# Is Your Patient Health Care Data Secure? Take These Four Checklist Tests And Be Sure!

| Entity | Violation | Fine, Jail Time |
|---|---|---|
| HIPAA Civil Penalties | HIPAA unknowingly violated | $100-$50,000 |
| | Due to reasonable cause, not due to willful neglect | $1,000-$50,000 |
| | Due to willful neglect, corrected within 30 days of notice | $10,000-$50,000 |
| HIPAA Criminal Penalties | Violation due to willful neglect, not corrected within 30 days of notice | $50,000, 1 year jail |
| | Violation committed through deception | $100,000, 5 years jail |
| | Sale or transfer of health information for profit or any personal gain or intent to harm | $250,000, 10 years jail |
| CA State Laws | Apply to individuals as well as health care providers and business associates | Up to $250,000, 10 years jail |

## Originally published in the Newsletter of Physicians Reimbursement Fund, Inc.

Originally published in the Newsletter of Physicians Reimbursement Fund, Inc.

By: Margaret S. Leonard

Does your practice use electronic health records? Do you rely on interactive websites or online portals where patients can enter their personal demographic and billing information? Do you utilize third party billing services? All of the above questions are important, and if you answered “yes” to any of them, it’s time to ask yourself one more question: Just how well is my patient data being protected? If you aren’t worried yet, you probably should be, because the risk of a security breach is high (and growing), and the potential penalties to you and your practice include extremely punitive fines, civil litigation, and even imprisonment.

One in 10 Americans has been affected by a large health data breach, according to the U.S. Department of Health and Human Services. If you think this could never happen to your practice, consider that one out of five health care organizations experienced a security breach in 2013. Additionally, health care data breaches accounted for 44 percent of all breaches in the same year, making 2013 the first time the health care sector has topped this list. Employee negligence, computer malware and viruses, digital intrusion/theft, and physical intrusion/theft were the

© 2012-2021 Freed Associates, Inc. 

most common causes of these breaches.

Federal and state fines for a single disclosure of a patient's protected personal health information could reach as high as $1.5 million, although this amount may fluctuate depending on the nature of the breach. However, that number doesn't even take into account legal fees, credit monitoring fees, IT recovery fees, or costs associated with reputation damage, meaning the total amount may be much higher.

Consider the potential financial impact to your medical office practice as summarized in the table below.

As you begin thinking about the protection of your patient data protection within your office, there are four specific areas of your practice to consider for HIPAA compliance and data security:

• IT security and risk considerations

• Electronic Health Record (EHR) system security

• HIPAA-related office policies and procedures

• Business associate (BA) agreements

**IT Security and Risk Considerations**

Reviewing your hardware and software infrastructure (servers, personal computers, and internet virus protection) is a key component of an office security and risk assessment. Below is a quick checklist for review:

• Is your hardware/software supported by a professional IT management company?

• Does this support include computer/server installation, data backup, system access logs, intrusion detection monitoring, and software updates including antivirus protection?

• Are your local computer/servers located in secure, locked locations?

• Is your office computer hardware susceptible to theft during office hours or after office hours?

• Beyond having an alarm system for after-hours security, does the staff provide continuous visual security for office systems during business hours?

• Do your office computers require security passwords?

• Is each computer and server password protected?

• Are your computer passwords viewable by visitors?

• Are the files and hard drives on your office computer desktops encrypted?

© 2012-2021 Freed Associates, Inc. 

• Are your office servers protected from accidental activation of fire suppression systems?

• Does your office local server provide a single point of data backup? (If so consider offsite data backup.)

• Is your office email secure (encrypted) when sending Personal Health Information (PHI)?

• Does your email provider provide encryption capability for transmission of patient PHI?

• Is your staff adequately trained in encryption procedures?

• Does your employee handbook indicate that all PHI sent via email will be encrypted?

• Does your office have a procedure to monitor that policies and procedures are followed?

• If your office website allows patients to enter their information or provide billing information, is that information encrypted?

**EHR Security**

Electronic Health Record system security considerations are frequently overlooked during implementation in an office practice. Here is a best practices checklist of specific EHR office policies and procedures for your office:

• Does your office have defined and monitored EHR access? Clinical patient information and billing information are prime considerations for access by office staff. Unauthorized access means inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use.

