CYBERSECURITY

KIM C. STANGER

Compliance Bootcamp

(2/20)

HOLLAND&HART LLP

This presentation is designed to provide general information on pertinent legal topics. The statements made are provided for educational purposes only. They do not constitute legal or financial advice nor do they necessarily reflect the views of Holland & Hart LLP or any of its attorneys other than the author. This presentation is not intended to create an attorney-client relationship between you and Holland & Hart LLP. Substantive changes in the law subsequent to the date of this presentation might affect the analysis or commentary. Similarly, the analysis may differ depending on the jurisdiction or circumstances. 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

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?

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?

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

CYBERLIABILITY LAWS

- Health Insurance Portability and Accountability Act ("HIPAA"), 45 CFR part 164
- FTC Breach Notification Rule, 16 CFR part 318
  - Applies to vendors of personal health info.
- Federal Trade Comm'n Act ("FTCA") § 5 (15 USC 45(a))
  - Prohibits unfair or deceptive acts affecting commerce.
- State breach notification laws
- State privacy statutes
- State consumer protection statutes

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

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
- Cybersec y Reports and Tools
- G

Suggested Practices

6:15 AM
3/2/2019

HOLLAND&HART LLP

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…

E-MAIL PHISHING ATTACKS

Anthem Pays OCR $16 Million in | Anthem to Pay Record $115M to

0/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html

"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."

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

top

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)

2. Suspicious Subject and content.

PayPal

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

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 Against 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>** 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

File Message

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!

LinkedIn

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

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:

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

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 <u>NOT</u>

- ***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

HOLLAND&HART LLP

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

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.

NBC NEWS HOME TOP VIDEOS DECISION 2016 MORE

TECH > SECURITY

GADGETS INTERNET INNOVATION MOBILE

TECH MAR 23 2016, 5:16 PM ET

Three U.S. Hospitals Hit in String of Ransomware Attacks

by CONNOR MANNION

SHARE

Three U.S. hospitals were hit hard this week by "ransomware" attacks that brought down their systems — the latest providers of medical care to be targeted in this way.

