CAPAssurance℠

A RISK PURCHASING GROUP

For Your Protection. For Your Success.

A program of

COOPERATIVE OF AMERICAN PHYSICIANS

The 6 Most Common HIPAA Violations

(and How to Prevent Them)

Table of Contents

This compendium seeks to provide useful information regarding the HIPAA Omnibus Final Rule, including highlighting many of the common violations. However, it is important that any provider seek appropriate advice from a licensed attorney with respect to any individual questions or impacts on their situation, as the Final Rule is both nuanced and complicated. Please do not rely on this brochure as legal advice, as it is not such advice nor intended to be. Rather, it is a broad primer on many of the important elements and common violations of the Final Rule.

Introduction

As every physician knows, a HIPAA violation can be costly.

A single action, such as the loss of a laptop, can result in multiple violations—up to $50,000 per patient record, with an annual maximum penalty of $1.5 million. In 2015 alone, the U.S. Department of Health & Human Services (HHS) Office of Civil Rights imposed a number of six-digit fines to healthcare organizations for the improper disclosure or handling of both personal health information (PHI) and electronic PHI (ePHI).

As an example, a practice in North Carolina recently agreed to pay $750,000 to settle charges that it potentially violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule by handing over x-rays for 17,300 patients to a potential business partner without first executing a business associate agreement. The 22-physician group also agreed to a robust corrective action plan.

While it's virtually impossible to ensure that your practice will never experience a HIPAA breach, there are a number of preventative measures you and your staff can take now to significantly reduce the likelihood of a violation and the potential penalties.

The following highlights the most common ways physicians and staff violate HIPAA regulations, as well as recommendations to help sufficiently protect your practice.

The 6 Most Common HIPAA Violations

1 Improper Use and Disclosure of PHI

Many HIPAA violations occur because staff members have not been adequately educated about their responsibilities to protect all patients' PHI. All staff should be properly trained on workstation security to significantly reduce the chances of a privacy breach. We offer the following tips:

- **Never share usernames and passwords**

  Educating your employees on the personal liability they face if a breach occurs using their login credentials is an effective way to help ensure they do not share their username and password with others. If a HIPAA breach occurs using their login credentials, they could be held personally liable for the breach and may face a monetary fine and/or criminal sanctions.

- **Always log out before leaving a workstation**

  An unattended workstation with access to PHI by an unauthorized individual may lead to a HIPAA breach. Staff should always log off when leaving a workstation when PHI is on the screen. Auto logoff with a short duration should be required on all office computers.

- **Assign highly secure passwords**

  When secure passwords are not required, most users revert to overly simplistic passwords that are easily hacked. In most cases, this can be prevented within the EMR/EHR and/or the operating system by requiring a unique personal identifier. Your employees should be encouraged to use strong passwords that include at least eight characters containing a combination of uppercase and lowercase letters, numbers, and special characters. Also encourage employees to change their password every 45-90 days for optimal protection.

- **Ensure the correct disclosure of PHI**

  Before releasing any information to outside parties, it is imperative that the patient give written authorization. The authorization form should include the patient's legal name, the specific information that is permitted

for disclosure, and the date through which the authorization is valid. All employees need to thoroughly understand this requirement.

- **Properly dispose of all PHI and other sensitive patient information**

  Sensitive information and PHI should never be placed in a regular trash can. Rather, it should be placed in a secure receptacle to be shredded, incinerated, or disposed of by an appropriate (business associate) vendor. Placing signs at trash cans, recycling bins, and shredding stations is an effective reminder for employees to dispose of PHI correctly.

2 Publicly Disclosing PHI

Discussing PHI with staff in the normal course of patient care is expected and necessary. But when unnecessary or irrelevant discussions take place, problems arise.

- **Never discuss clinical conditions within earshot of others**

  Use caution when conducting conversations with coworkers about patients in walkways, hallways, and other public spaces. Remember that keeping the conversation anonymous does not prevent a potential violation.

- **Avoid gossip**

  All employees should be careful to avoid gossiping, even if they believe no one will find out about their conversation. Unfortunately, sharing information casually with friends, family, and coworkers is one of the most common HIPAA violations.

