HIPAA COMMUNICATION

Prevent Your Mobile Devices From Causing A HIPAA Violation

Dexcomm
ANSWERING AND COMMUNICATIONS SERVICES
YOUR VOICE. HEARD.

Thank you for joining us for our brief introduction to HIPAA and mobile devices. As a telephone answering service serving hundreds of medical clients in many different states, we have developed strategies and skills which allow us to comply with HIPAA and to expertly serve our diverse clientele. This e-book is our effort to share our experience with you and allow your office to quickly and easily become HIPAA compliant without undergoing the extensive research and expense we experienced. In doing research for this project, we came across two alarming facts: Approximately 80% of physicians use mobile devices to access Protected Health Information (PHI); only 40% of physicians place a mid-level priority on the security of their systems and only 24% say it is a top priority. The reality is that physicians are using mobile devices more every day and many of the devices lack even the most basic security measures. Following a few simple steps suggested here and practicing your own due diligence can certainly save some heartache in the future.

Thanks for listening,

Jamey Hopper

INSIDE THIS ISSUE:

HIPAA, Medical Offices and Mobile Devices 4

Legislation 6

Note Board 9

How Do I Protect Mobile Devices 10

Tool Box & Checklist 11

Our Dedication To You 12

Appendices 13

Meet the Experts

You are invited to "ASK THE EXPERT" found in the bottom right-hand corner of each section.

JAMEY HOPPER
President

STEFFY RITTER
Business Manager

DANA LEWIS
Training Supervisor

KYLE DUHON
Systems Engineer

KARL SCHOTT
Operations Supervisor

HIPAA, Medical Offices and Mobile Devices

The amount of Protected Health Information (PHI) that could be on your employee's phone is staggering. Access to the protected information can be as easy as unlocking a smart phone. Mobile devices collect and contain PHI such as a patient's name and phone number or a picture of a patient's wound while they were in the office for a routine visit.

Are you prepared for a situation as simple as a member of your staff answering a call on their cell phone? Who has access to this information? What if when the employee is at home, their teenage daughter is playing with the mobile device and sees a text message that contains PHI? You now have a HIPAA violation. There is even the possibility that the daughter sees a name she recognizes and places the information on Facebook, Twitter or any other social media site.

You will find a downloadable Mobile Device Policy that you can customize to your office's needs in the Toolbox Section.

Here are just a few questions that you may want to...

ask your staff | think about | discuss

Are your employees aware of the different settings within their phones for text messages?
There are settings which will allow only a number or a name of the person texting to be visible.

Is your smart phone password protected?

With the production of newer and more "tech savvy" smart phones which now have the capability of reading aloud an incoming text message, what procedures does your office have in place from preventing persons not privy to that information from hearing these text messages?

When your office experiences a turnover in staff, are the proper procedures being followed with updates and removals of old information with new information to prevent the release of PHI to the wrong person?

Are you documenting a patient's history, such as wounds, with your camera phone? How is this patient's EPHI protected on your phone to avoid violating HIPAA regulations?

Are you a home health or hospice agency providing medical services within the homes of patients? Do your nurses answer their cell phones within the patient's home? Are they removing themselves from the current patient's home to avoid HIPAA violation when taking a message regarding another patient?

Health Insurance Portability and Accountability Act

The guidance that started as an attempt for consumers to keep their health information private and make their insurance portable has become a large legislative issue. Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 and updated in 2000, 2002, 2003, 2004, 2005 and 2006! While there are many aspects that we can discuss about HIPAA, we are going to focus on the specific legislation as it relates to mobile devices.

Congress realized that the advancements in technology called for additional legislation to protect the privacy of an individual's health information known as Protected Health Information (PHI). The Privacy Rule sets standards to protect PHI transmitted electronically by three covered entities; health plans, healthcare clearing houses and healthcare providers. The Security Rule sets standards for protecting the confidentiality, integrity and availability of all electronic PHI created, received, maintained or transmitted. The Office for Civil Rights oversees and enforces the Privacy Rule and the Security Rule.

So what is protected under the Privacy Rule?

Electronic Protected Health Information (EPHI) is any "individually identifiable health information maintained in electronic media or transmitted or maintained in any other form or medium". As you can imagine, this could include everything from a patient's name to private medical history. Basically, anything that would identify someone. Any number of pieces of EPHI could be on a mobile device in order for a physician to serve his or her patient. Due to sensitivity of the information, it **must** be secured.