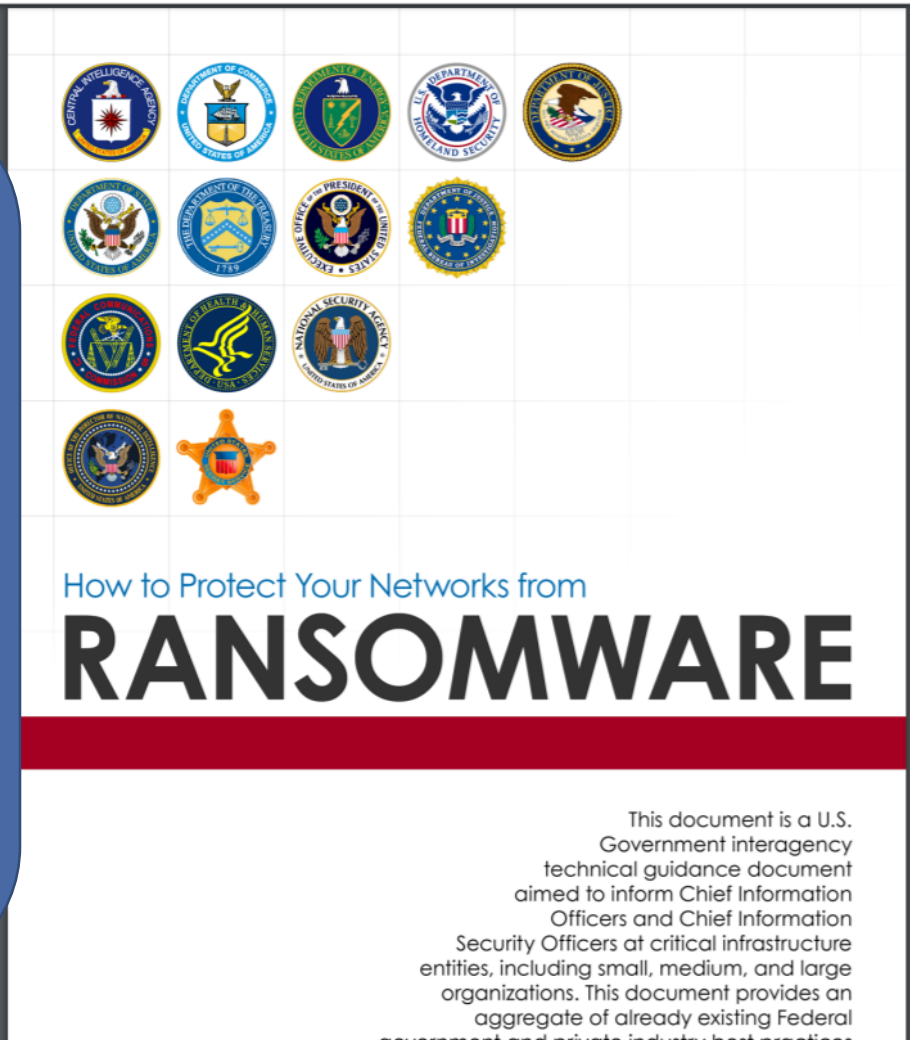
HOLLAND&HART LLP

HTTPS://WWW.JUSTICE.GOV/CRIMINAL-CCIPS/FILE/872771/DOWNLOAD

How to Protect Your Networks fr

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 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

FACT SHEET: Ransomware and HI

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 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 identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;

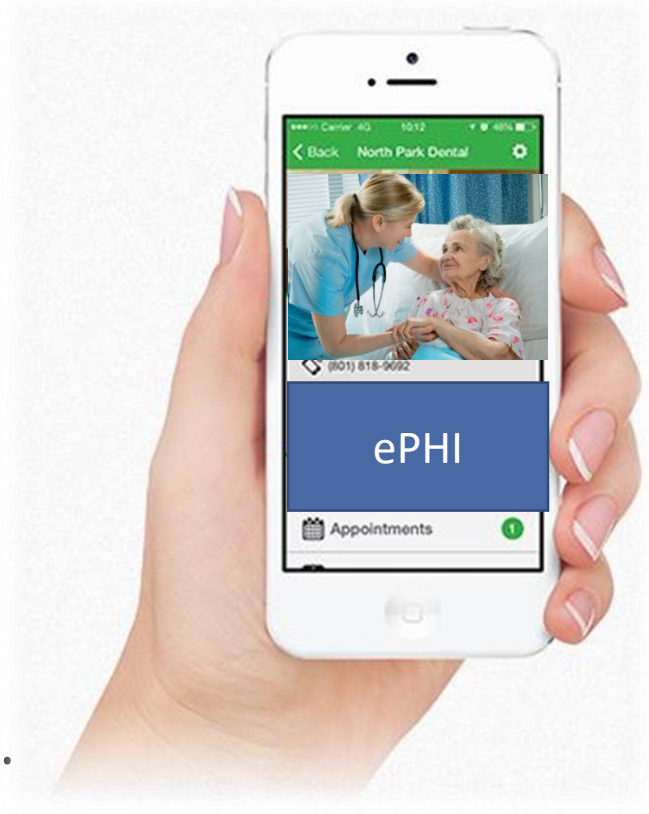
3. LOSS OR THEFT OF EQUIPMENT OR DATA

ComputerHope.com

HOLLAND&HART LLP

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)

<u>The corollary:</u>

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

A-Z Index

About HHS | Programs & Services | Grants & Contracts | Laws & Regulations

Home > About > News > $2.5 million settlement shows that not understanding HIPAA requirements creates risk

Search News Releases

Search

View 2016 - 1991 archive →

Text Resize A A A | Print | Share

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

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 +

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

1:41 PM
3/9/2019

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

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/

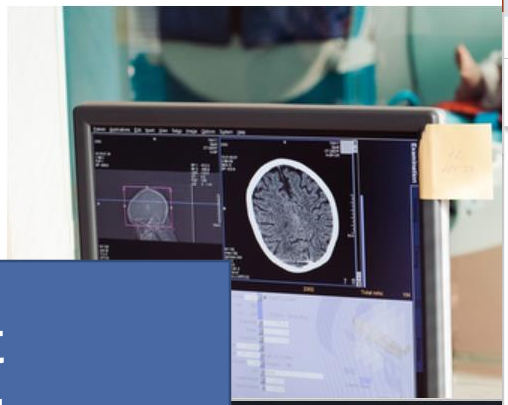
Malware Alters CT Scans and Creates and Removes Tumors

