Duke Medicine Security Awareness

July 2014
Chuck Kesler, MBA, CISSP, CISM
Chief Information Security Officer
Duke Medicine
Shelly Epps, MS
Information Security Analyst
Duke Medicine

DATA CLASSIFICATION: PUBLIC

The Information Security Tug-of-War...

Laws & Regulations
Business & Legal Risks
Strict Policies & Procedures
Reduced Revenues & Reimbursements
Higher Costs
Quick & Easy Access to Clinical Records
Research & Innovation
Engagement & Collaboration
Agility & Time to Market
Flexibility & Adaptability

DATA CLASSIFICATION: PUBLIC

Five Reasons Why Healthcare Workers Should Care About Information Security...

1. It's the right thing to do! Securing the personal data that we are entrusted with is part of our mission to "care for our patients, their loved ones, and each other."
2. It's the law! In fact, there are multiple laws that affect healthcare organizations: HIPAA, HITECH, Meaningful Use, FISMA, FERPA, etc...
3. Healthcare organizations are always under attack, and we all have a role in preventing those attacks from being successful.
4. Effective management of information security risks can help protect an organization's intellectual property, brand, and mission.
5. Planning for security will increase the likelihood of receiving research grants and contract funding.
What Motivates Cyber Criminals?

- Curiosity and recreation
  - Still a motivator for those looking to prove themselves
- Espionage
  - Sophisticated attacks against government, military, or industry targets
  - May be motivated by political or monetary gains
  - Goals may be theft of intellectual property or disruption of critical infrastructure
- Hacktivism
  - Want to call attention to their social or political causes
  - Often "anti-establishment" in nature
- Underground economy for stolen data
  - Cybercriminals have built a huge black market for developing malware, conducting Internet-scale operations, and laundering money
  - Medical records, SSNs, credit card numbers, and other PHI can be monetized on the black market; used by criminals for identity theft and financial fraud
The Black Market Value of Healthcare Data

- Healthcare organizations are a popular target... some examples:
  - Advocate Healthcare (IL): 4 million records (computer theft)
  - SCBS of NJ: 840,000 records (computer theft)
  - Utah Department of Health: 780,000 records (hacking)
  - AHMC Healthcare (IL): 759,000 records (hacking)
  - Emory Healthcare: 315,000 records (lost hard drives)
  - South Carolina Department of Health: 228,000 records (malicious insider)

- Medical records, SSNs, credit card numbers, and other PHI are highly valued on the black market
  - Studies have shown that individual medical record can fetch anywhere from $50 to over $1,000, vs. less than $1 for a credit card

What's Happening? Key Takeaways

- Hacking, stolen devices, and fraud are consistently the most frequent sources of data breaches
- External attacks represent a bigger threat than malicious insiders, but accidental disclosures by employees are a significant source of data breaches
- Healthcare and education sectors are highly targeted (averaging 1/3rd of reported breaches)
- Passwords and email addresses are being increasingly targeted, particularly through phishing
- Smartphones, tablets, and other mobile devices are expanding the potential for data loss events

What if an EHR System is Breached via a Phishing Attack?

- An attacker that acquires a valid username and password for a healthcare worker may be able to:
  - View and download medical records
  - Modify medical records
  - Write orders and prescriptions
  - Change billing
  - File false insurance claims
  - Conduct identity theft
Malicious vs. Legitimate Email Inbound to Duke, January – December 2013

![Graph showing the comparison between Malicious, Spam, and Valid email messages inbound to Duke in January - December 2013.](image)

Monthly Averages
Malicious: 99.1M
Spam: 5.0M
Valid: 17.7M

DATA CLASSIFICATION: PUBLIC

Phishing – Webmail Message

From: Duke.edu member service [mailto:phishpery@duke.edu]

Subject: Phishing – Webmail Message

You have One New Message!
e-mail.duke.edu

Contact Us About OIT Services, Duke University

More Phishing – URL Shorteners

From: Duke University

Subject: More Phishing – URL Shorteners

Dear Subscriber,

We are currently working on system maintenance.
As a precaution, we are requiring you to confirm your continued maintenance.
Update your activities with us now.

Click the link to view the following:
http://bit.ly/1jF6gR

This is a temporary measure. Failure to comply may result in Service suspension.

Thank you,
Duke University

© 2010 Duke University, Durham, NC 27708 | (919) 660-1211

DATA CLASSIFICATION: PUBLIC
Where Does that URL Shortener Link Go?

Tip: add a "+" after a bitly.com link to see where the link will take you.

