLLAND&HART LLP

Cyberliability Costs

2017 TrendMicro Report

- Costs healthcare industry $6 billion per year

2018 Ponemon Report

- Average cost for breach
  - For hospitals, $2M over two years
  - $408 per compromised record

Cybersecurity Laws

HOLLAND&HART LLP

Cyberliability Laws

- Health Insurance Portability and Accountability Act ("HIPAA"), 45 CFR part 164
  - Privacy Rule.
  - Security Rule
  - Breach Notification Rule

  More about this later…
- FTC Breach Notification Rule, 16 CFR part 318
  - Applies to vendors of personal health information (i.e., entities that allow persons to maintain their health info online) and their service providers.
  - Must notify individuals of breaches.

Cyberliability Laws

- Food and Drug Administration, 21 CFR part 11
  - Electronic records that are required by FDA must satisfy certain standards to ensure their authenticity, integrity, and confidentiality.
- 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.

LabMD, Inc., In the Matter of

TAGS: Health Care | Consumer Protection | Privacy and Security | Data Security

LAST UPDATED: FEBRUARY 5, 2016

In the Matter of LabMD, Inc., a corporation

FTC MATTER/FILE NUMBER: 102 3099

DOCKET NUMBER: 9357

RELATED CASE: LabMD, Inc. v. Federal Trade Commission

CASE SUMMARY

The Federal Trade Commission filed a complaint against medical testing laboratory LabMD, Inc. alleging that the company failed to reasonably protect the security of consumers' personal data, including medical information. The complaint alleges that in two separate incidents, LabMD collectively exposed the personal information of approximately 10,000 consumers. The complaint alleges that LabMD billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The case is part of an ongoing effort by the Commission to ensure that companies take reasonable and appropriate measures to protect consumers' personal data.

FTC v. LabMD

"The Commission's complaint alleges that LabMD failed to take reasonable and appropriate measures to prevent unauthorized disclosure of sensitive consumer data – including health information – it held. Among other things, the complaint alleges that the company:

- did not implement or maintain a comprehensive data security program to protect this information;
- did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information;
- did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- did not adequately train employees on basic security practices; and
- did not use readily available measures to prevent and detect unauthorized access to personal information."

Cyberliability Laws

- State Breach Notification Laws
  - Typically require notice to individuals if certain personal info is compromised by a security breach.
- State Privacy Statutes
  - May require confidentiality of personal info.
  - May require notification of breaches reports.
- State Consumer Protection Statutes
  - Prohibit unfair or deceptive practices.
- Others?

Cyberliability Contract Issues

- Payment Card Industry Data Security Standards (PCI-DSS)
  - Agreements with major credit cards require businesses to comply with certain data security rules.
- Business Associate Agreements
  - Requires BAs to comply with HIPAA security standards.
- Insurance Coverage
  - Insurer may deny coverage if misrepresent data security practices. (*Columbia Casualty Co. v. Cottage Health Sys.,* challenging coverage for $4.1 million settlement)
- Others?

Cyberliability Lawsuits

- Private Lawsuits
  - Consumer protection statutes.
  - Breach of fiduciary duty.
  - Infliction of emotional distress.
  - Negligence.
  - Negligence *per se* based on HIPAA or state laws.
  - Intrusion upon seclusion or solitude, or into private affairs.
  - Public disclosure of embarrassing private facts.
  - Publicity which places a person in a false light in the public eye.
  - Appropriation of name or likeness.
  - Whatever a creative plaintiff's lawyer may cook up…

Cybersecurity Act of 2015

- Establishes framework to develop cybersecurity guidance for industry segments and share info re cybersecurity attacks.
  - HHS must develop voluntary cybersecurity guidance for the healthcare industry.
  - Allows entities to share info relevant to cyberattacks without liability.
    - Must remove personal info.
- Law is currently voluntary.

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

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…

PayPal PayPal

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:

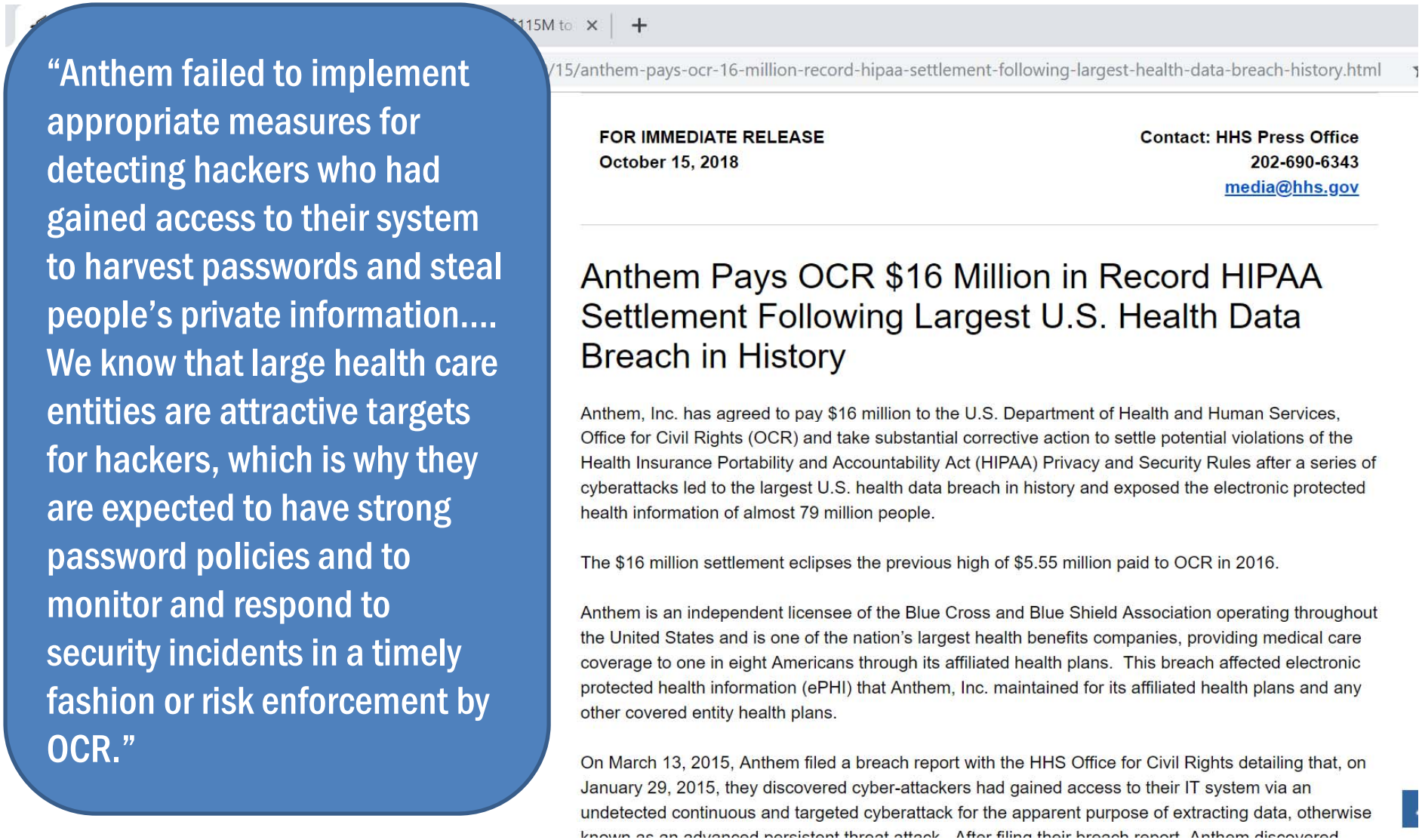
Confirm Your Account Now

Log in to confirm your account

paypal

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

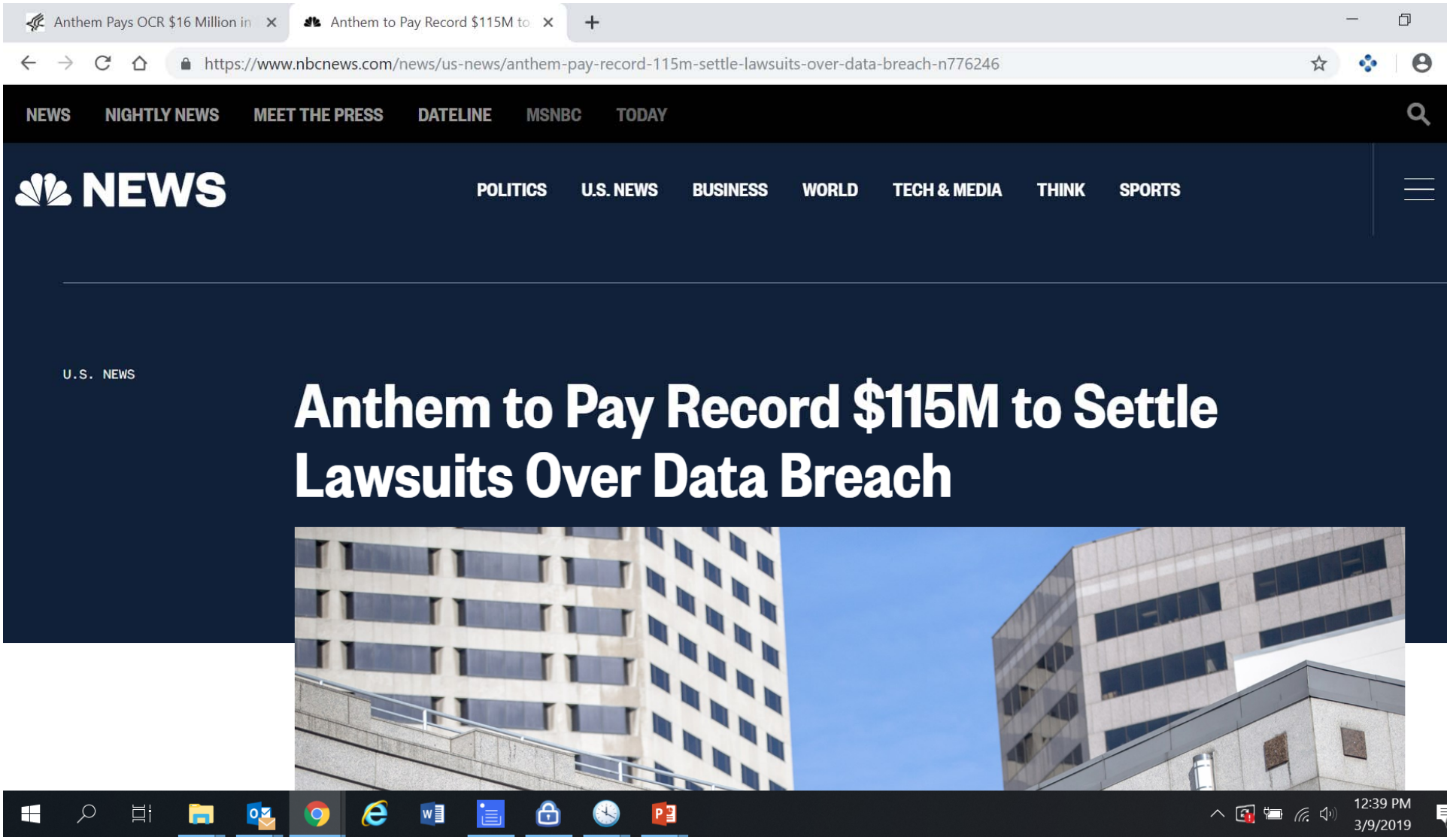
Anthem, Inc. has agreed to pay $16 million to the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) and take substantial corrective action to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules after a series 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.

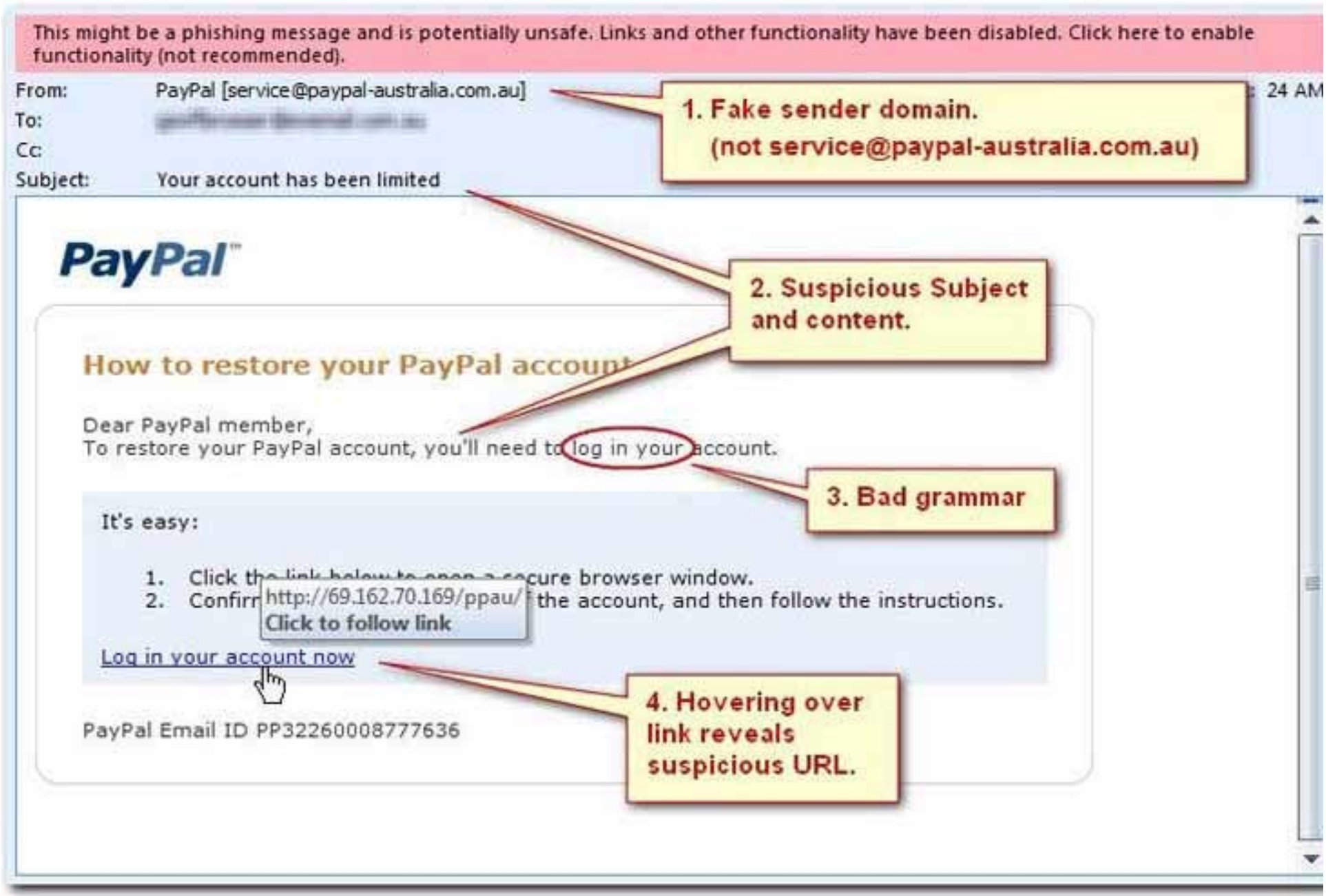
The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016.