Case Study

A healthcare system that services Massachusetts had to send 384 letters notifying patients that a home health nurse's PDA was missing. The mobile device contained patients' personal information which included social security numbers and health insurance information. The primary use of the PDA was to document care while the nurse visited with patients. Each nurse's PDA is connected to the healthcare's system, which updates the electronic medical records at the end of the day.

The nurse reported the loss of the PDA immediately, but the report did not reach the compliance officer for several weeks due to a "lapse of communication."

The mobile device was not encrypted but did require a password. Reportedly, the healthcare system would not discount a hacker's ability to get past the password. They offered the patients a "security freeze" on their credit reports, and conducted in-house training on HIPAA security with all their staff.

Security Rule

Methods of protection are broken down into three categories of safeguards; administrative, physical and technical.

ADMINISTRATIVE SAFEGUARDS

The covered entity must identify and analyze potential risks and implement security measures that reduce those risks and vulnerabilities to a reasonable and appropriate level.

PHYSICAL SAFEGUARDS

Implement policies and procedures regarding the transfer, disposal and reuse of electronic media. When your staff members receive a new mobile device, the old one that contains PHI stored on it must be disposed of properly. Ensure that disposed office machinery, such as fax machines, do not contain retrievable PHI.

TECHNICAL SAFEGUARDS

This section deals with access control and encryption to make sure that only those authorized view PHI and that transmission of data is secure.

Have you trained your staff on the proper way to secure their mobile device according to your policy?

How many records are stored on the device?

Do your mobile devices all have passwords and are the passwords changed frequently?

Is the data encrypted on their mobile devices?

Where is the mobile device kept if it is not being used?

Does anyone in your office frequently take their mobile device home with them?

So what does that really mean?

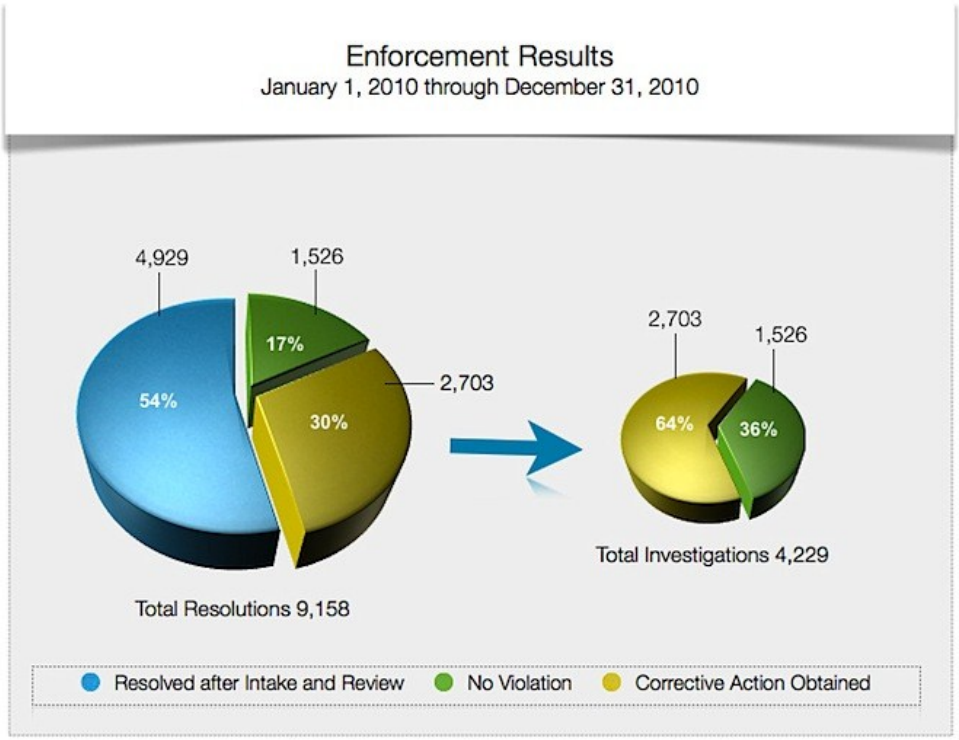
It means that all PHI that is stored in any format must be protected and staff must be trained with all of your procedures that accomplish said protection.

DeXcomm

Health Information Technology for Economic and Clinical Health Act, 2009

The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law as part of the American Recovery and Reinvestment (ARRA) Act of 2009. The main focus of HITECH was to encourage the use of health information technology.