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

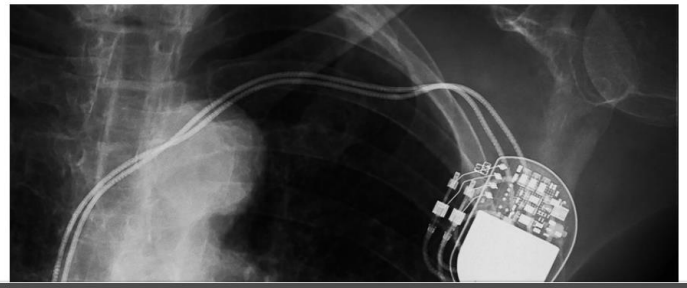
SHARE

SHARE

TWEET

COMMENT

EMAIL



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

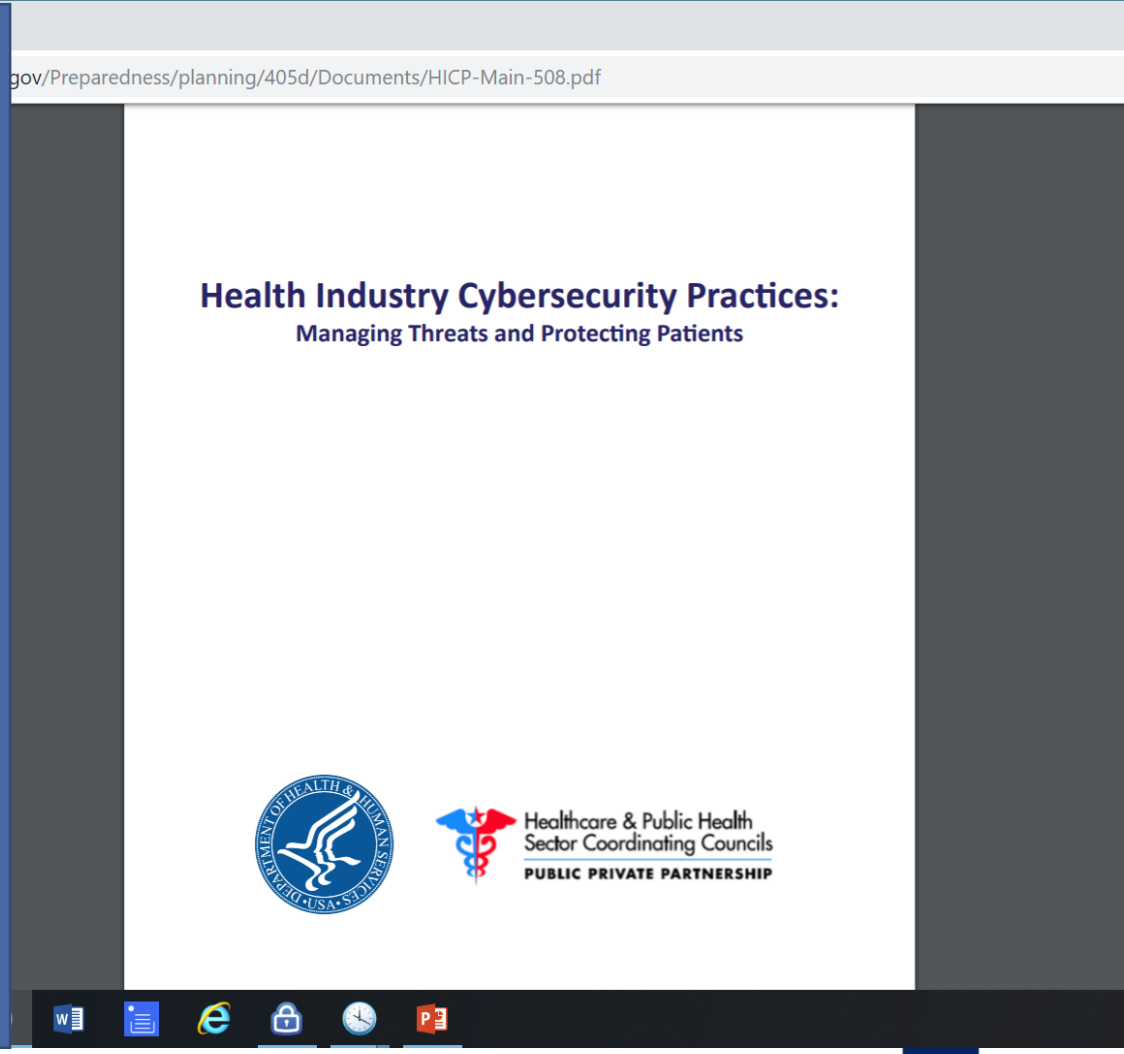
ADDITIONAL RESOURCES

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