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.

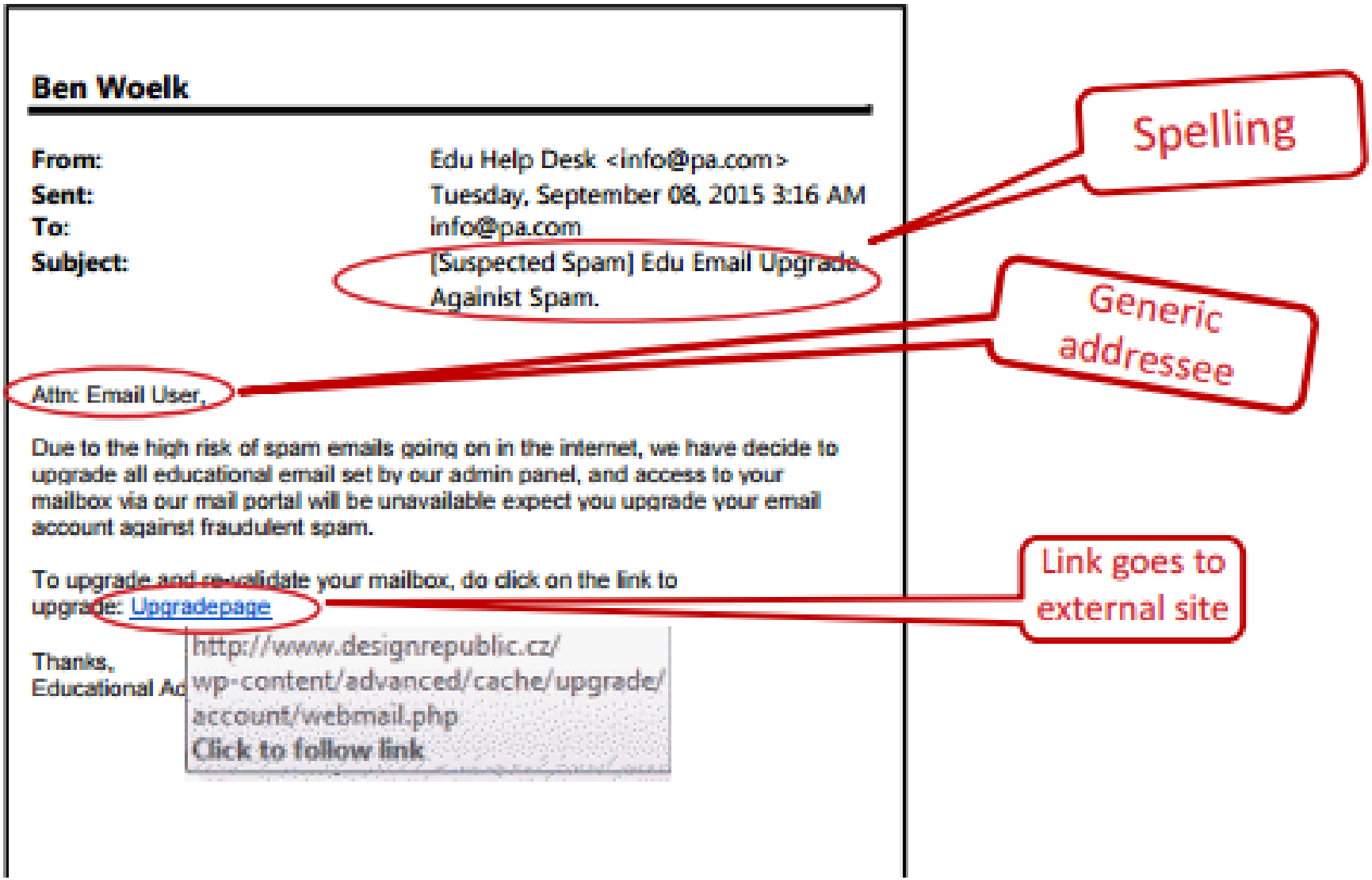
On March 13, 2015, Anthem filed a breach report with the HHS Office for Civil Rights detailing that, on January 29, 2015, they discovered cyber-attackers had gained access to their IT system via an undetected continuous and targeted cyberattack for the apparent purpose of extracting data, otherwise known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

E-mail Phishing Attack




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]
To:
Cc:
Subject: Your account has been limited
1. Fake sender domain.
(not service@paypal-australia.com.au)
PayPal
2. Suspicious Subject and content.
How to restore your PayPal account
Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.
3. Bad grammar
It's easy:
1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.
http://69.162.70.169/ppau/
Click to follow link
Log in your account now
4. Hovering over link reveals suspicious URL.
PayPal Email ID PP32260008777636

May also appear to be internal e-mails



E-mail Phishing Attack

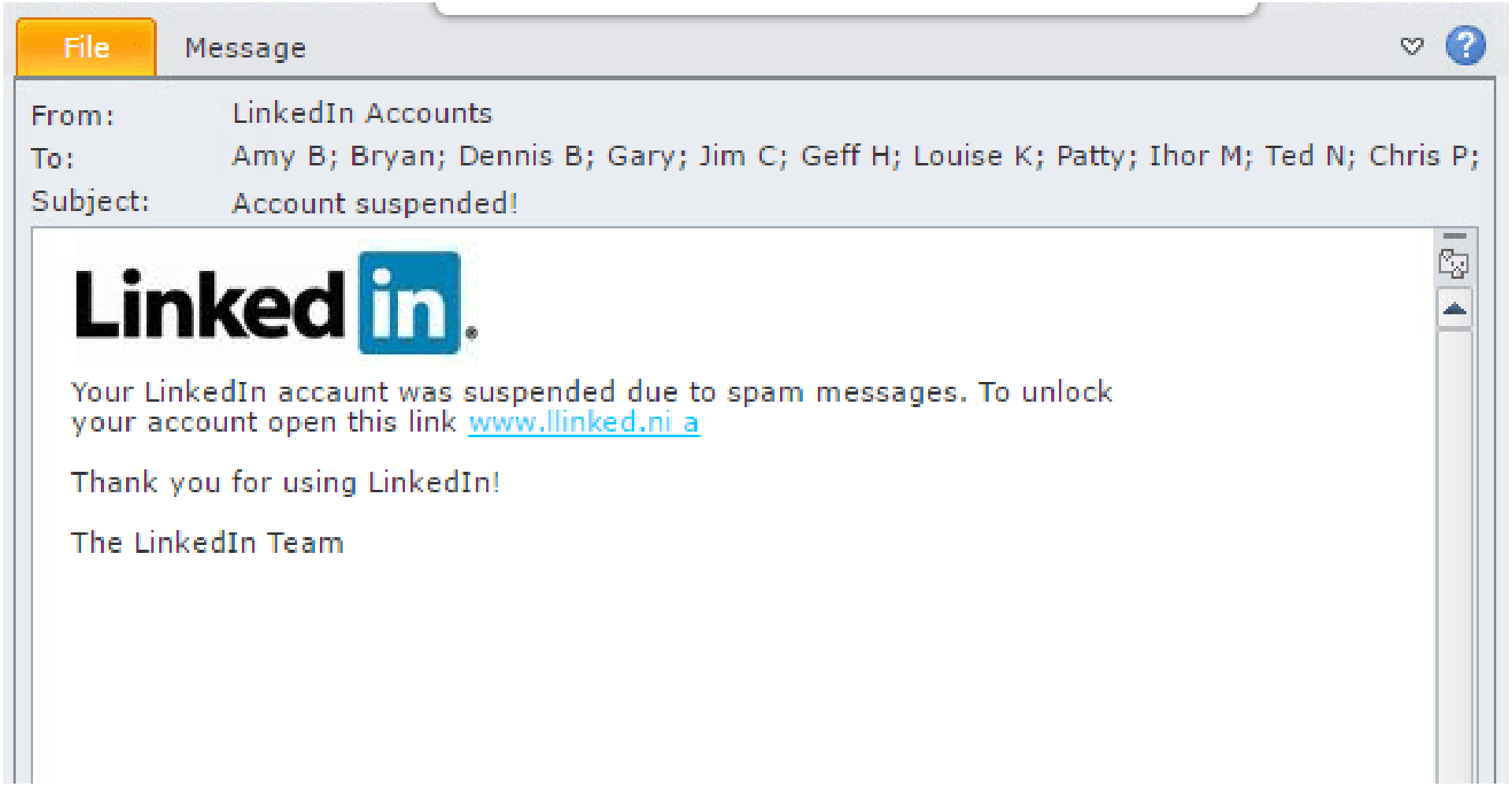
From: **Costco Shipping Agent <manager@cbcbuilding.com>** Hide
Subject: Scheduled Home Delivery Problem
Date: January 6, 2014 10:54:37 PM MST
To:
Reply-To: Costco Shipping Agent <manager@cbcbuilding.com>

Costco WHOLESALE

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.

E-mail Phishing Attacks



HOLLAND&HART LLP

From: HelpDesk [mailto:xxxxx@connect.ust.hk]

Sent: Wednesday, April 12, 2017 2:23 PM

To: *[redacted]*

Subject: Validate Email Account

This is to notify all Students, Staffs of University that we are validating active accounts.

Kindly confirm that your account is still in use by clicking the validation link below:

Validate Email Account

Sincerely

IT Help Desk

Office of Information Technology

The University

amazon

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

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.

Print Issue | E-Weeklies | Conferences | Webinars | Whitepapers | Multimedia | Lists | About Us

Physicians | Leadership | Executive Moves | Transaction & Valuation | Human Capital and Risk | Patient Flow

Health Information Technology

Hospitals are hit with 88% of all ransomware attacks

Written by Max Green | July 27, 2016 | Print | Email

189 Share Tweet 36 5

Hospitals and health systems have more to lose than organizations in other sectors when it comes to hacks. Patient data sells for more money than any other kind of information on the black market. Adding insult to injury, a new report suggests that the healthcare industry is hit significantly harder by ransomware than in any other — 88 percent of attacks hit hospitals.

HOLLAND&HART LLP

BREAKING: Early movers: PCLN, GRMN, BLMN, KMI, CPB, AZN, TMUS & more

CYBERSECURITY

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING | CYB

The hospital held hostage by hackers

Anita Balakrishnan
15 Hours Ago
CNBC

Los Angeles medical workers are dealing with an internal emergency straight out of science fiction, one that cybersecurity experts say is increasingly common.

CNBC (February 17, 2016)

- Hollywood Presbyterian Hospital hit by ransomware.
- Medical record system shut down.
- Hackers demand $3.7M in bitcoin.
- Hospital pays $17K.

Ransomware Attackes

UK hospitals hit with massive ran

https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

THE VERGE TECH REVIEWS SCIENCE CREATORS ENTERTAINMENT VIDEO MORE

In 2017, UK healthcare system subjected to WannaCry ransomware.