<http://bitly-print.ru/....../DukeOnline.html>

DATA CLASSIFICATION: PUBLIC

More Phishing – Cryptolocker

DATA CLASSIFICATION: PUBLIC

More Phishing - Salaries stolen

DATA CLASSIFICATION: PUBLIC
HIPAA Penalties for Data Security and Privacy Breaches

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation ($)</th>
<th>All such violations in an identical provision per calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect - Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Average Cost (in $) of a Data Breach per Record by Industry

Source: Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis

REGULATORY LANDSCAPE
Laws that Affect Healthcare Organizations

• Federal Regulations
  – HIPAA Security & Privacy Rules
  – Final Omnibus Rule
  – HITECH Meaningful Use provisions
  – FISMA
  – 21 CFR Part 11 and other FDA regulations for clinical trials
  – FERPA for educational institutions

• Industry Regulations
  – The Joint Commission (JCAHO)
  – PCI Data Security Standard

• State-based Identity Theft Laws
  – 46 states have some form of data breach notifications law in place
  – Example: North Carolina Identity Theft Protection Act

Some Key HIPAA Considerations for Privacy and Security

• Establishing organizational authority for privacy and security
• Defining and protecting Protected Health Information (PHI)
• Logging and monitoring of access to PHI
• Managing Business Associate relationships
• Data breach responses and notifications

Key Points About PHI

• PHI must be encrypted when sent across a network
  – Exemption exists for carrier networks (e.g. AT&T, Verizon, Sprint, Time Warner), also referred to as “conduits”

• PHI must be encrypted if stored on a mobile device
  – Codified in Meaningful Use Stage 1
  – Safe Harbor: if an encrypted laptop with PHI is lost or stolen, it isn’t considered a breach; if it isn’t encrypted, then it is a breach

• PHI can be protected by de-identification or anonymization
  – Anonymization is the removal of all PHI elements
  – De-identification replaces elements of PHI with proxy values that can be tied back to the original value by a broker
  – De-identification technique must be statistically sound enough to prevent re-identification of the individual
Future Challenges for Information Security in Healthcare

What Can You Do?
SECURITY TIPS AND BEST PRACTICES

Secure System Usage Memo

Coming in FY15 – Duke Medicine Annual Security Awareness Training
• Initially for staff working on Federal contracts with FISMA requirements
• Rolled out to all DUHS staff by end of June 2015
What Can I Do? Staying Protected When Connected

At Work

And On the Go!

At Home

Understand Duke Data Classification Standard & Sensitive Electronic Information (SEI)

Duke has a three-tier Data Classification Standard to help identify the security requirements for how data should be handled:

\- **Sensitive**: information that Duke is required by law or regulation to protect, or otherwise protects to mitigate institutional risk. Explicit institutional approval is needed to access sensitive data.

\- **Restricted**: information that we want to protect but that would not significantly harm us if disclosed. Access to restricted data is determined by business process need.

\- **Public**: information that can be accessible to the general public.

**Sensitive Electronic Information**, or SEI, must always be protected with the tightest controls. Some examples of SEI include:

\- Protected Health Information
\- Social Security Numbers
\- Credit Card Numbers

Practice Good Password Management

Use strong passwords or passphrases

Use different passwords for different sites

Consider passphrases instead of traditional passwords

\- Example: “SassyRedHeels1776”

Set passcodes on your mobile devices

\- Usually enables the device’s encryption features

Use Multi-Factor Authentication (MFA) where available

\- MFA combines passwords (“something you know”) with at least one other piece of information: something you have, or something you are (e.g. biometrics)

\- Duke provides a free MFA tool called Duo


Never share your password!
Think Before You Click! Practice Safe Web Browsing & Email

Use skepticism when opening emails or web sites

That little padlock icon can make a huge difference
  • Look for https for secure transmission

Be familiar with the security and privacy settings on your web browser and email client
  • Web sites can track personal information and surfing habits
  • Cookies, cached pages, and history are all stored by your web browser and can potentially be accessed by web sites

Use social networking sites (e.g. Facebook, Twitter, LinkedIn, etc...) responsibly

Never send PHI or other sensitive information to personal email (e.g. Gmail, Yahoo) or cloud storage sites (e.g. Dropbox, etc...)