Several changes were made with this legislation, including that business associates are now subject to the same requirements as covered entities. Not only do you have to comply with all of the HIPAA rules but now your answering service, CPA, attorney, and other professional service organizations that may see PHI also have to comply. Penalties have increased and are now being levied. Fines range from $100 in a "did not know" offense to $1,500,000 for "willful neglect". If **a breach does happen that contains over 500 records, the media must be notified.** Finally, each State Attorney General may now prosecute separately from the Department of Health and Hospitals Secretary (HHS), making fines a serious issue in the event of a breach.



Enforcement Results. January 1, 2010 through December 31, 2010. Accessed 15 Feb. 2012. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html>

So what does this really mean?

Given all of the above legislation and the large number of mobile devices on the market and in our businesses today, it has become difficult for physician offices and their business associates to manage all of the devices. Everything from a USB flash drive to an electronic tablet or even a camera phone has become a potential source of a PHI breach. It is important that you craft a mobile device policy that allows you to reasonably meet all of the rules. Administering this policy and knowing that you have done what the law requires will allow you a better night's sleep.

Case Study

December 11, 2007. Dr. Adam Hansen, Chief Resident of General Surgery at the Mayo Clinic Phoenix Hospital, admitted taking inappropriate photos of a patient, who was under anesthesia during an operation, and showing the pictures to his colleagues. The doctor is no longer employed with Mayo and the patient contacted his attorney.

NOTE BOARD

Common uses for mobile devices in a clinical setting:

*Patient database
*Contact information
*Test results
*Surgery schedules
*Procedure lists
*Prescriptions

Case Study

Mobile devices are not only used to input information, but they can also be used maliciously with the digital camera found in the cell phone. Rady Children's Hospital in San Diego, CA forbade employees from carrying cell phones after investigators found photos of children on a respiratory therapist's computer and cell phone. The therapist had been molesting many of the severely disabled children while under his care. The therapist later pleaded guilty to child molestation and pornography and was sentenced to 45 years in prison.

Note:

Transmitting text messages without encryption that has private health information is as easy as two doctors texting each other to follow up on the previous days patients. One doctor might text, "What happened with that critical patient last night." The other doctor might respond, "She was diagnosed with an infection, admitted to the hospital, room 214."

For the spying eyes in a crowded elevator, they would have all the identifiable information for that patient including the gender, the diagnosis, and the room the patient was located to cause a breach in HIPAA.

The Office of Civil Rights (OCR) will notify a covered entity of a Failure to Comply and provide them the opportunity to produce written evidence of above circumstances that would reduce or bar a penalty.

How Do I Protect Mobile Devices...

There are three safeguards to protect your mobile devices that are used to access or store EPHI under the responsibility of a HIPAA compliant entity utilizing HIPAA's Security Rule.

Administrative Safeguards

Start by taking an inventory of all of the devices within your practice that are used to access and/or store EPHI. We recommend including what the device is intended for in regards to use/access to EPHI. To take this up a level, include the operating system the device is using. Remember your inventory will need regular updating depending on changes in employment and system updates. Tip: Set reminders in your calendar.

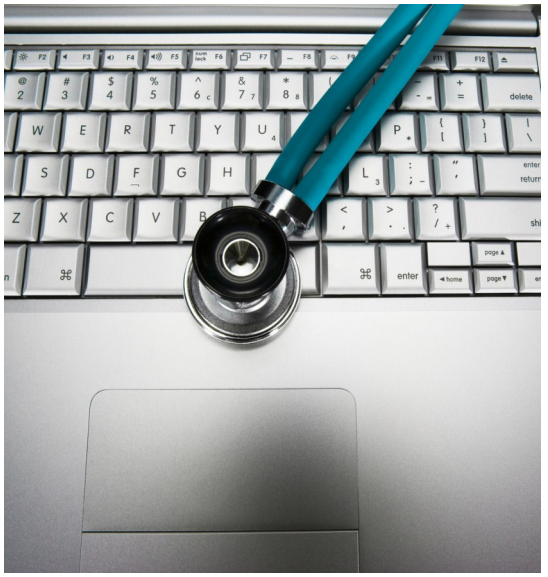
Review your practice's policies to make sure they encompass mobile devices. Training and enforcement is, as always, the key to your practice's success.