- **16 hospitals shut down**
- **45,000 computers across 74 countries**

TECH CYBERSECURITY

UK hospitals hit with massive ransomware attack

52

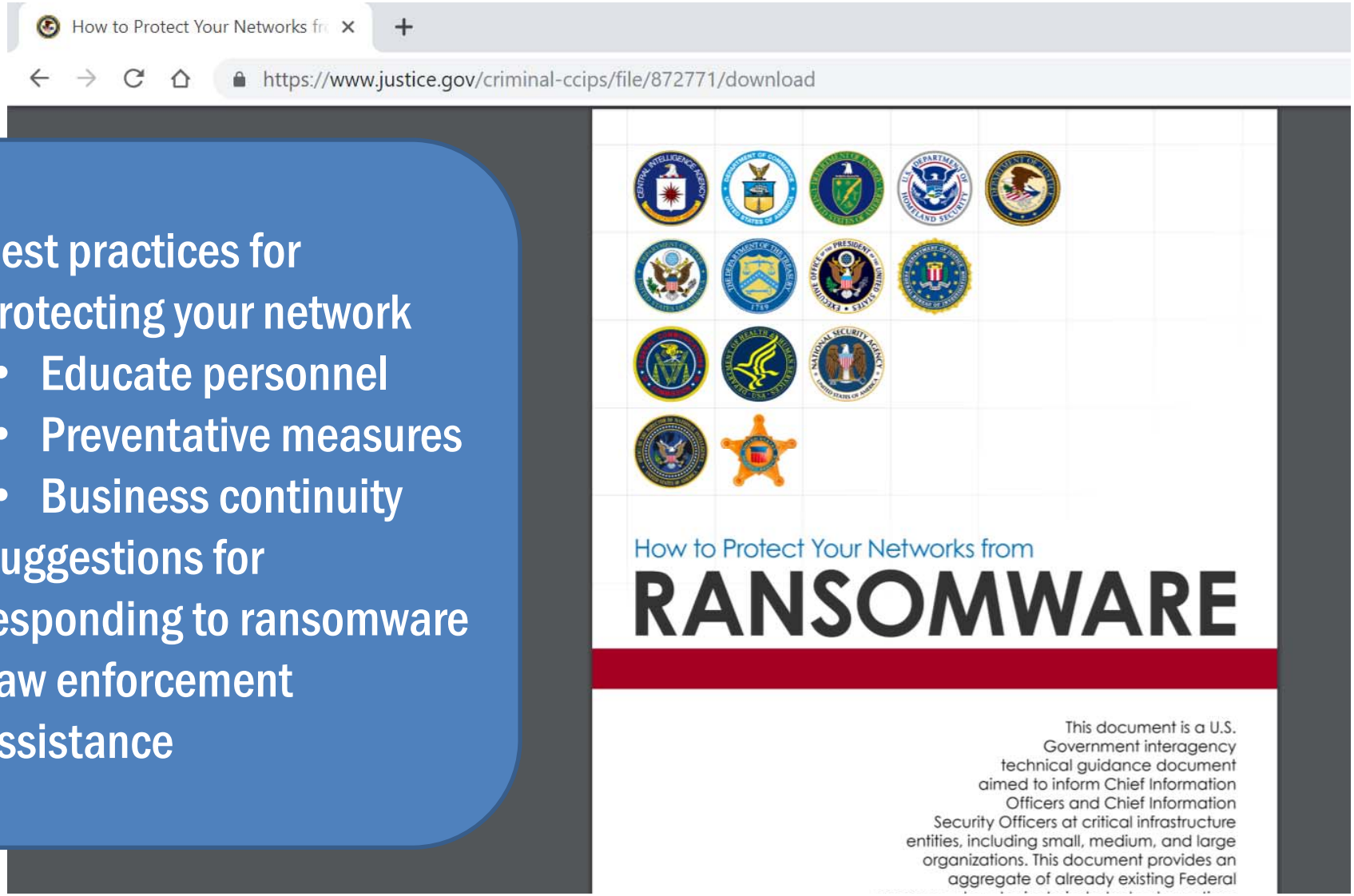
Sixteen hospitals shut down as a result of the attack

By Russell Brandom | May 12, 2017, 11:36am EDT

SHARE

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

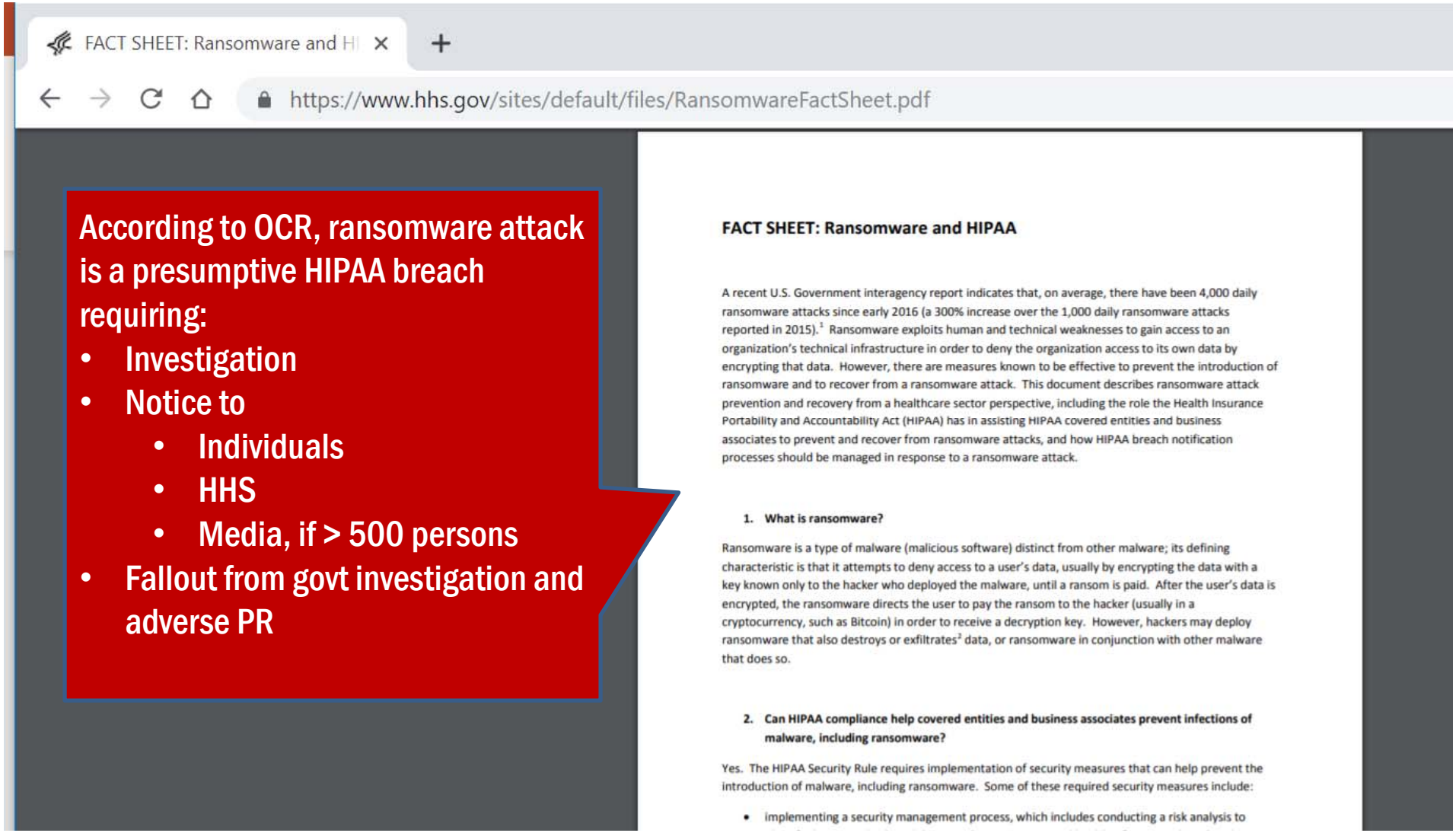


Ransomware Attacks

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.

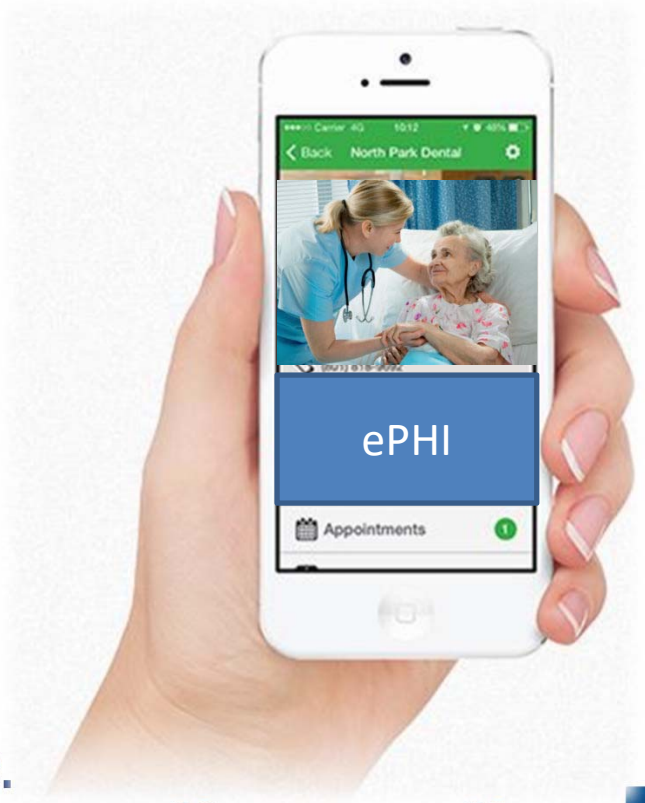
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf



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.

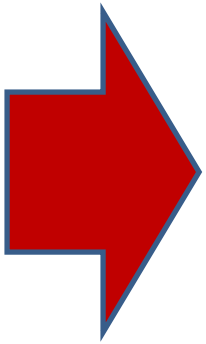


HOLLAND&HART LLP

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.

Search News Releases

Search

View 2016 - 1991 archive

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

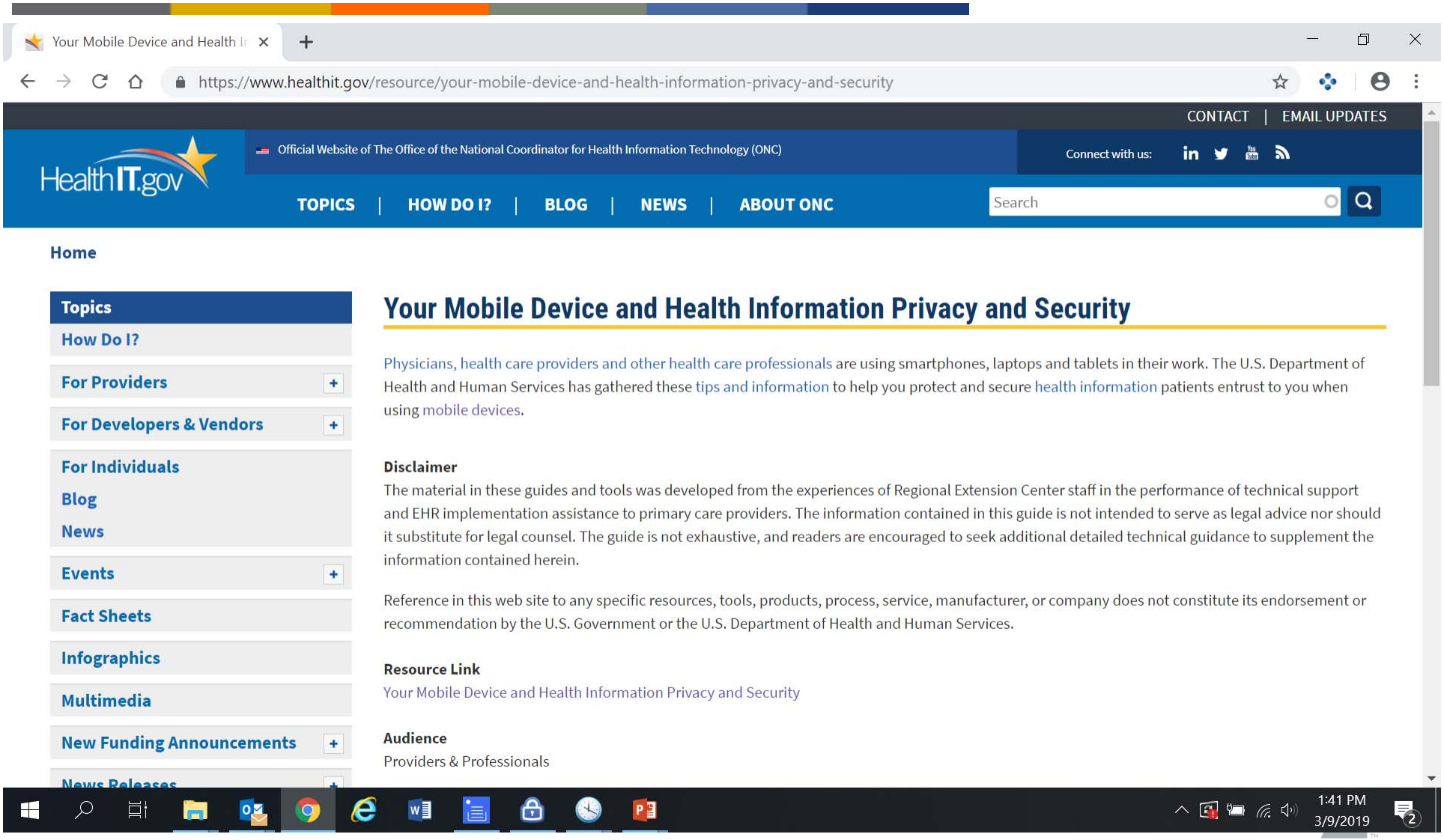
- Willful neglect.
- Mandatory penalties of:
  - If correct w/in 30 days:
    - $11,182 to $57,051 per violation
    - Max $114,102 per type per year.
  - At least $57,051 per violation if don't correct w/in 30 days
    - $57,051 per violation
    - Max $1,711,533 per type per year

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



Mobile Devices: Tips to Protect and Secure Health Information

HealthIT.gov
Advancing America's Health Care

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.