• Are procedures in place for routine auditing of EHR access logs? Routine monitoring of EHR access logs is required to insure that PHI is appropriately accessed by staff.

• Are consequences for unapproved access to PHI described? Informing office staff at the start of employment and during routine performance reviews of office policy regarding PHI access is a best practice.

• Is there an office policy and procedure addressing both planned and unplanned termination of staff system access? Often system access is controlled by an offsite IT vendor. Prompt notification of staff termination (planned and unplanned) is critical to protection of office PHI.

• Does your office provide security for office computers and computer access?

• Are computers and office servers secured (locked doors) during non-office hours, and is access monitored by staff during working hours of the office?

• Is there a policy and procedure addressing system passwords (format, password change policy, password security)? An office policy requiring password changes often meets resistance by office staff but is a best practice

© 2012-2021 Freed Associates, Inc. 

for IT security/PHI security. An office policy for IT configuration regarding password complexity and password protection is routine for EHR systems but easily overlooked.

• Are there policies and procedures addressing EHR data recovery and restoration? The need for data recovery and restoration may occur as a result of a disaster (e.g., fire, flood, earthquake, temporary building disruption) or disruption of EHR vendor applications. Having offsite data storage with a reputable IT vendor will facilitate office data recovery and restoration. Your office will benefit from having well-documented procedures for staff notification, office down time, and patient notification.

**HIPAA Compliance**

HIPAA-related office policies and procedures frequently overlook specific items. Here is a checklist of specific HIPAA-related items for inclusion in your office policies and procedures:

• Does your employee handbook adequately address HIPAA/PHI education?

• Is the frequency of HIPAA training (for new employees and continual training) described?

• Are employees required to pass a test demonstrating HIPAA knowledge upon employment?

• Are employees required to pass a test demonstrating HIPAA knowledge at defined intervals of employment?

• Are there clearly-defined guidelines for employee social media use? Social media office policy considerations should note that information obtained through your work is confidential, posting patient information without authorization is a violation of the patient's right to privacy and confidentiality, and de-identification of PHI requires removal of all 18 PHI identifiers, which includes "Any other unique identifying number, code, or characteristic" (e.g., photo of a wound; description of a patient's condition).

• Does your employee handbook adequately address HIPAA/PHI information transmission, destruction, and data breach notification?

• Do your office procedures address the security of paper documents containing PHI?

• Are paper documents containing PHI adequately secured (in secured storage or protected from theft or viewing) within the office during office hours?

• Are there policies and procedures for the secure destruction of paper documents containing PHI?

• Do your office procedures address the security of facsimile transmissions containing PHI?

• Does your office policy address procedures required to insure PHI is transmitted to the correct recipient?

• Does your office policy address notification procedures in the event of incorrect receipt of PHI?

© 2012-2021 Freed Associates, Inc. 

• Do your office procedures address notification by staff about a data breach (e.g., transmission to other external entities, accidental loss of office PHI)?

**Business Associate Agreements**

A Business Associate is a person or organization that performs functions or provides services that involve the use or disclosure of individually identifiable health information. For example, PRF is a Business Associate to each of its Insureds.

Every health care provider who transmits health information electronically in connection with certain transactions is a Covered Entity. Common transactions include claims, benefit eligibility inquiries, and referral authorization requests.

Business Associate functions or activities on behalf of a Covered Entity include claims processing, data analysis, utilization review, and billing. Business Associate services to a Covered Entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Individuals and organizations are not considered Business Associates if their functions or services do not involve the use or disclosure of PHI, and where any access to PHI would be incidental, if at all.

A checklist of items sometimes overlooked in medical office BA agreements follows:

• Does your BA agreement outline when and how the BA may disclose PHI?

• Are PHI conditions of use by the BA clearly outlined?

• Are the exclusions identified so that the BA will not disclose PHI except as permitted?

• Does the language outline how the BA implements HIPAA safeguards for electronic PHI?

• Does the agreement state that the BA is to report to the Covered Entity any use or disclosure of PHI not covered by contract?

• In the agreement, does it say that the BA must return or destroy any PHI as covered by the contract at the conclusion of the contract?

Performing your own security and risk assessment may help you avoid disastrous compliance consequences. We strongly urge you to use these checklists to expose risks you were not aware existed. In the end they will provide you with piece of mind regarding the security of PHI within your practice.

© 2012-2021 Freed Associates, Inc. 