Physical Safeguards

Just like anything you want to protect, keep it in a safe location. Ensure that all devices are never left unattended, and are locked in a drawer or in an office when not in use. When outside of your office, make sure the device is either always with the person responsible for it or in a secure location such as a glove box or car trunk. It only takes a second for someone to grab such a small item. Remember that if the item is lost or stolen, report it immediately!

Technical Safeguards

If the electronic PHI is stored and transmitted in encrypted form, then you do not need to notify patients if there is a security breach. Any data can be encrypted. Encryption is a process that converts plain text into cipher text that is unreadable to any unintended entity who has accessed the file without "permission." It works by using a mathematical algorithm called keys that code and decode the cipher text. This process is performed by computer programs or specific hardware designed for this purpose.



HHS states that any HIPAA compliant entity is not exempt from the breach notification requirements if the entity keeps the keys on the same device as the encrypted data. Ask your vendor before selecting your encryption product. Keys can be stored on a USB flash drive, a key server or be regenerated as needed. For more information visit HIPAA Security Rule FAQ Regarding Encryption. On your computer, programs such as Microsoft® Encrypting File System (EFS) are built-in encryption programs that are easy to use by just changing the properties of the folder. Click here for a full list of programs.

The same protection extends to your mobile devices, which should also be password protected. Change your passwords at least every 90 days. Any EPHI that is utilized or stored on a mobile device must also be encrypted. This includes accessing a web portal on the mobile devices web browser, SMS/text message, email or images.

Don't forget

Other mobile devices items like USB flash drives, memory/smart cards, CDs, DVDs, PDAs, remote access devices and security hardware.

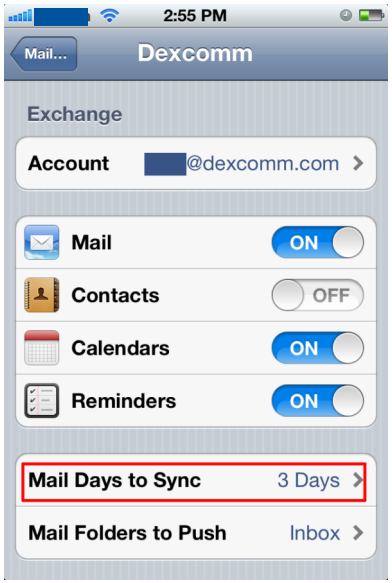
Tool Box

- Mobile Security Tool Kit
- Password Locks
- HIPAA Security Guidance
- What is a Covered Entity
- Mobile Device Policy
- Inventory Forms

Checklist

- ☐ **Ability** to enable auto password lock after __ minutes
- ☐ **Ability** to remotely wipe mobile device if device is stolen or lost
- ☐ **Ability** to log visits each time a mobile device connects to your network
- ☐ **Ability** to perform surprise security checks
- ☐ **Inventory** of all mobile devices – *You need to know what you have in order to protect what you have*
- ☐ **Policy** Password locks on mobile devices
- ☐ **Policy** to install available software updates to mobile devices
- ☐ **Policy** to restrict the number of emails stored on the mobile device *(Example: only keep 3 days of email)*
- ☐ **Policy** to only install approved software on device
- ☐ **Policy** to change password on mobile device every 90 days
- ☐ **Policy** to review logs every __ days/months
- ☐ **Policy** to report when a device is lost or stolen ASAP
- ☐ **Policy** to report any data breach ASAP
- ☐ **Policy** to only backup mobile device on approved/secure computer
- ☐ **Policy** Bluetooth should only be used for passive devices *(Example: hands free kits)*
- ☐ **Policy** to restrict use of mobile device while driving

Mobile Solutions



PROGRAMMING Mobile devices can have programming installed that encrypts EPHI that is used or stored on it. Certain programming applications can record real-time messages for your practice's records, and groups the messages by threads. Features may also include remote disabling if the mobile device is lost or stolen.

NETWORK FILTERS Network Access Control (NAC) are filters deployed on network routers that make IT installed programs contingent upon use. If you think a tech-savvy staff member may try to remove or hack the programming from their phone, the filter would not allow access to your network.

Our Dedication To You

We've given tools and education based on years of serving clients like you. When deciding which business associate fits your needs, we recommend a partner that has dedicated time and resources to protect you and your business.

One of the ways we dedicate time and resources into our partnerships with our clients and friends is through our staff and their development.