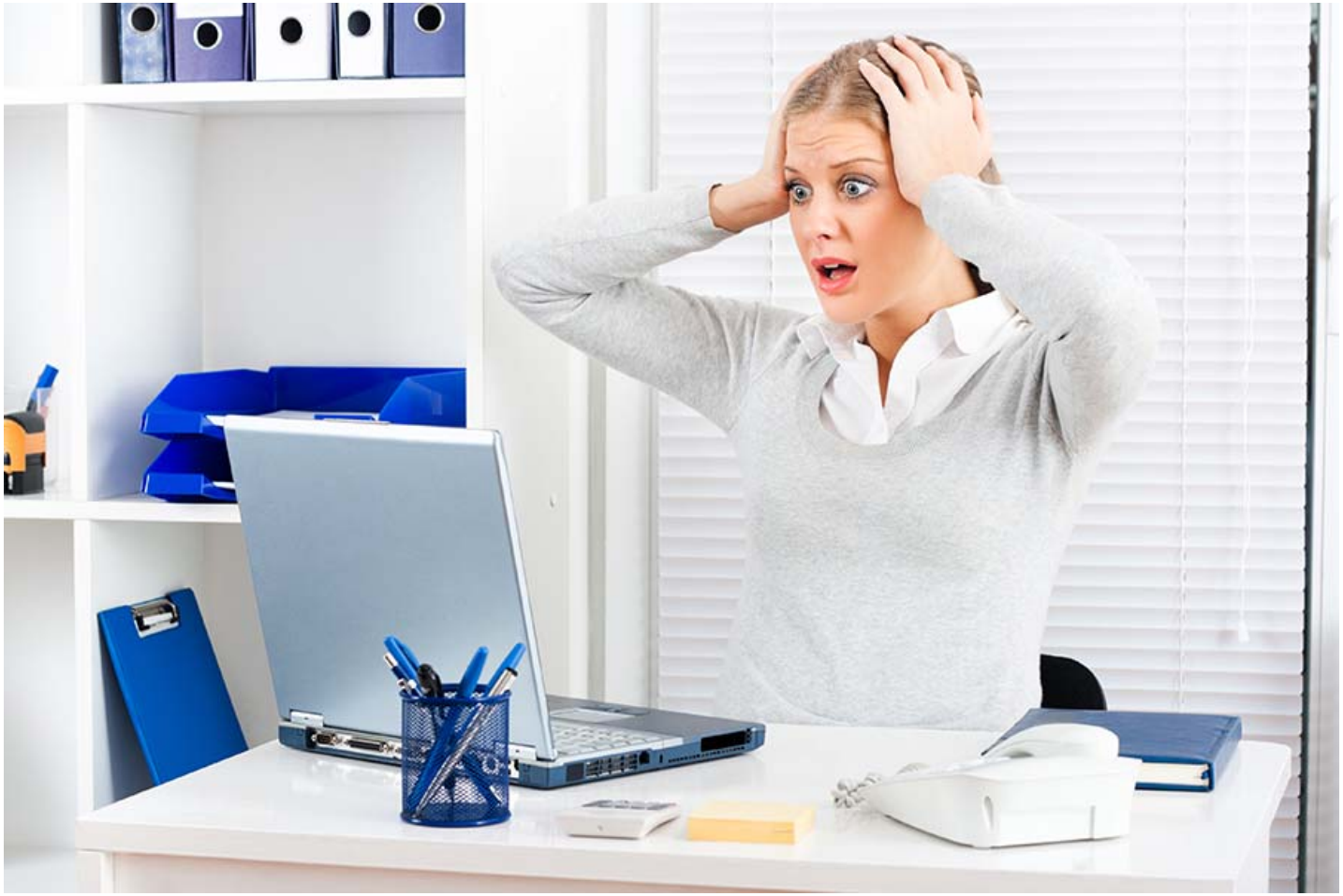
Delete all stored health information before discarding or reusing the mobile device.

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



HOLLAND&HART LLP

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

HOLLAND&HART LLP

Malware Alters CT Scans and Cre

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

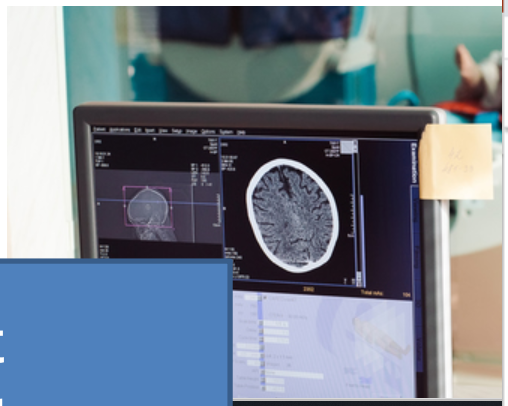
Malware Alters CT Scans and Creates and Removes Tumors

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

Search

Search

Posted By HIPAA Journal on Apr 5, 2019



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

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

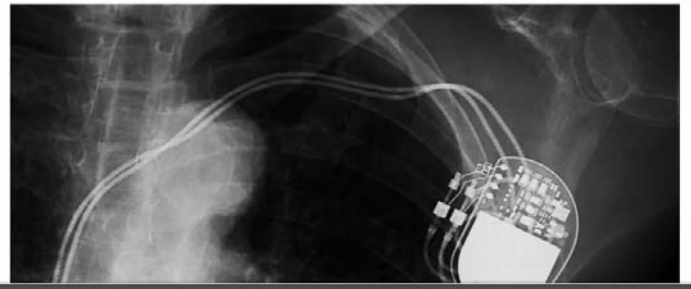
SHARE

SHARE

TWEET

COMMENT

EMAIL



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

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

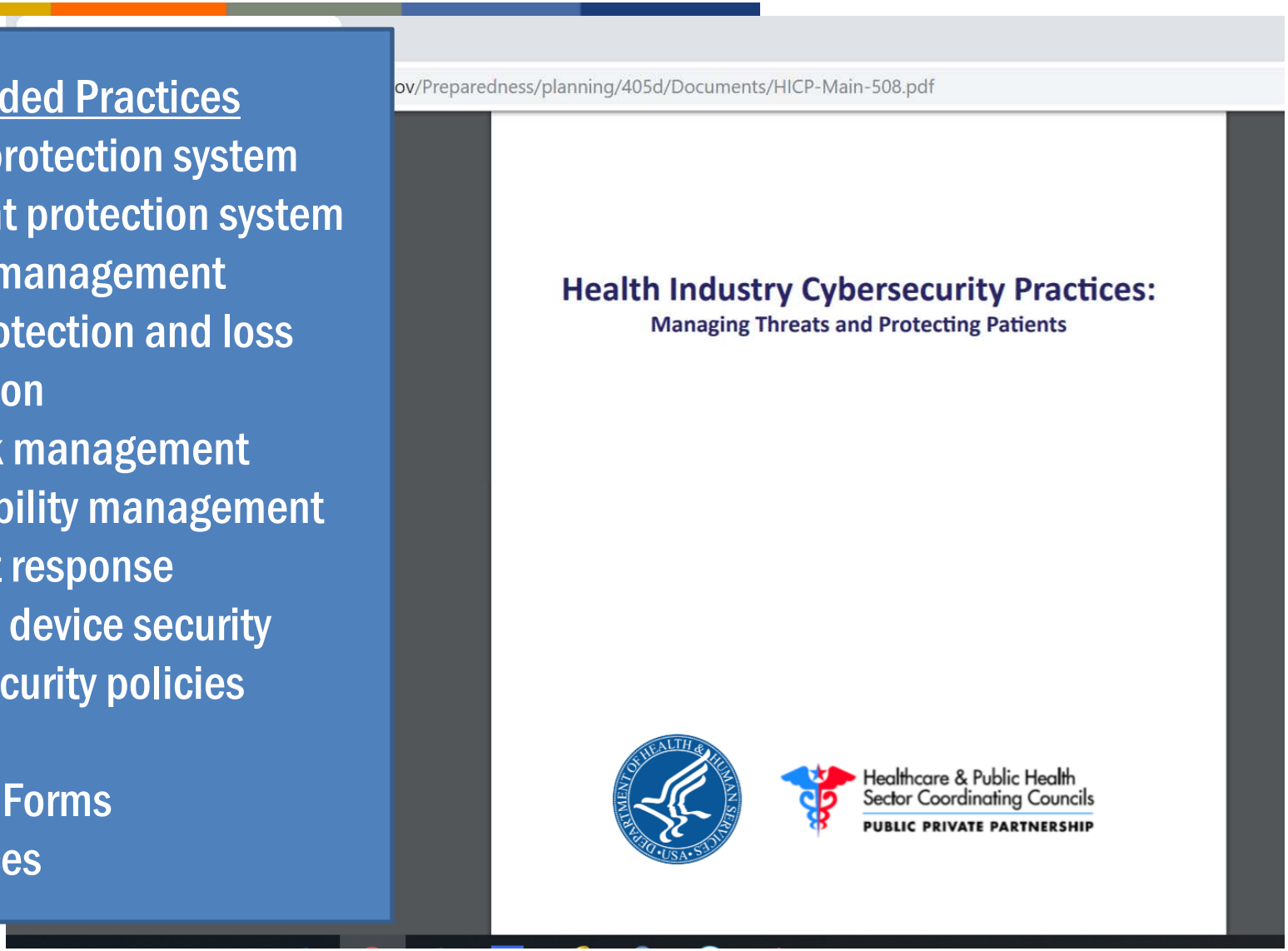
- Communicate with device mfr
- Follow mfr instructions
- Patch devices after patch has been validated and tested
- Assess security on networked devices
- Assess devices risks
- Contract carefully
- Access controls for outsiders

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



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

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 Criminal Penalties

Applies if employees or others obtain or disclose protected health info from a covered entity without authorization.

Conduct	Penalty
Knowingly obtain info in violation of law	• $50,000 fine • 1 year in prison
Committed under false pretenses	• $100,000 fine • 5 years in prison
Intent to sell, transfer, or use for commercial gain, personal gain, or malicious harm	• $250,000 fine • 10 years in prison

(42 USC 1320d-6(a))

HOLLAND&HART LLP

HIPAA Civil Penalties

Conduct	Penalty
Did not know and should not have known of violation	• $114 to $57,051 per violation • Up to $28,525 per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Violation due to reasonable cause	• $1,141 to 57,051per violation • Up to $114,102 per type per year • No penalty if correct w/in 30 days • OCR may waive or reduce penalty
Willful neglect, but correct w/in 30 days	• $11,182 to $57,051 per violation • Up to $285,255 per type per year • Penalty is mandatory
Willful neglect, but do not correct w/in 30 days	• At least $57,051 per violation • Up to $1,711,533 per type per year • Penalty is mandatory

(45 CFR 160.404; see also 74 FR 56127)

HIPAA: Avoiding Civil Penalties

You can likely avoid HIPAA civil penalties if you:

- Have required policies and safeguards in place
- Train personnel and document training.
- Respond immediately to mitigate and correct any violation.
- Timely report breaches if required.

No "willful neglect" = No penalties if correct within 30 days.

HIPAA: Additional Consequences

- State attorney general can bring lawsuit.
  - $25,000 fine per violation + fees and costs.
- Under HITECH, patients may recover % of fines.
  - Waiting for final rules.
- Patients can probably bring lawsuit.
  - No private cause of action under HIPAA, but HIPAA may represent standard of care.
- Must impose employee sanctions.
- HHS is conducting audits.
- Must self-report breach of unsecured PHI.

It's better to comply.

HIPAA Privacy Rule

- May not use or disclose protected health info ("PHI") without patient's authorization except in limited circumstances.
- Must give patients certain rights concerning their PHI.
- Must implement reasonable safeguards to protect PHI.
- Must execute business associate agreements.

(45 CFR 164.502-.514)

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

OCR Settlements in 2018 (record $28.7 million)		
12/18	Hospital allowed access to 62,500 patient records via internet. No risk analysis, inadequate security systems, no BAA.	$3,000,000
12/18	Hospital failed to terminate former employees access to eHI, allowing access to ePHI. No BAA.	$111,400
12/18	Hospital's PHI was viewable on vendor's Website. Failed to conduct risk assessment, implement security policies, or execute BAA.	$500,000
10/18	Anthem cyberattack exposed PHI of 79,000,000 people. Resulted from spear phishing e-mails. Failed to conduct risk assessment, review system activity, or implement adequate security.	$16,000,000 (largest ever)
6/18	Theft of unencrypted laptop from home of hospital employee. Failure to encrypt devices despite identifying that as a risk.	$4,348,000
2/18	Fresenius allowed unauthorized access to ePHI. Failed to conduct appropriate risk assessment, protect hardware containing ePHI when left facility, encrypt data.	$3,500,000
12/17	Cancer center failed to implement safeguards to protect ePHI despite prior warnings that its information had been hacked.	$2,300,000
4/17	Monitoring company's laptop containing 1,390 patients' info stolen from car; insufficient risk analysis and no finalized security policies.	$2,500,000
4/17	FQHC's info hacked; no risk analysis and insufficient security rule safeguards.	$400,000

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.

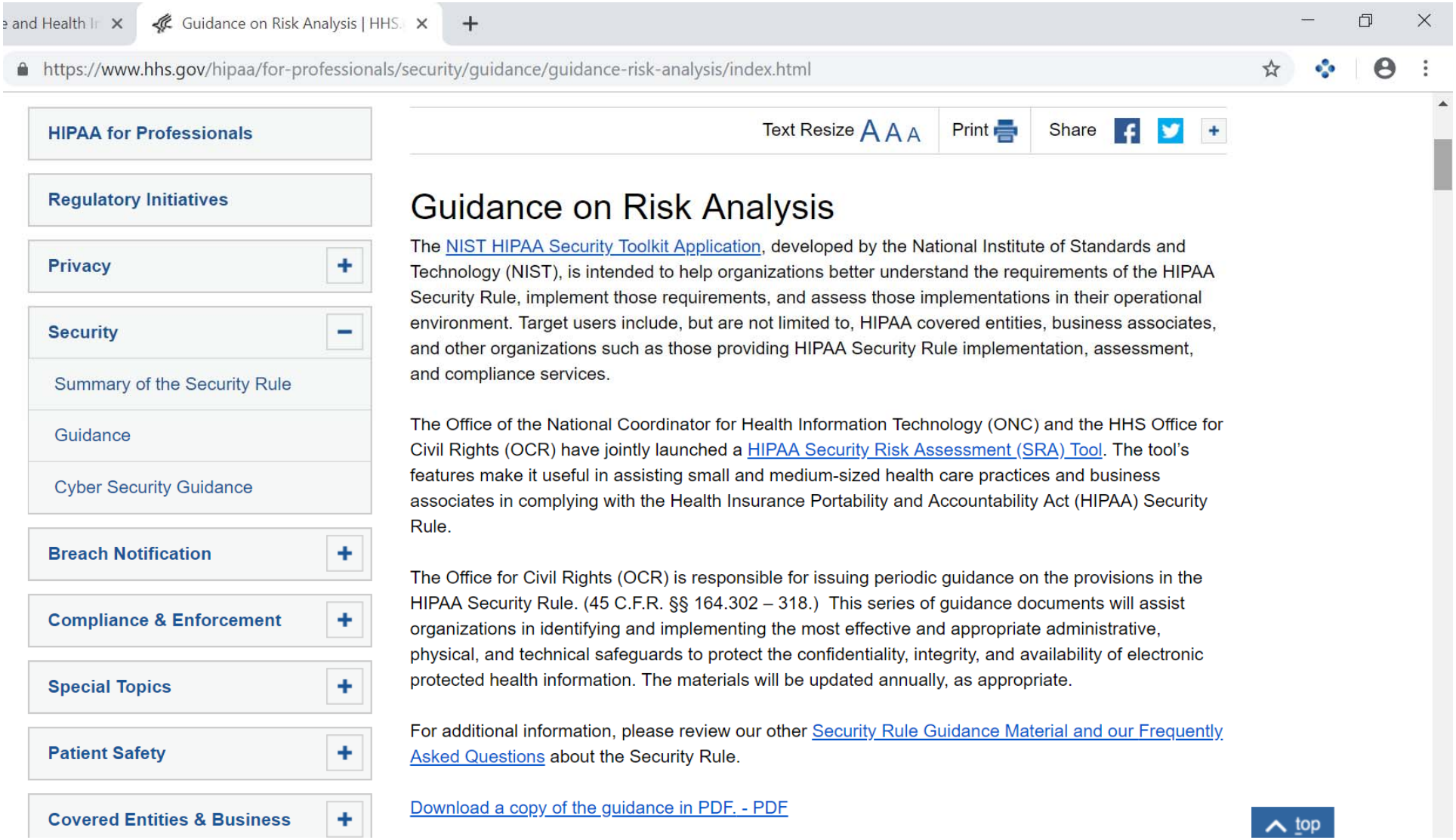
(45 CFR 164.308(a)(1))

- Ongoing process.