HOLLAND&HART LLP

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.

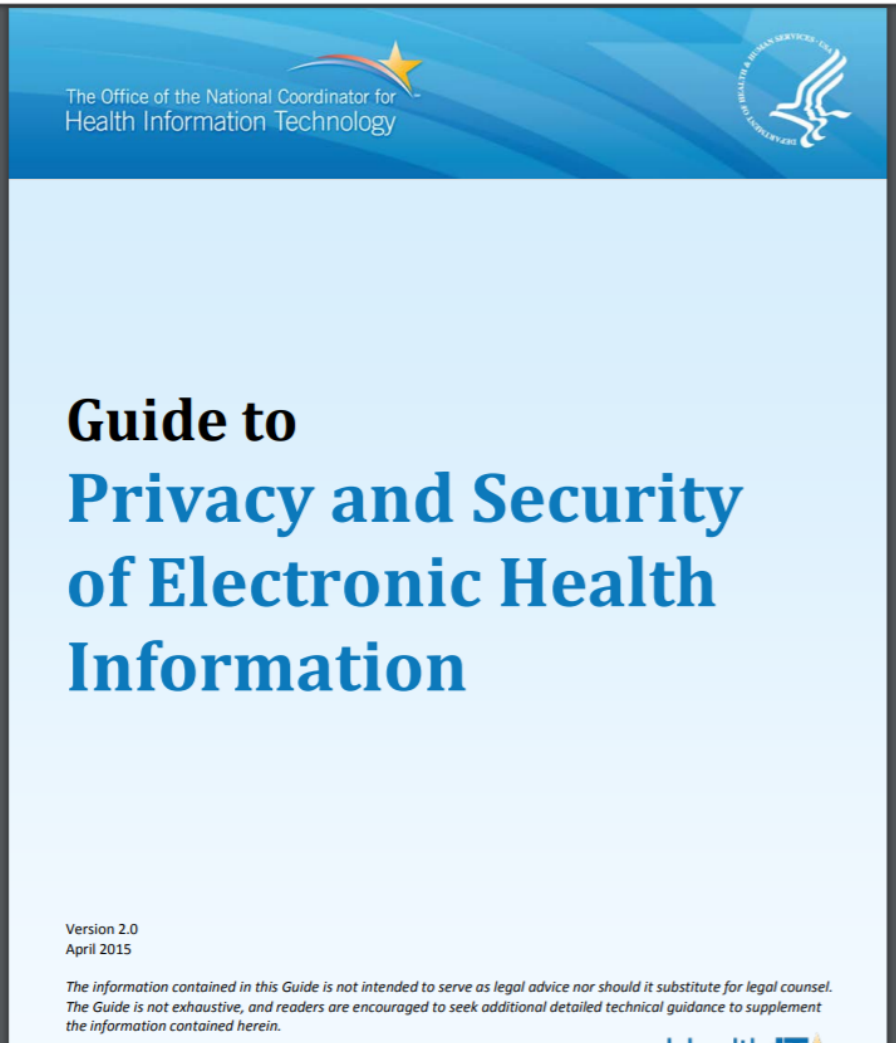
U.S Department of Health and Human Services (HHS) Resources

- **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.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