- **Implement and enforce a strict social media policy**

  For many employees, use of social media is as natural as speaking on the phone. Therefore, a confidentiality agreement and a strong social media policy need to be in place. This should be supplemented with proper and recurrent education to ensure your staff understands the importance and sensitivity of the information in their workplace. Employees should never disclose work-related sensitive patient information through social media, such as Twitter, Facebook, and the like.

3 Failing to Maintain Mandated HIPAA Documentation and Conduct Risk Assessments

HIPAA requires physicians to complete an inordinate amount of paperwork that can be easily put off—but which is critical to keep up to date in the event of a breach. We therefore recommend that you:

- **Conduct and maintain documented periodic risk assessments**

  The HIPAA Omnibus Rules require **all** covered entities and business associates to conduct a thorough risk assessment **at least once a year.** A proper risk assessment typically encompasses review of administrative, physical, and technical safeguards along with organizational and policy documentation. It should demonstrate that all policies align with the actual practices, and that appropriate staff education has been conducted and is documented.

  HIPAA requires that you perform a periodic "risk analysis" of your practice. A risk analysis is a mandatory analysis of your practice that identifies the strengths and weaknesses of the safeguards your practice has in place to protect patient information and privacy. A risk analysis should include an evaluation of at least three types of safeguards you should utilize in your practice: (1) physical safeguards; (2) technical safeguards; and (3) administrative safeguards.

  A risk analysis is a formal process and must be documented in writing. The risk analysis should include documented review of each type of safeguard, as well as any identified weaknesses and/or deficiencies of those safeguards in your practice. After you identify any existing weaknesses and/or deficiencies in your safeguards, you should either take the appropriate steps to address those weaknesses and/or deficiencies in your safeguards or document the reasons why you cannot reasonably address or implement those safeguards.

Remember, each practice is unique and a risk analysis must consider these differences in privacy and security needs, resources, and capabilities. For example, a risk assessment for a specialty surgical group of 20 physicians may look very different from a risk analysis for a medical practice of two or three psychiatrists.

A risk analysis should be ongoing. There should be continuous examination of security, especially as equipment and systems change. The HIPAA Security Rule* does not specify how frequently to perform a risk analysis. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annually or every three years) depending on circumstances of their environment. We recommend at least annually.

- **Prepare a breach response plan**

  Develop and implement specific tailored breach response plans that detail what will happen when a loss of data or an incident occurs. This should include contacting your medical professional liability carrier and your HIPAA compliance vendor. Identify roles and responsibilities for each staff member involved in patient care.

- **Review your Business Associate Agreements (BAA)**

  All business associate agreements should be reviewed to ensure that each of the components are in line with the contractual obligations and adhere to the "Minimum Necessary Standard," which states that the only information shared about patients is "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

***The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.**

4 Exposing Yourself to Hackers/Cyber Risk

Cybercriminals are increasingly targeting healthcare, and your patients' medical records are the prime target of hackers. A medical health record is extremely valuable: experts say it can sell for $60 to $70 on the black market, compared to just 50 cents or one dollar for a stolen Social Security number. Protecting your practice from cybercriminals, hackers, and malware is not easy and smaller entities may require the expertise of a third party IT expert. The following are some steps which must be taken to limit cybercriminal access to your records:

- **Install software patches**

  Not keeping your server and your workstations up to date exposes your entire network. Many recent data breaches occurred because of tardiness in installing software patches. Stay on top of software updates and enable automatic updates where possible for workstations and mobile devices. For servers, we recommend manual installations of updates, but with automatic downloads and notifications.

  Critical software that needs to be patched include: EHRs, Java, Flash, Office products, Web browsers, and operating systems like Windows and Mac OS X. Turn off unnecessary Web browser plugins like Java and Flash whenever possible (or at least enable "click-to-play" for Web plugins) to minimize the danger of "drive-by" infections.

- **Ensure HIPAA-compliant, properly configured firewalls**

  In most cases, firewalls designed for home use or provided by your Internet service provider for free do not meet HIPAA security and configuration requirements. Ensure your firewalls meet HIPAA standards.

  Also, simply having a firewall doesn't guarantee that it's configured securely. Managing traffic appropriately at the firewall level is essential.