Elements

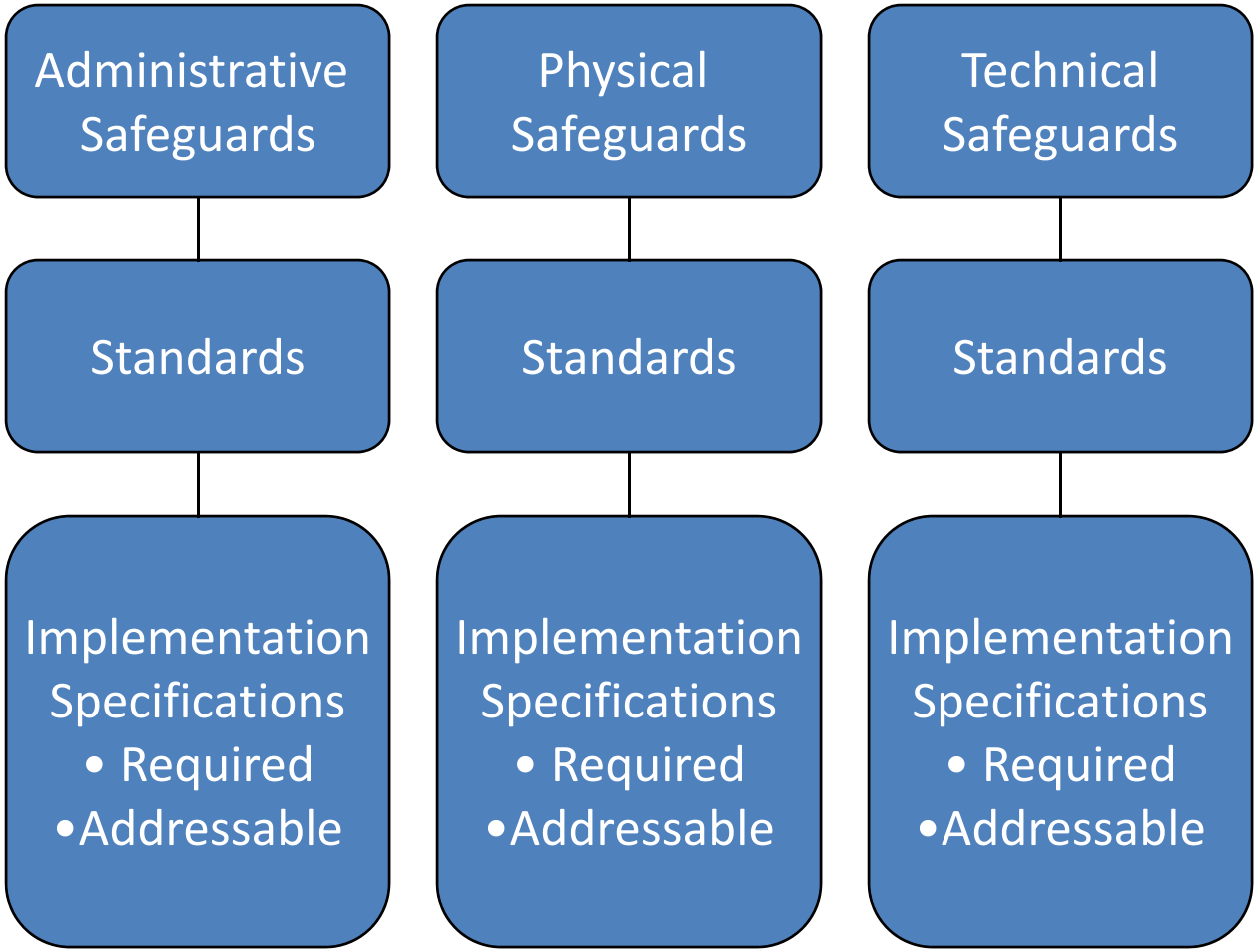
- Scope includes all ePHI in any format, including hard drives, portable media, mobile devices, servers, transmission, storage, networks, etc.
- Track flow of ePHI
- Identify threats and vulnerabilities
- Asses current security measures
- Assess likelihood of threat
- Determine level of risk
- Confirm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

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



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

Safeguards


Administrative Safeguards
Physical Safeguards
Technical Safeguards
Standards
Standards
Standards
Implementation Specifications
• Required
•Addressable
Implementation Specifications
• Required
•Addressable
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.

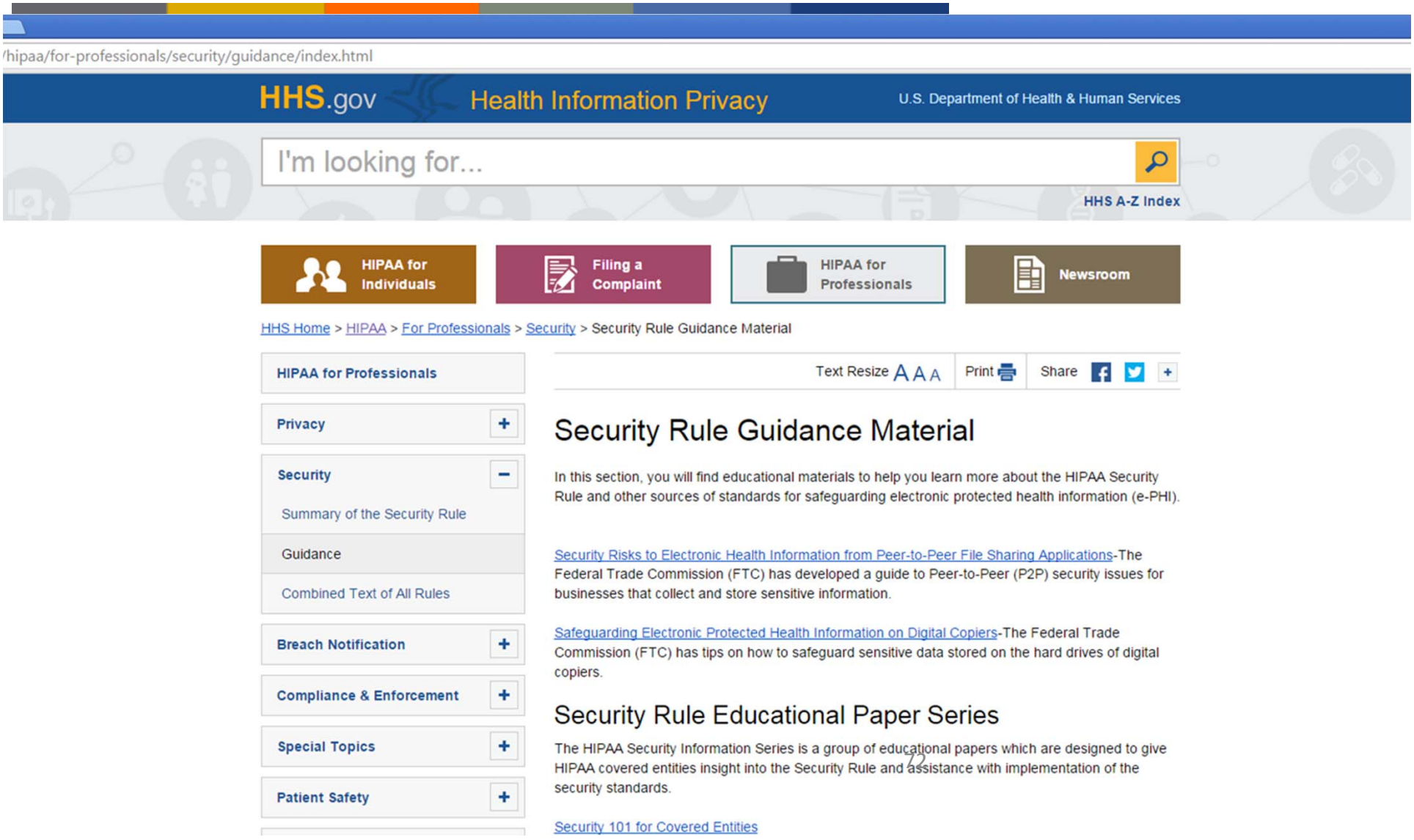
(45 CFR 164.310)

Security Rule: Technical Safeguards

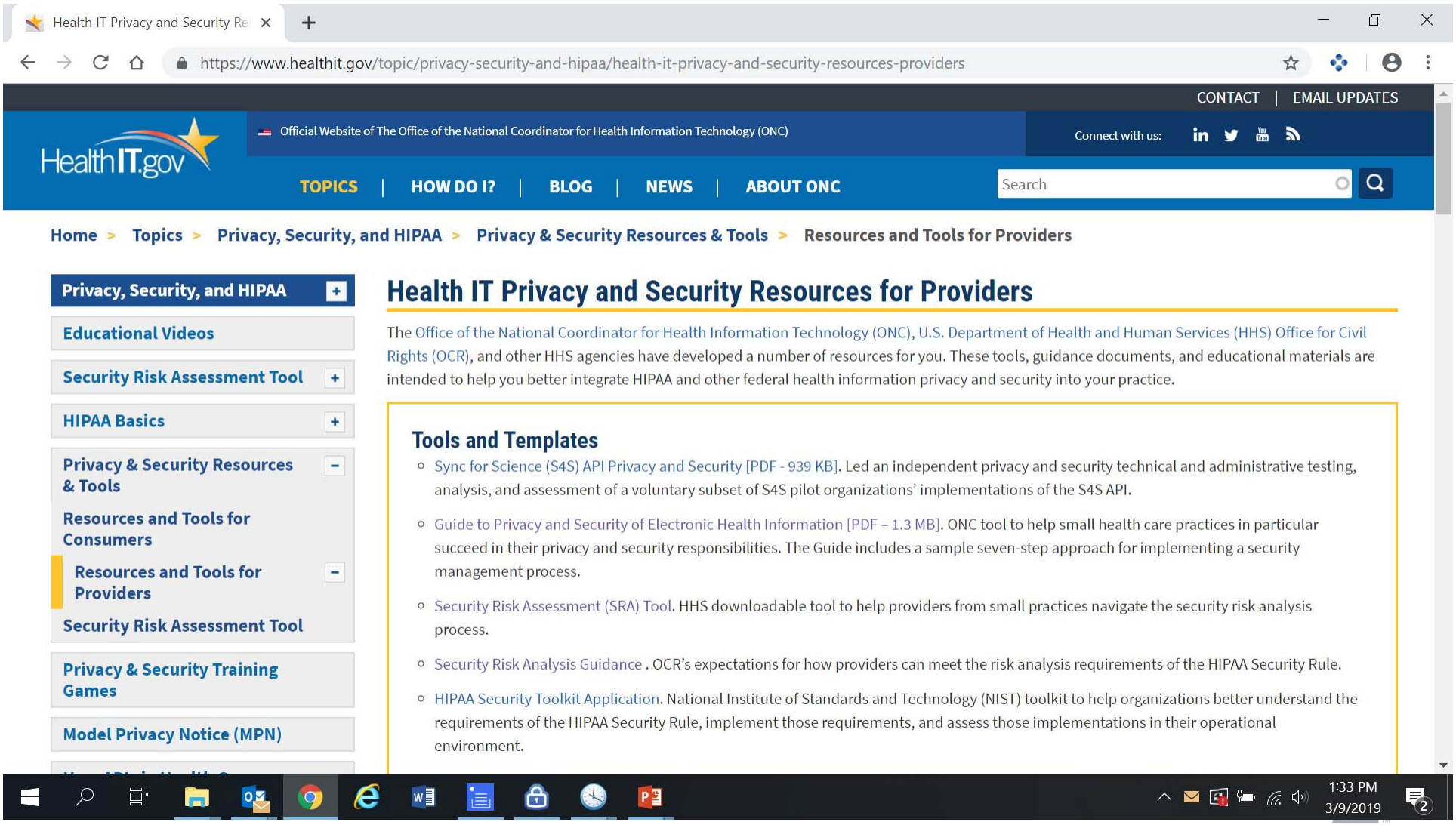
- Assign unique names or numbers to track users.
- Implement automatic logoff process.
- Use encryption and decryption, where appropriate.
- Implement systems to audit use of e-PHI.
- Implement safeguards to protect e-PHI from alteration or destruction.
- Implement methods to ensure e-PHI has not been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



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



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.