Our Hiring Process

All new hires are put through an extensive application process involving several interviews with multiple company executives, background checks, drug screening and are required to sign a confidentiality agreement. This is to ensure that potential employees exemplify our core values, fit within our company culture and have the skills needed to serve our customers.

Our Training Process

Upon hire, we enter them into an extensive classroom based training setting where they are educated under the supervision of a dedicated and experienced training department on our operating system and our focus on customer service.

The training department has outlined eight levels of education. Each level has specialized training dependent upon the complexity of the accounts. Operators improve by advancing through the different levels of education by completing training and testing. They receive one-on-one training that is on going throughout their time employed at Dexcomm. The highest operator level to achieve is focused on our medical related fields.

Since 1989, before HIPAA was implemented, Dexcomm focused on and conducted confidentiality training because of our long history and understanding of the medical community. Starting in 2003, operators were introduced to two subject matter experts (SMEs); one with a registered nurse (RN) who has over 25 years of experience and an attorney who is specialized in HIPAA regulations. The RN explains in detail what to expect when speaking with doctors, other nurses and various health-care providers. The attorney educates the operators on HIPAA rules and regulations. Our operators are then given a written test on both SMEs seminars.

Once the initial training program is completed, their education is not over; operators are moved into advanced training. In this ongoing phase, they attend monthly in-services and are consistently monitored and evaluated by a large team of managers. The Training Department, who oversees this process, ensures HIPAA compliance, maintains our high-level of customer service and enforces quality control.

Your Voice. Heard.

Please let us know if we can provide you with any additional information such as other e-books, white pages or our services.

Appendices

Acronyms

ANSI – American National Standards Institute

ARRA – American Recovery and Reinvestment Act of 2009

CMS – Centers for Medicare & Medicaid Services within the Department of Health and Human Services.

EFS – Electronic Filing System

EPHI – Electronic Protected Health Information

HIPAA – Health Insurance Portability and Accountability Act

HITECH – The Health Information Technology for Economic and Clinical Health Act

HHS – U.S. Department of Health and Human Services

NAC – Network Access Control

PDA – Personal Digital Assistant also known as a personal data assistant, is a mobile device that functions as a personal information manager.

PHI – Protected Health Information

Glossary

Access. the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. 45 C.F.R. §164.304 Definitions

Access Control Standard. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. 45 C.F.R. § 164.308(a)(4)[Information Access Management].

1. Unique User Identification (Required)

2. Emergency Access Procedure (Required)

3. Automatic Logoff (Addressable)

4. Encryption and Decryption (Addressable)

Addressable. Implementation specification is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so. 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306 (d)(3)

Administrative safeguards. Administrative actions, and policies and procedures, to man age the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. 45 C.F.R. §164.304 Definitions

Breach. The acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. 45 C.F.R.§ 164.402 Definitions.

(1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Covered Entity. The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is:

a) a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider")

b) a health care clearing house

c) a health plan

Encryption. A method of converting an original message of regular text into encoded text. http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2021.html

HITECH. The Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology.

Keys. Also known as encryption key, algorithms that transfer the data into streams or blocks of seemingly random alphanumeric characters. An encryption key might encrypt, decrypt, or perform both functions, depending on the type of encryption software being used. WiseGEEK.com

Programming. Designed to perform a specific function directly for the user or, in some cases, for another application program. [Examples of application programs include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs. Application programs use the services of the computer's operating system and other supporting programs.] Techtarget.com/definition

Protected Health Information. Individually identifiable health information:

(1) Except as provided in paragraph

(2) of this definition, that is:

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information in:

(i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

(ii) Records described at 20 U.S.C. 1232g (a)(4)(B)(iv); and

(iii) Employment records held by a covered entity in its role as employer.

Physical safeguards. Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. 45 C.F.R.§164.304

Privacy Rule. Requires a covered entity to have written policies and procedures as necessary to implement the privacy standards in the Rule and to train workforce members on those policies and procedures, as necessary and appropriate for the workforce members to perform their functions. 45 C.F.R. § 164.530(b)

Reasonable cause. Means circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated. 45 C.F.R. §160.401

Security Rule. Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. 45 C.F.R. §160

Technical safeguards. The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. 45C.F.R. §164.304

Willful neglect. Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. 45 C.F.R.§160.401

Works Cited

Dearing, Dan . "Five steps to securing mobile data for HIPAA compliance." SC Magazine. 1 Jul. 2008. 13 Feb. 2012. <http://www.scmagazine.com/five-steps-to-securing-mobile-data-for-hipaa-compliance/article/112019/>. Dolan, Pamela L. "Data security breaches often triggered by carelessness." amednews.com. 22 Feb. 2010. 30 Jan. 2012. <http://www.ama-assn.org/amednews/2010/02/22/bil20222.htm>.

