Securing Confidential Patient Information

Is Your Medical Practice Safe from PHI Theft?

In addition to caring for patients, your practice is responsible for ensuring the confidentiality of patients' health and financial information. Unfortunately, data breaches are an ever-increasing danger—and present additional liability risk.

The numbers speak for themselves. The U.S. Department of Health and Human Services (HHS) aggregates reports of major breaches (affecting 500 people or more); it has logged 944 incidents affecting the personal information of about 30.1 million people from 2009 to 2013. A Washington Post analysis of HSS data cited the following causes and number of people affected:

- Theft – 17.4 million people;
- Data loss – 7.2 million people;
- Hacking – 3.6 million people; and
- Unauthorized access to accounts – 1.9 million people[i]

Healthcare organizations are frequent targets of cyber attacks—accounting for 48.8% of all cyber breaches in 2013 (up from 34.5% in 2012).[ii] 2014 numbers will likely show a steep increase, as well, including the high-profile hacking of Anthem, Inc. BlueCross BlueShield.

What is Legally Required?

HHS, under the Health Insurance Portability and Accountability Act (HIPAA), requires covered entities (CE) comply with privacy and security standards when dealing with protected health information (PHI). These standards were introduced to protect the privacy, confidentiality, security, integrity, and availability of PHI.

The HHS defines PHI as "individually identifiable health information," oral or recorded in any form (including electronic), that is:

- maintained, transmitted, or stored by a CE; and
- relates to an individual's past, present, or future physical or mental health or condition.[iii]

HIPAA requires that CEs conduct a risk assessment to address cyber vulnerabilities as well as health data breaches and other adverse security events. A comprehensive step-by-step approach is important when implementing processes to protect PHI and mitigate exposure caused by unauthorized use and/or disclosure of electronic PHI.

HIPAA/Cyber Liability Checklist

Use our five-step checklist to help your practice analyze and address cyber risks:

☐ **1. Select a team that will ensure the expertise needed to perform a risk assessment.**
If your practice is smaller-sized: HIPAA requires every CE to designate one person (the Privacy Officer) to be responsible for PHI privacy and security. Often the office administrator is the designated Privacy Officer. The "team" may be the Privacy Officer and one other person. Optimally, these people should be knowledgeable about the type of data stored, location of that data, and data breach reporting requirements. If the team is not well versed in data security issues and threats, an outside information technology firm may be necessary.

☐ **2. Identify all sources of electronic PHI (ePHI), including:**
Devices

- ☐ Computers
- ☐ Laptops
- ☐ Servers
- ☐ External Storage Arrays (e.g., additional storage to server)
- ☐ Network-Attached-Storage (NAS) devices
- ☐ Cell Phones
- ☐ Smartphones (e.g., iPhone, Droid, etc.)
- ☐ Cameras
- ☐ Voicemail recordings
- ☐ Routers
- ☐ Video surveillance system
- ☐ Tablets (e.g., iPad)
- ☐ Reader devices (e.g., Kindle)
- ☐ Music players (e.g., iPod, mp3 player, etc.)
- ☐ Digital copy machines
- ☐ Scanner with storage drive
- ☐ Fax machines
- ☐ Phones (e.g., if phone numbers are logged)
- ☐ Medical devices with local storage (e.g., ultrasound machine, MRI machine, etc.)
- ☐ Any other device that may store or allow access to ePHI

Offline Media

- ☐ Compact discs (CD-ROMs, such as copies of radiographs)
- ☐ DVDs
- ☐ Thumb drives (a.k.a. flash drives)
- ☐ External hard drives such as USB, eSATA or Firewire
- ☐ Backup tapes
- ☐ SAN disks (e.g., storage for cameras)
- ☐ Memory sticks
- ☐ Smart cards (used for secure log-in in some organizations)

- ☐ Encryption keycards
- ☐ Door keycards
- ☐ Floppy/Iomega disks
- ☐ Hard drives (e.g., secondary backup drives or stored hard drives from old computers)
- ☐ Any other external media type

Off-site Services

- ☐ Off-site backup services
- ☐ Off-site hosted services (e.g., Google Apps, "Cloud computing," Yahoo email, Microsoft hosted exchange, ultrasound storage off-site, etc.)
- ☐ Websites
- ☐ File Transfer Protocol (FTP) sites
- ☐ Email spam filtering services
- ☐ Web filtering services
- ☐ Any other off-site service that may be relevant