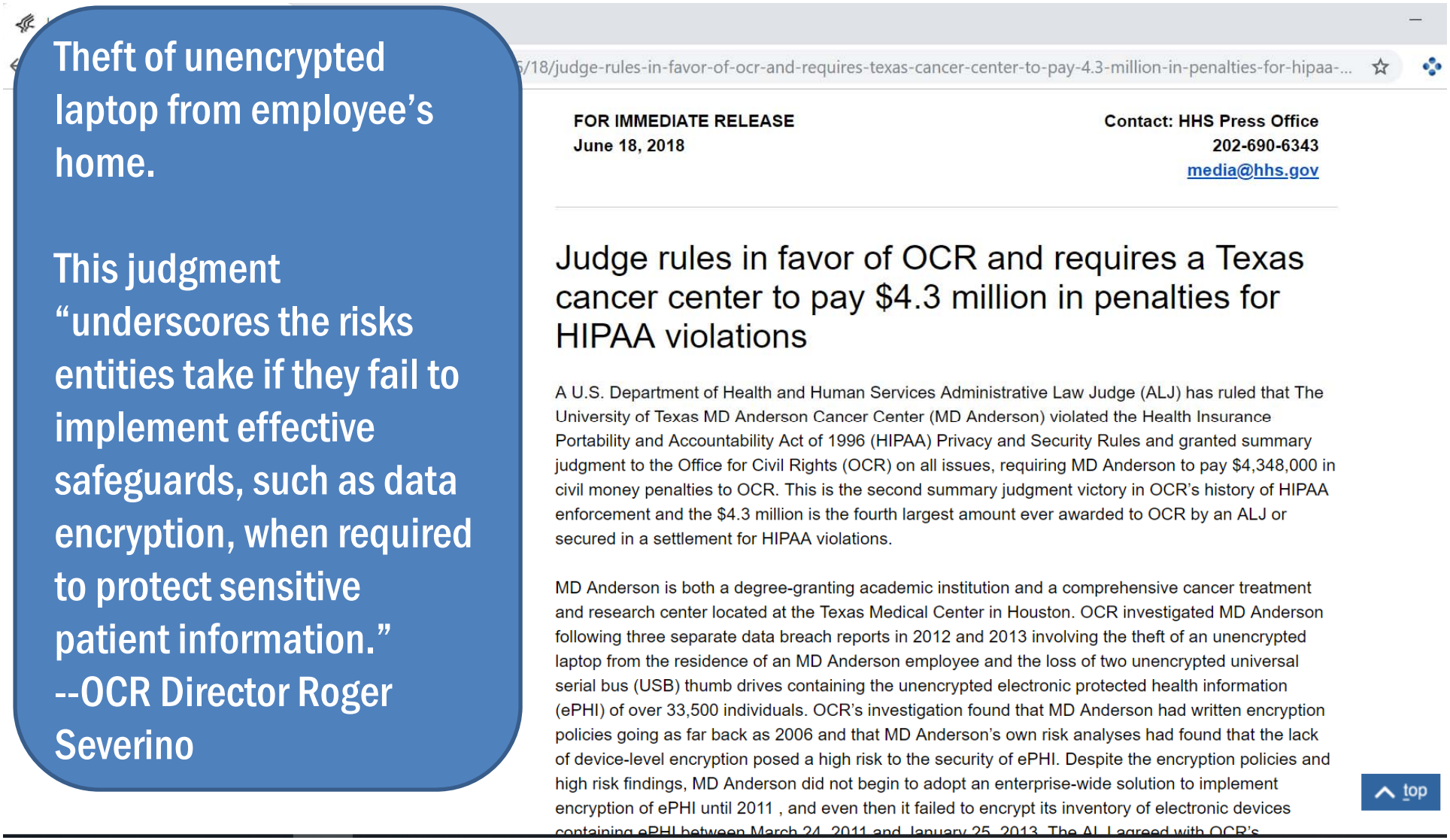
  (2)(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

- 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



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

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

top

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)

Business Associates

- May disclose PHI to business associates if have valid business associate agreement ("BAA").

(45 CFR 164.314 and .504(e))

- Business associates =
  - Entities that create, receive, maintain, or transmit PHI on behalf of a covered entity.
  - Covered entities acting as business associates.
  - Subcontractors of business associates.

(45 CFR 160.103)

Business Associates

Common Business Associates

- External IT support
- Software vendors
- Data storage, processing, and destruction companies
- Billing and coding
- Consultants
- Management companies
- Auditors
- Accountants
- Lawyers
- Others?

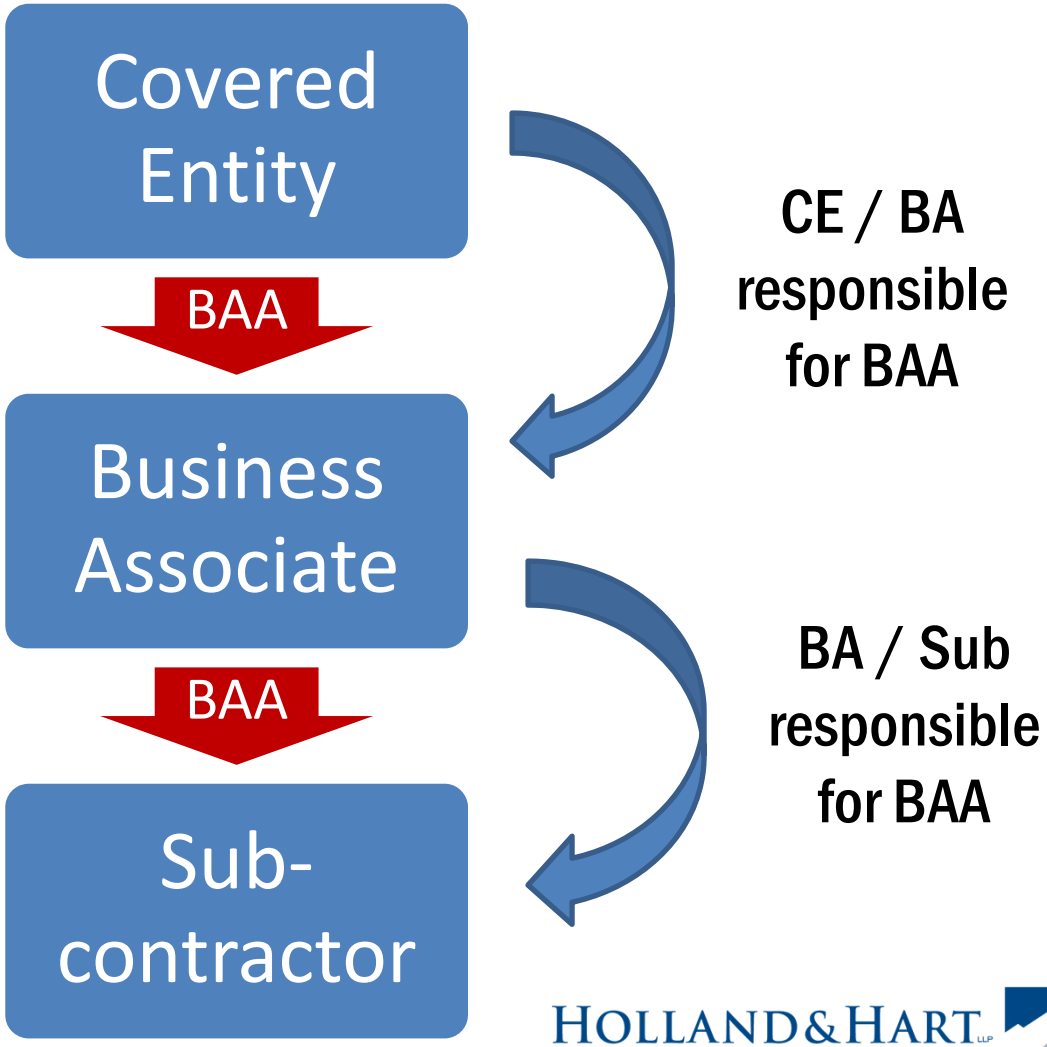
Not Business Associates

- Entities who are not receiving PHI to perform function for a covered entity or the covered entity's business associate.
- Employees
- Workforce members
- Persons whose access is incidental only, e.g., janitor, plumber, etc.

Business Associate Agreements

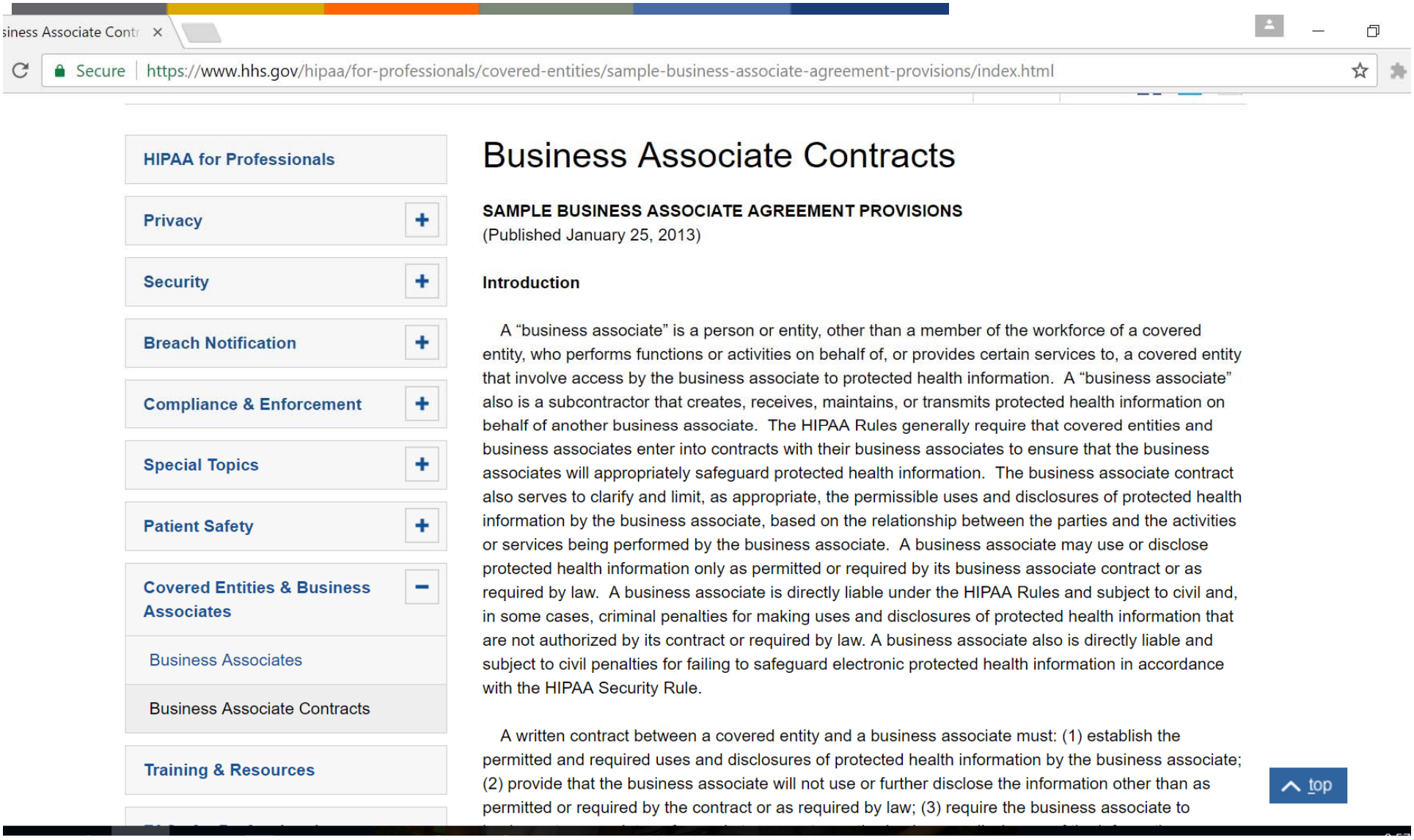
Must contain required terms, e.g.,

- Permitted uses
- Must comply with Security Rule
- Must report breaches
- Must get BAAs with subcontractors
- Must assist covered entity in responding to patient rights
- Termination.



HOLLAND&HART LLP

https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html



Recent OCR settlements based in whole or part on failure to have BAA

Date	Conduct	Penalty
12/18	Health system failed to have BAA with contractor that maintained ePHI	$3,000,000
12/18	Hospital failed to have BAA with web-based vendor	$111,400
12/18	Hospitalist group failed to enter BAA with billing company	$500,000
12/17	Cancer care center failed to enter BAAs with vendors	$2,300,000
4/17	Pediatric clinics failed to enter BAAs with file storage company	$31,000
8/16	Health network failed to enter BAAs	$5,500,000
7/16	Medical university failed to obtain BAA with cloud-based storage vendor	$2,700,000
4/16	Radiology group failed to have BAA; x-rays left by vendor	$750,000
3/16	Health system failed to have BAA; laptop stolen from care of BA's employee	$1,550,000

Breach Reporting (45 CFR 164.400)

Breach Notification

- If there is "breach" of "unsecured PHI",
  - Covered entity must notify:
    - Each individual whose unsecured PHI has been or reasonably believed to have been accessed, acquired, used, or disclosed.
    - HHS.
    - Local media, if breach involves > 500 persons in a state.
  - Business associate must notify covered entity.

(45 CFR 164.400 et seq.)

"Breach" of Unsecured PHI

- Acquisition, access, use or disclosure of PHI in violation of privacy rules is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the info has been compromised based on a risk assessment of the following factors:
  - nature and extent of PHI involved;
  - unauthorized person who used or received the PHI;
  - whether PHI was actually acquired or viewed; and
  - extent to which the risk to the PHI has been mitigated,

  unless an exception applies.