- **Install intrusion prevention software**

  Unlike most firewalls, intrusion prevention devices or software use regularly updated intrusion definition databases to assist them in keeping your network locked down from the outside world. Consider intrusion protection an extra, but critical, step in keeping your electronic patient records safe.

- **Maintain up-to-date antivirus software**

  Keeping your antivirus definitions database up to date is as important as having it in the first place. The easiest way to manage the antivirus software in your practice is to use a centrally managed solution. Popular programs like AVG include network manageable antivirus software.

  Apple and mobile users aren't immune from attack either. Malware attacks targeting Apple OS X, iOS, and Android are on the rise so antivirus software is important no matter what operating system.

5 Compromising Data by No or Poor Encryption Technology

HIPAA recommends PHI be encrypted whenever possible, including while in transit (including across your local network) and when at rest on laptops, workstations, mobile, and storage devices. Encryption has become even more crucial as storage capacities increase—a single USB stick could hold hundreds of thousands of patient records! Below are must-do tips to help ensure your data is never compromised:

- **Secure all laptops, tablets, smartphones, and USB drives**

  Portable devices are the most commonly breached and stolen form of media. It is critical that all devices have encrypted storage of at least 128–bit strength and strong passwords.

  Other important safeguards for mobile devices include implementing remote wipe capabilities, passcode-protecting smartphones, and increased training and awareness of the risks.

- **Ensure strong wireless encryption**

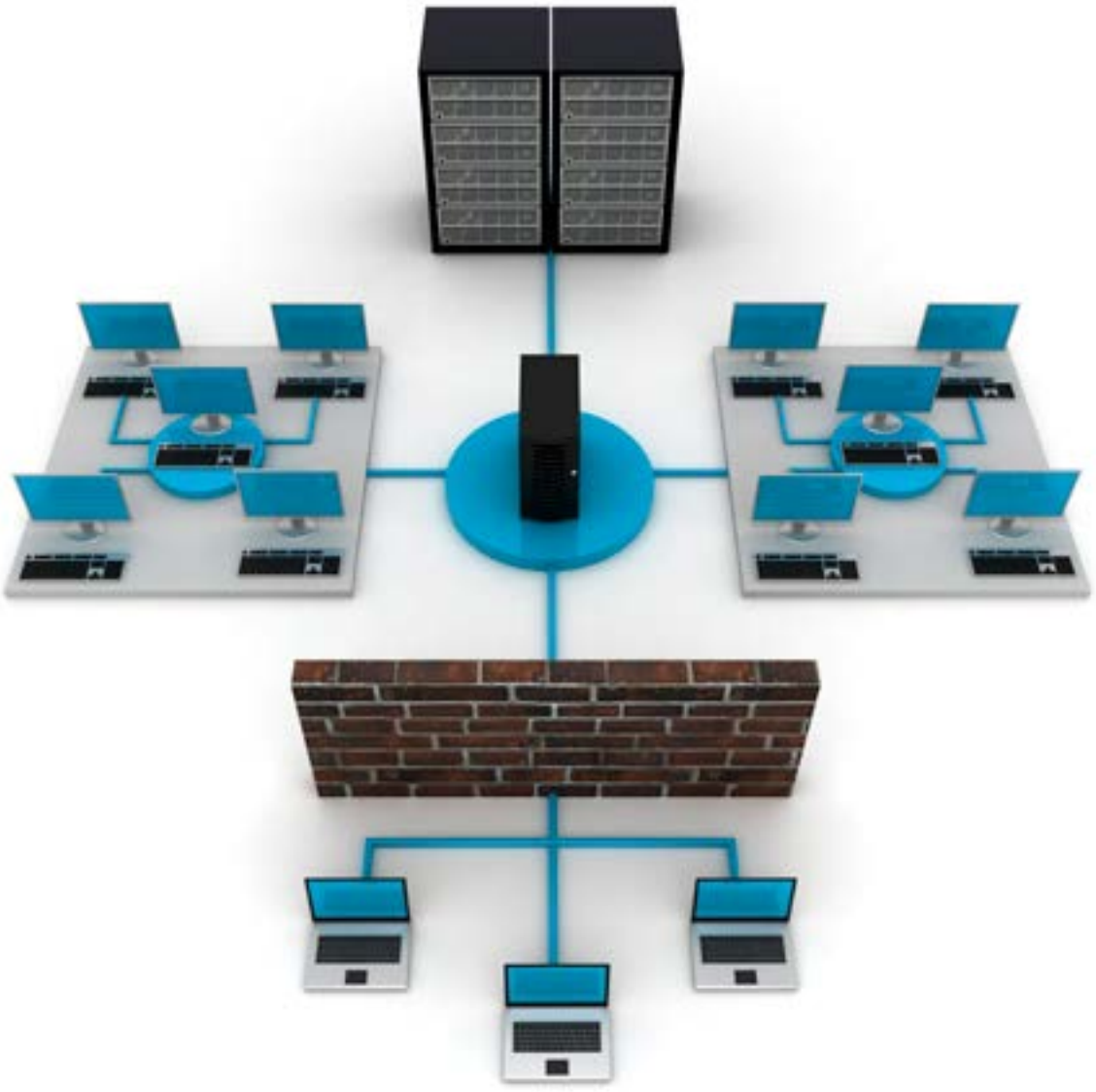
  Gaining wireless access to your network is the equivalent of giving a hacker a seat in front of your server. Older wireless devices that only support WEP encryption should be upgraded to devices that support newer, higher-level encryption algorithms.