Data in Transmission

- ☐ Internal email
- ☐ External email
- ☐ FTP
- ☐ Web traffic
- ☐ File-sharing programs (e.g., Web DAV, Limewire, Napster, LAN-based work stations/servers)
- ☐ SQL or other database traffic
- ☐ Any other type of data transmission

Remote Access

- ☐ Webmail
- ☐ POP3 email
- ☐ IMAP email 3
- ☐ Outlook email
- ☐ ActiveSync email syncing to a phone
- ☐ Remote desktop
- ☐ Terminal server
- ☐ VPN
- ☐ Go-to-My PC
- ☐ LogMeIn
- ☐ Team Viewer
- ☐ PC Anywhere
- ☐ VNC
- ☐ Web Portal
- ☐ Any other type of remote access

☐ **3. Identify all methods of communicating ePHI, such as:**

- ☐ FAX transmissions
- ☐ Emailing
- ☐ Internet
- ☐ Text messaging
- ☐ Instant messaging

☐ **4. Develop a Risk Assessment Matrix to include:**

- ☐ *Source* – Identify each source of confidential information (e.g., electronic PHI) in your organization and each method used to transmit this information to others.
- ☐ *Risk* – Identify each risk for the delineated HIPAA Standard of Implementation Specification; "risk" means what can happen.
- ☐ Vulnerability – Identify a vulnerability specific to the risk identified; "vulnerability" means how a risk can happen.
- ☐ *Threat* – Document any threat specific to the risk identified; "threat" means who can cause the risk to happen.
- ☐ *Actor* – Document whether the actor who could carry out the threat is inside or outside of your organization.
- ☐ *Access* – Document whether the risk is via a computer network or is an actual physical threat.
- ☐ *Likelihood* – Document the probability of the identified risk actually occurring (e.g., score 1, 2, or 3 with 3 indicating the highest probability).
- ☐ *Severity* – Document the severity of what would occur if the identified risk is carried out. Score as explained above.
- ☐ *Risk Score* – Determine the calculated risk score by multiplying the Likelihood Score by the Severity Score. Your result will be between one and nine, with nine being the most significant risk.
- ☐ *Comments* – Document any unique considerations or issues for increased awareness around each risk.

A sample Risk Assessment Matrix is provided on page five.

Sample Risk Assessment Matrix[iv]

	A	B	C	D	E	F	G	H	I	J	K
1	Source, Location and Risk				Threat			Risk Score			
2	Source of PHI	Location of Source	Risk (What could happen)	Vulnerability (How the risk could occur)	Threat (Who causes the problem. e.g. User; Hacker; Technology failure; users of mobile devices; etc)	Actor (Internal or external or both)	Access method (Network access; Physical access; etc.)	Likelihood (L/M/H) (1/2/3)	Severity (L/M/H) (1/2/3)	Risk Score Probability X Impact 1 - 9	Comments
3											
4	Old PCs for disposal	all areas	Unauthorized access to PHI stored on the hard drive	PCs with PHI stored on the hard drive could be disposed in the general trash bins; anyone who retrieves the PCs would have access to the information on the hard drive(s)	Workforce members who throw PCs away; public (who may dumpster dive)	Internal and external	Physical (an employee physically throws the PC away	2	3	6	This is just a sample for the purposes of discussion
5											
6											
7											
8											
9											
10											

☐ **5. Train staff**

- ☐ Train all staff on how to avoid, detect, and report cyber-incidents.
- ☐ Include information specific to security risks and vulnerabilities identified in your risk assessment.
- ☐ Conduct training annually or more often, as indicated.
- ☐ Document training content, date conducted, and staff who participated.

Resources

Additional information for medical practice security is available from the Office of the National Coordinator for Health Information Technology (ONC) at:
http://www.healthit.gov/sites/default/files/small-practice-security-guide-1.pdf

You also can contact a ProAssurance Risk Resource advisor for assistance with your risk questions and concerns. Call toll free 844.223.9648 or email RiskAdvisor@ProAssurance.com.

---

[i] http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/

[ii] Identity Theft Resource Center, http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachStatsReport.pdf

[iii] 45 CFR § 160.103

[iv] http://proassurance.nas-cyber.com/cms/client/(S(gt0el045kj35tu45nmw4l345))/Client.aspx?command=display&page=ds160&parm=&file=&SstateID=68&Sstate=Texas