(45 CFR 164.402)

"Breach" of Unsecured PHI

- "Breach" defined to exclude the following:
  - Unintentional acquisition, access or use by workforce member if made in good faith, within scope of authority, and PHI not further disclosed in violation of HIPAA privacy rule.
  - Inadvertent disclosure by authorized person to another authorized person at same covered entity, business associate, or organized health care arrangement, and PHI not further used or disclosed in violation of privacy rule.
  - Disclosure of PHI where covered entity or business associate have good faith belief that unauthorized person receiving info would not reasonably be able to retain info

(45 CFR 164.402)

Notice to Individual

- Without unreasonable delay but no more than 60 days of discovery.
  - When known by anyone other than person who committed breach.
- Written notice to individual.
  - By mail.
  - Must contain elements, including:
    - Description of breach
    - Actions taken in response
    - Suggested action individual should take to protect themselves.

(45 CFR 164.404(d))

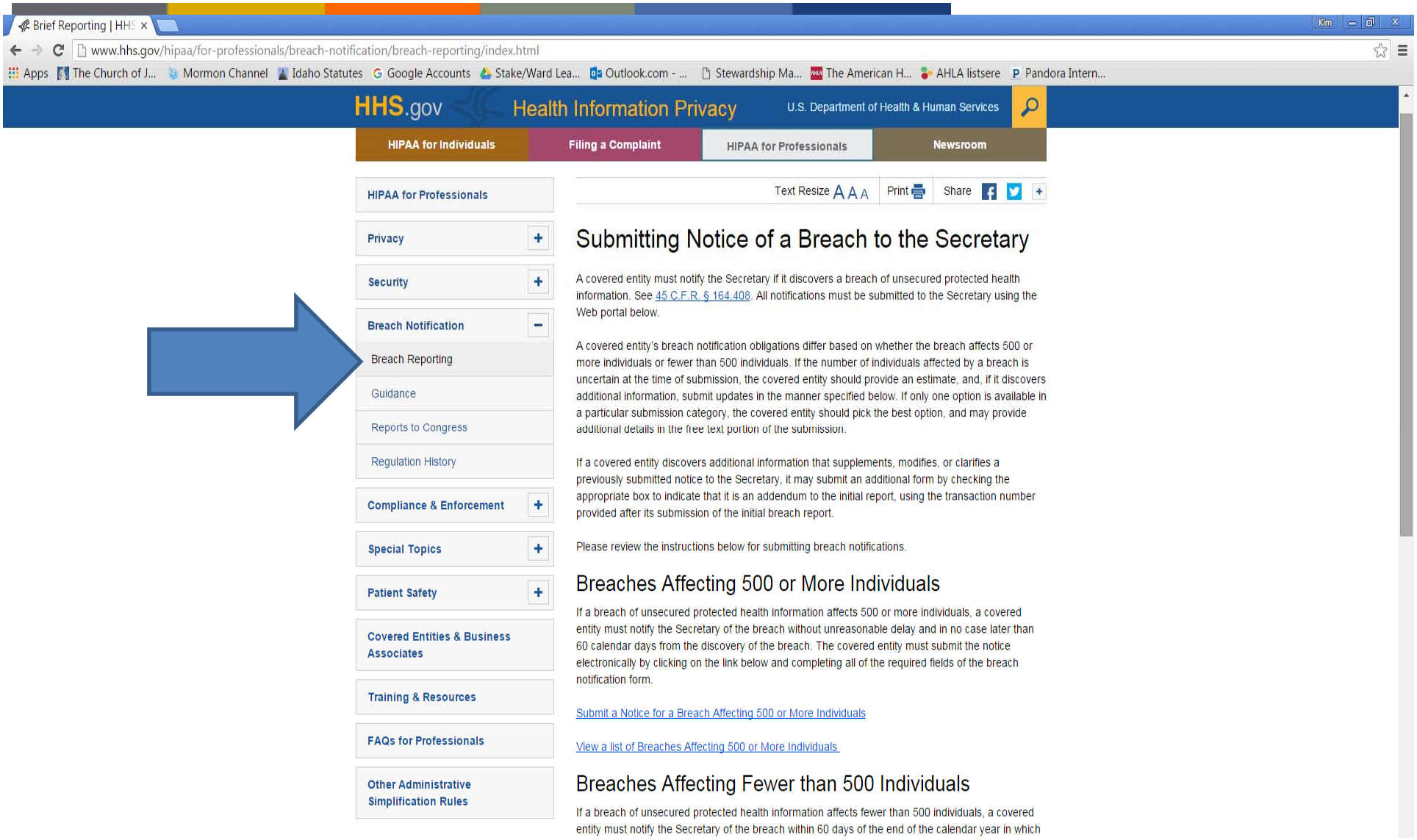
Notice to HHS

- If breach involves fewer than 500 persons:
  - Submit to HHS annually within 60 days after end of calendar year in which breach was discovered (i.e., by March 1).
- If breach involves 500 or more persons:
  - Notify HHS contemporaneously with notice to individual or next of kin, i.e., without unreasonable delay but within 60 days.

(45 CFR 164.408)

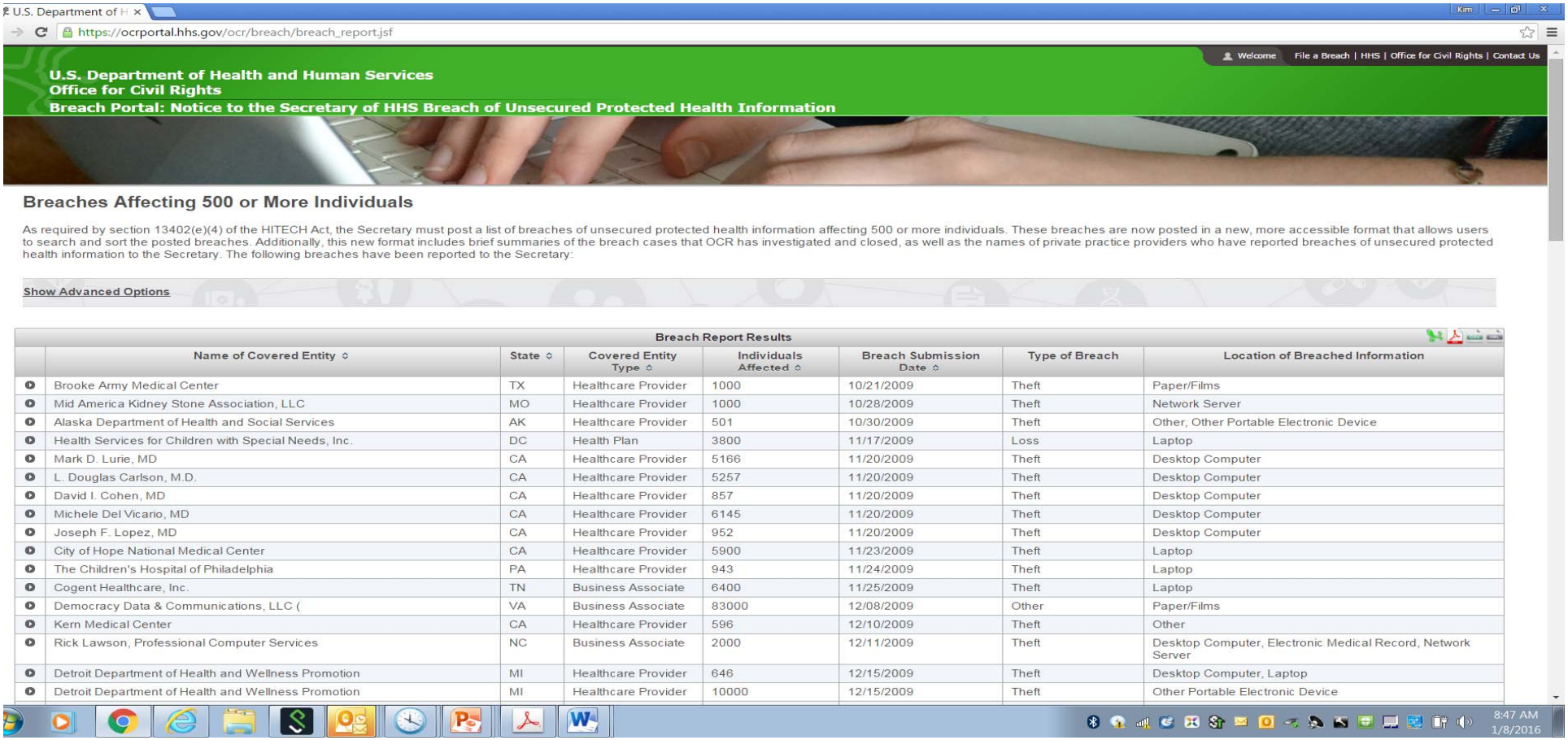
- Submit report at http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

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



Notice to HHS

- HHS posts list of those with breaches involving more than 500 at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsfpersons



U.S. Department of H ×

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Welcome | File a Breach | HHS | Office for Civil Rights | Contact Us

U.S. Department of Health and Human Services
Office for Civil Rights
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
Mark D. Lurie, MD	CA	Healthcare Provider	5166	11/20/2009	Theft	Desktop Computer
L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer
David I. Cohen, MD	CA	Healthcare Provider	857	11/20/2009	Theft	Desktop Computer
Michele Del Vicario, MD	CA	Healthcare Provider	6145	11/20/2009	Theft	Desktop Computer
Joseph F. Lopez, MD	CA	Healthcare Provider	952	11/20/2009	Theft	Desktop Computer
City of Hope National Medical Center	CA	Healthcare Provider	5900	11/23/2009	Theft	Laptop
The Children's Hospital of Philadelphia	PA	Healthcare Provider	943	11/24/2009	Theft	Laptop
Cogent Healthcare, Inc.	TN	Business Associate	6400	11/25/2009	Theft	Laptop
Democracy Data & Communications, LLC (	VA	Business Associate	83000	12/08/2009	Other	Paper/Films
Kern Medical Center	CA	Healthcare Provider	596	12/10/2009	Theft	Other
Rick Lawson, Professional Computer Services	NC	Business Associate	2000	12/11/2009	Theft	Desktop Computer, Electronic Medical Record, Network Server
Detroit Department of Health and Wellness Promotion	MI	Healthcare Provider	646	12/15/2009	Theft	Desktop Computer, Laptop
Detroit Department of Health and Wellness Promotion	MI	Healthcare Provider	10000	12/15/2009	Theft	Other Portable Electronic Device

8:47 AM
1/8/2016

Notice to Media

- If breach involves unsecured PHI of more than 500 residents in a state, covered entity must notify prominent media outlets serving that state (e.g., issue press release).
  - Without unreasonable delay but no more than 60 days from discovery of breach.
  - Include same content as notice to individual.

(45 CFR 164.406)

HOLLAND&HART LLP

Notice by Business Associate

- Business associate must notify covered entity of breach of unsecured PHI:
  - Without unreasonable delay but no more than 60 days from discovery.
  - Notice shall include to extent possible:
    - Identification of individuals affected, and
    - Other info to enable covered entity to provide required notice to individual.

(45 CFR 164.410)

- Business associate agreements may impose different deadlines.

Wyoming Breach Reporting Statute (WSA 40-12-501)

HOLLAND&HART LLP

Wyoming Breach Reporting Statute

- Generally requires commercial entities to immediately investigate and notify subject persons if:
  - Unauthorized acquisition of computerized data that materially compromises security, confidentiality, or integrity of data;
  - "personal identifying info", i.e.,
    - Name + certain other identifiers (e.g., SSN; driver's license; account #, credit card #, debit card # + code; tribal ID; username or e-mail + password; birth/marriage certificate; health info; individual tax ID);
  - Misuse could cause injury to Wyoming resident; and
  - Misuse is likely to occur.
- AG may bring suit to enforce statute or recover damages.
- Compliance with HIPAA satisfies Wyoming statute.