Dolan, Pamela L. "Smartphones blamed for increasing risk of health data breaches." amednews.com. 19 Dec. 2011. 30 Jan. 2012. <www.ama- assn.org/amednews/2011/12/19/bil21219.htm>. Dolan, Pamela L. "Health care's top 2012 issues: technology, social media, security." amednews.com. 13 Dec. 2011.<www.ama-assn.org/amednews/2011/12/12/bisd1213.htm>.

Dolan, Pamela L. "Physician texting provides quick communication – and an easy way to violate HIPAA." amednews.com. 31 Oct. 2011. 30 Jan. 2012. <http://www.ama-assn.org/amednews/2011/10/31/bica1031.htm>. Eckelbecker, Lisa . "Health data Missing." Telegram.com. 9 2008. 8 Feb. 2012. <http://www.telegram.com/article/20080419/NEWS/804190436/1116>.

"Guidance on Risk Analysis Requirements Under the HIPAA Security Rule." US Department of Health & Human Services. 14 Jul. 2010.<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf>.

"HIPAA And Security Breaches: Most Frequent Issues and Causes, and Trends for Future Threats." Bay Bio: Northern California's Life Science Association. 3 Aug. 2011. 20 Feb. 2012. <http://www.baybio.org/events/details/hipaa-security-breaches-most-frequent-issues-causes-trends-future-threats/>.

"HIPAA Email Encryption Requirements." HIPAA Email Compliance. 13 Feb. 2012. <http://hipaaemailcompliance.org/hipaa-email-encryption-requirements/>. "HIPAA Security Guidance." LogRhythm.com. 28 Dec. 2006.<http://www.logrhythm.com/LinkClick.aspx?fileticket=TXoFif%2B0MOU%3D&tabid=113>.

"HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information." American Medical Association. 2010.<http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf>. "HIPAA Security Series - 4 Security Standards: Technical Safeguards." US Department of Health & Human Services. May. 2005.<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf>. "HITECH Requires a Health Check on Data Protection." Toughbloggers.com. 3 Feb. 2011. 2 2012. <http://www.toughbloggers.com/2011/02/03/hitech-requires-a-health-check-on-data-protection/>.

"Health Information Privacy: Summary of the HIPAA Privacy Rule." U.S. Department of Health & Human Services. 15 Feb. 2012. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html>. Kissel, Richard . "NIST Special Publication: 800-88: Guidelines for Media Sanitization." National Institute of Standards & Technology. Sep. 2006>.

Leyden, John . "Lost mobiles to pile up in taxis in run up to Xmas." The register. 30 Nov. 2009. 7 Feb. 2012. <http://www.theregister.co.uk/2009/11/30/taxi_lost_kit_survey>.

Markus, Patricia A. "Cell Phone Camera Use in Healthcare Facilities: Shutter It." Smith Moore Leatherwood. 29 Jan. 2009.<http://www.smithmoorelaw.com/files/Publication/0b479c5a-08e8-4754-bff6-487214574a66/ Presentation/PublicationAttachment/6cd8d168-6601-4464-b3eb-4a2d1e16dfee/20090129-hitnews-markuszuiker.pdf>.

McGee, Marianne K. "How Secure Are Your Clinicians' Moblie Devices? ." Information Week. 16 Nov. 2011. 8 Feb. 2012. <http://www.informationweek.com/news/healthcare/mobilewireless/231903089>. Ralph, Chris . "Risk Analysis for HIPAA Compliancy." SANS. 6 Jan. 2005.<http://www.sans.org/reading_room/whitepapers/hipaa/risk-analysis-hipaa-compliancy_1554>.

"Tattooed privates prove not so private." PogoWasRight.org. 10 Dec. 2007. 8 Feb. 2012. <news.yahoo.com/s/ap/20071220/ap_on_fe_st/odd_tattoo_photo;_ylt=A0WTUe8ybWpH7CEB6iIDW7oF.>

"What does "willful neglect" mean under HITECH/HIPAA?." LawtechTV.com. 7 Jul. 2009. <http://www.lawtechtv.com/home/2009/07/what-does-willful-neglect-mean-underhitechhipaa.html>.