/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

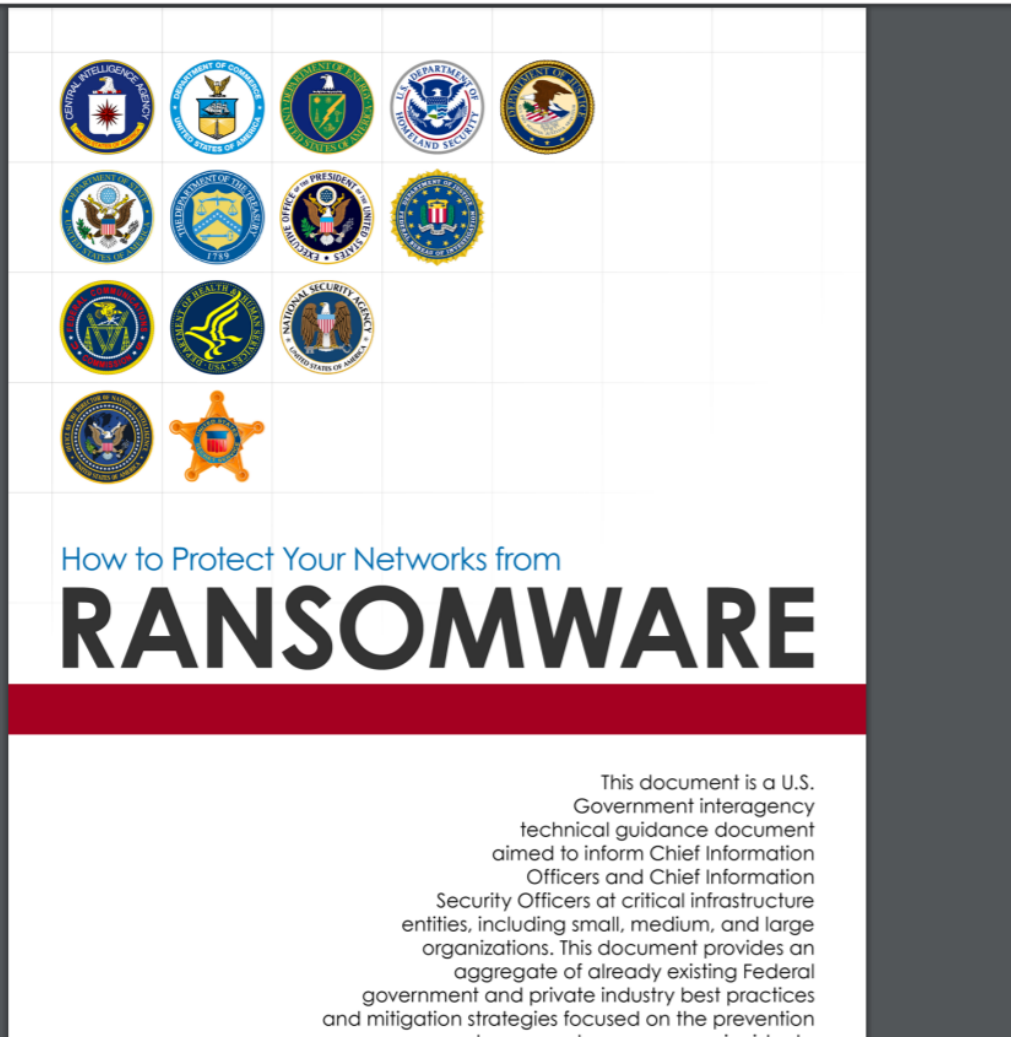
The information contained in this Guide is not intended to serve as legal advice nor should it substitute for legal counsel. The Guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein.

HTTPS://WWW.JUSTICE.GOV/CRIMINAL-CCIPS/FILE/872771/DOWNLOAD

How to Protect Your Networks fr

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 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 government and private industry best practices and mitigation strategies focused on the prevention

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 p
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)
- ctice managers and administrators
- bulatory surgery centers
- Medical device and life science companies

Oh Yes! IT'S FREE

Past Webinars
Publications

Most Popular Stories

7:34 AM
2/8/2017

HOLLAND&HART LLP

QUESTIONS?

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

Lisa M. Carlson
Office: (208) 383-3910
Cell: (208) 949-0845
lcarlson@hollandhart.com