(WSA 40-12-502)

Additional Resources

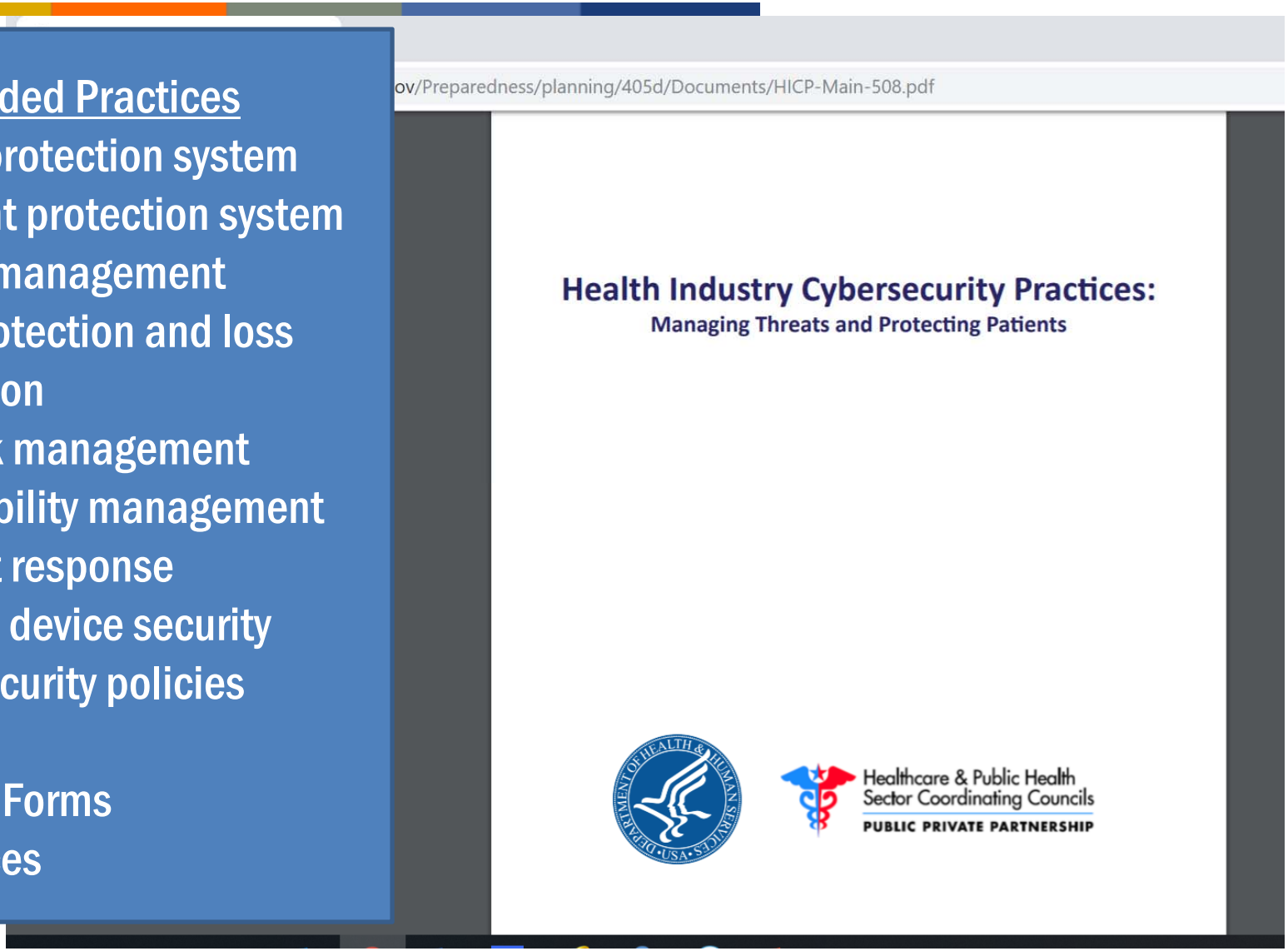
HOLLAND&HART LLP

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



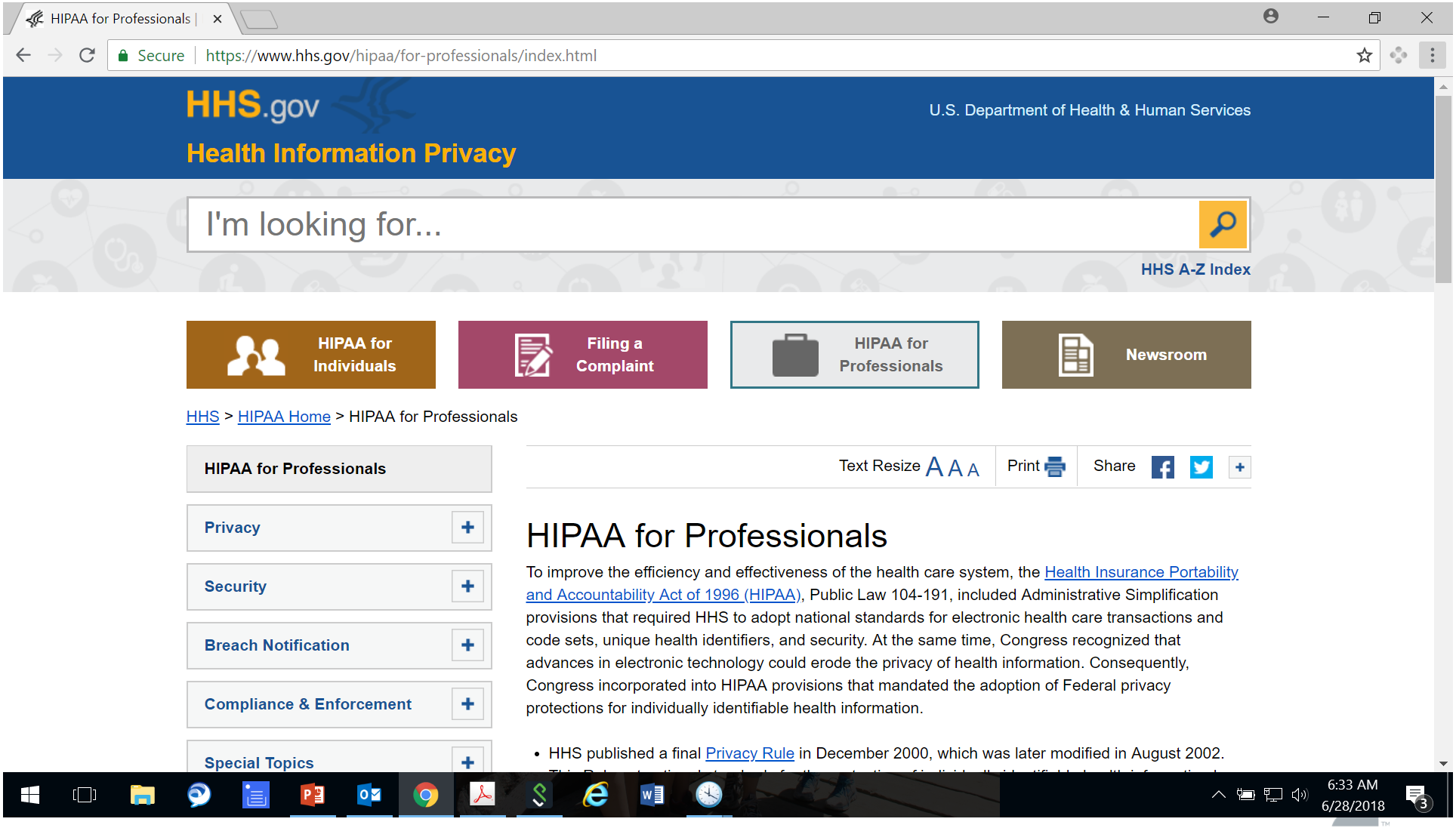
Appendix F: Resources

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

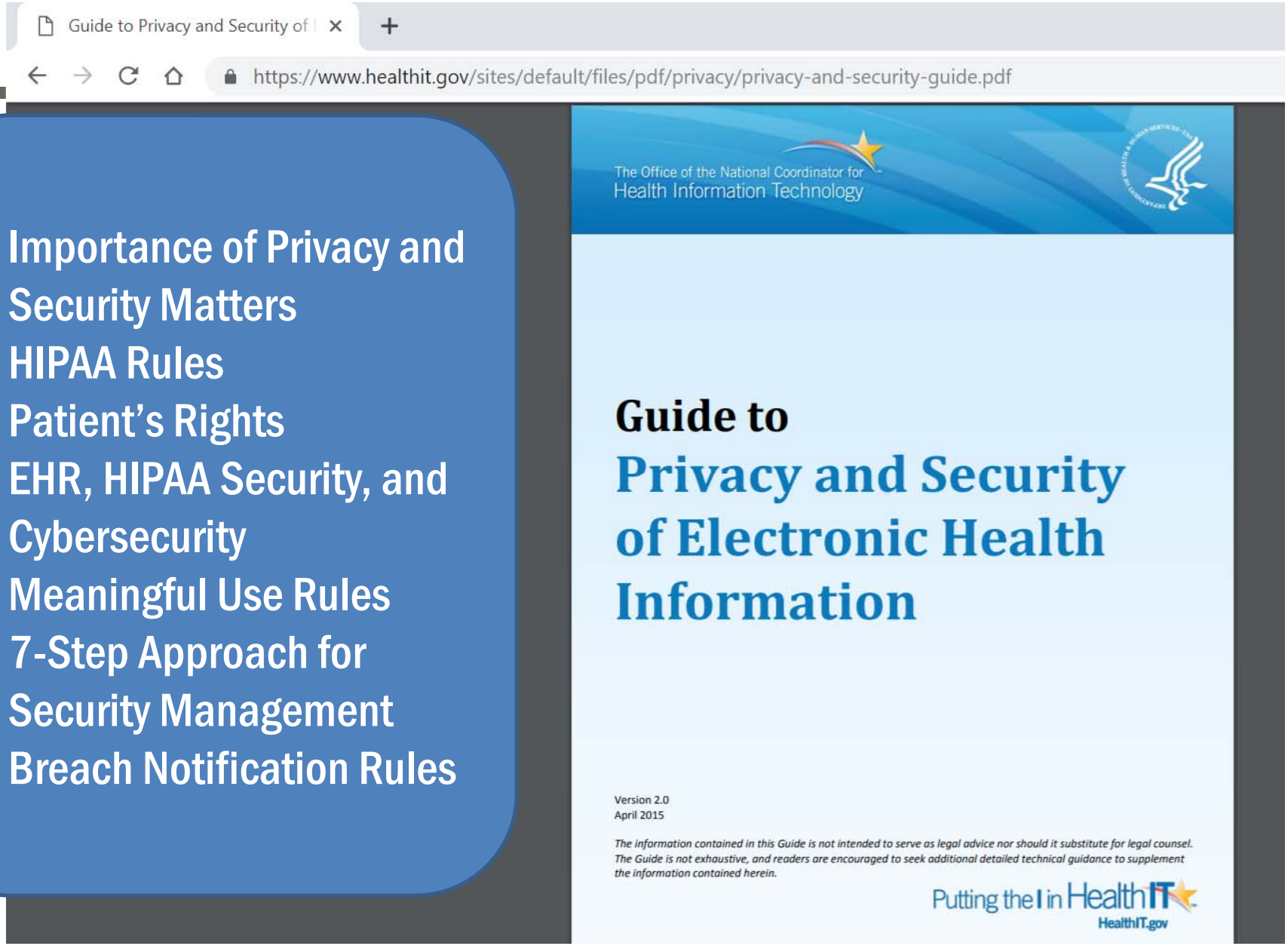
- **Security Risk Assessment Tool**
  - **Link:** https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment
  - **Description:** Security Risk Assessment Tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and 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

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



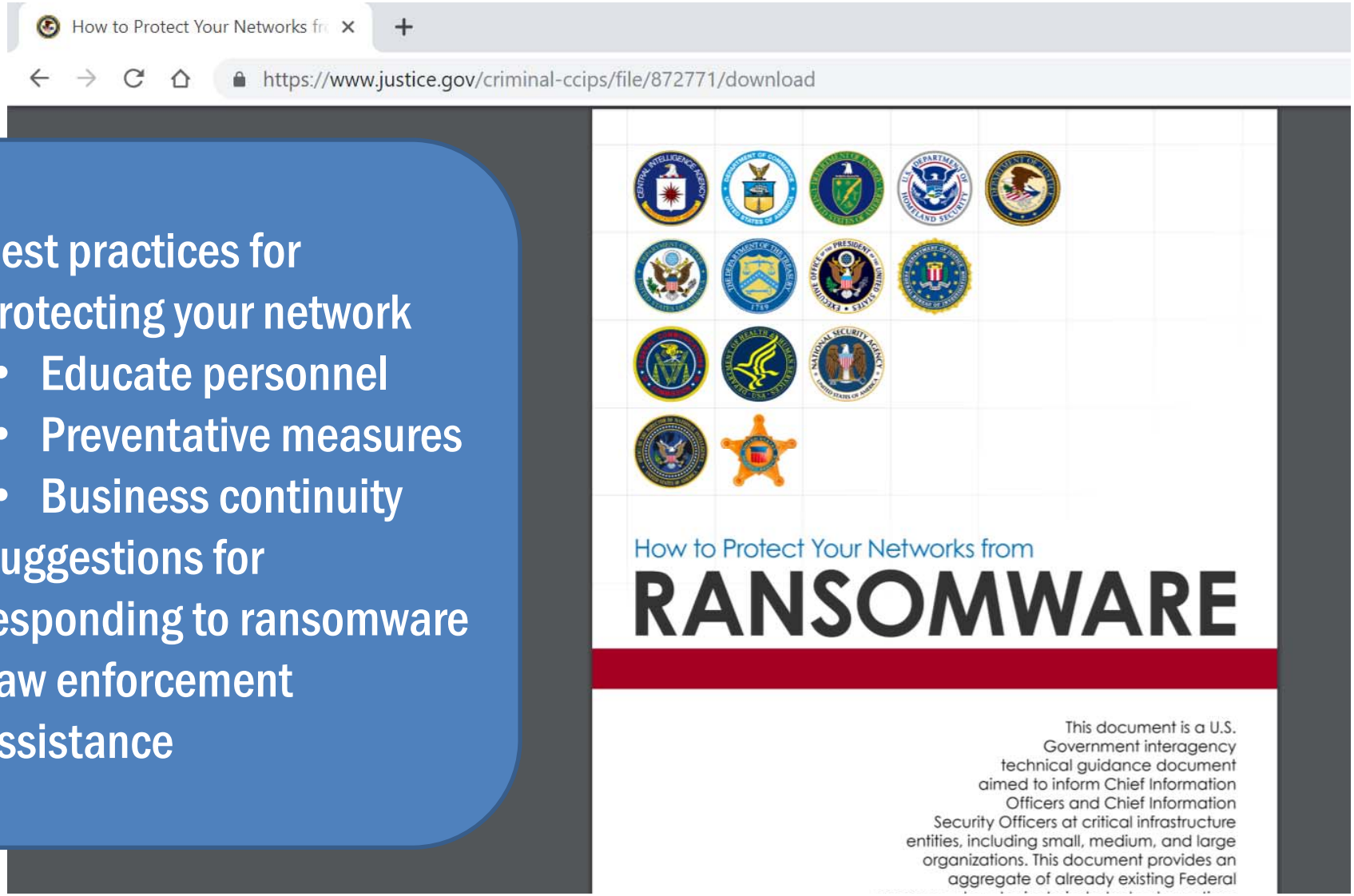
https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-

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



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



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

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

Past Webinars
Publications

HOLLAND&HART LLP

Kim C. Stanger

Office: (208) 383-3913

Cell: (208) 409-7907

kcstanger@hollandhart.com

HOLLAND&HART LLP