Protect Your Computers

Maintain up-to-date anti-virus (AV) software
  • Also install anti-virus on your home computers. Symantec AV software for home use is free to all Duke faculty, staff, and students
  • See: https://oit.duke.edu/comp-print/software/license/detail.php?id=199

Regularly apply security patches
  • Managed by your IT staff at work
  • On your personal systems, you should regularly patch your Operating Systems, web browsers, plugins, office applications and multimedia tools

Protect your screen
  • Use a password-protected screen lock when you’re not using your computer
  • Prevent your screen so others can’t view it

Configure and manage systems per IT standards and policies
  • At work, only install software that has been authorized by your IT department. On your personal systems, use caution when downloading software

Use a VPN (Virtual Private Network) to remotely access applications especially from vulnerable locations such as hotels, coffee shops, airports and conferences
Protect Your Mobile Devices

Encrypt all laptops and portable media that may contain sensitive information:
- Duke uses Symantec’s PGP product for encryption – contact your department’s IT support team for details.

Be familiar with and use the security settings on smartphones and tablets:
- Set a PIN or password
- Enable automatic locking of the device
- Use automated controls to remotely wipe the device, or wipe the device after excessive failed login attempts
- Do not jailbreak or otherwise tamper the device’s operating system! This bypasses basic security controls that can more easily allow malware to infect the device.

Know what you have stored on mobile devices – especially USB flash drives!

Keep sensitive data on a server – avoid making copies to a laptop or mobile devices.

Protect Data Storage, Transmission & Backup

- With the exception of receiving Duke Medicine email on personal devices, do not store PHI/SEI on non-Duke owned systems or devices.
- PHI/SEI on mobile devices or removable media must be encrypted per the Mobile Computing and Storage Device Standard.
- Clinical data may not be shared with vendors or other third parties unless there is a Business Associate Agreement (BAA) in place.
- Duke Medicine research data must be stored on Duke Medicine managed servers and locked file cabinets, unless outlined in an informed consent or a Data Agreement has been put in place to allow the third party to receive that data.

Did You Know?

Metadata can be hidden inside the digital layers of certain types of files. Even though it may not be obvious, if metadata contains PHI, it must be protected using the same standards.

Practice Good Physical Security

- The guy stood next to the door and said with a sheepish grin, “I forgot my ID, can you let me in?”
- Lock your workstation when away from your computer.
- Secure all portable devices (laptops, cell phones, USB/thumb drives, etc.) when not in use.
- Lock up documents that contain sensitive information. Don’t leave them at printers or fax machines unattended.
- When traveling, monitor your laptop as it passes through TSA security at the airport and promptly pick it up. Never place it in checked baggage.
- If you need to store your laptop in a car, lock it in trunk.
- Pay attention to people in your office area. Question or report a stranger’s presence or suspicious activity. Wear your Duke-issued ID badge when at work.
Promptly Report Security Incidents

Information security incidents include compromised systems, attacks made on or from Duke computers, illegal or inappropriate use, and abuse of computer privileges. For instance:
- Someone is using a computer without authorization.
- Your files appear to have been tampered with.
- Sensitive information has been disclosed.
- A Duke web page has been defaced.
- Your computer is acting strange.

Report security incidents to the Duke Medicine Service Desk as soon as possible.

If you have questions regarding information security policies, standards, guidelines, alerts, or other general questions, please contact the Duke Medicine Information Security Office (ISO).

Key Contact Information:
Duke Medicine Service Desk:
Phone: 919-684-2243
https://duke.service-now.com

Information Security Office (ISO):
Email: infosec@dm.duke.edu

Duke University Police:
Phone: 919-684-2444

Tips for Duke Medicine Researchers

Using ICF for authorization:
- Work with IRB and CRU/entity oversight.
- Clearly list all parties who will receive or access SEI (e.g., sponsor and contracted business partners).
- Avoid non-verified assurances (e.g., HIPAA compliant, secure, safe).
- Think through the potential risks and make sure they are clearly outlined.
- If you’re not sure, ask questions.

Research Data Security Plan:
- Work with your RDSP reviewers.
- IRB does not review the RDSP.
- All storage, both paper and electronic, must be accurately listed in the RDSP and updated as changes are made.
- If you’re not sure whether/how to list something, ask questions.

Mobile Devices:
- All mobile devices that will be given to study participants, particularly those that will be taken home during the course of the study, should be securely configured by authorized IT staff.
- Devices should be securely wiped between use for different participants.

Sponsor Devices:
- All sponsor devices must be reviewed by authorized IT staff and must meet the same requirements as Duke property prior to collecting data or connecting to the Duke network.

Thank You!

Chuck Kesler
Chief Information Security Officer
Duke Medicine
Email: chuck.kesler@duke.edu
Twitter: @chuck_kesler

Shelly Clark Epps
Information Security Analyst
Duke Medicine
Email: shelly.clark@duke.edu