  Although any encryption is better than nothing, if you are not using the Advanced Encryption Standard (AES), you may not meet HIPAA standards for PHI. Network passwords need to meet the same standards as other passwords and should be changed on a regular basis and after staffing changes.

6 Improperly Disposing PHI

PPHI can end up in unexpected places. Be sure to always think through where and how PHI can remain on devices and networks.

- Just because the lease on a piece of equipment is over, it doesn't mean your responsibility for the data on it has ended. Many networked peripherals store information, and often that information contains PHI. Be sure to erase all data from copier hard drives, faxes, syncing devices, and other hard device hard drives. A properly documented and executed disposal policy can prevent this common source of HIPAA violation.



Conclusion

It is important to remember that while the Office of Civil Rights can impose stiff penalties in the case of a breach, whether they actually *will* is determined by the answers to the following questions:

1. Is there a current risk analysis?
2. What safeguards were in place before the breach?
3. What safeguards were operational when the breach occurred?
4. What has changed since the breach?

Actions to take now:

- Review your current PHI and BAA practices and take adequate safeguards. Be careful to thoroughly document those safeguards. Consider hiring a third party HIPAA service to help you.
- Review your current risk analysis. If you have not performed a risk analysis, it is strongly recommended that you do one.
- Ensure that you have adequate cyber risk coverage.

In case of a breach:

- Immediately contact your HIPAA compliance provider, medical professional liability carrier, and your cyber risk insurance provider.
- Take recommended steps to mitigate and notify as needed.

Special Thanks

CAP would like to extend special thanks to Jeff Mongelli, who compiled the list for *The 6 Most Common HIPAA Violations* and was of invaluable assistance in providing expert review for this booklet.

Jeff is the Chief Executive Officer of Acentec, Inc., a nationwide provider of HIPAA compliance and medical IT management services. He is a well-known speaker at industry events and is frequently quoted in national publications on IT security and HIPAA compliance. Jeff has over 25 years of in-depth IT and security experience.

About the CAPAssurance

CAPAssurance, a Risk Purchasing Group, provides large medical groups, hospitals, and healthcare facilities access to superior professional liability insurance and flexible coverage options. (CAP) has supported California's best physicians for 40 years with outstanding medical professional liability coverage.

As a program of Cooperative of American Physicians, Inc. (CAP), CAPAssurance provides exceptional claims defense, and risk and practice management programs designed to help you mitigate risk, improve patient satisfaction, and run a financially successful organization.

Cooperative of American Physicians, Inc. is licensed as a property and casualty broker-agent and surplus line broker (California license No. OB72723). Insurance purchased by CAPAssurance is from a "non-admitted" or "surplus line" insurer that is not licensed by the state of California.

333 S. Hope Street, 8th Floor, Los Angeles, CA 90071