Physician's Guide to HIPAA Compliance

UNDERSTANDING HIPAA: TOP 10 TIPS

1. WHAT IS PROTECTED HEALTH INFORMATION? – All "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. RULE OF THUMB: If it contains any type of health data (including payment information) and identifies the individual or there is a reasonable basis to believe it can be used to identify the individual, it is PHI.

2. WHO IS A COVERED ENTITY? – Health plans, health care clearinghouses, health care providers (includes physicians) conducting certain financial and administrative transactions electronically (e.g., claim submission, billing, and fund transfers). Actively-practicing physicians should assume "covered entity" status.

3. WHO IS A BUSINESS ASSOCIATE? – A person or entity to whom a covered entity discloses PHI so as to carry out, assist with, or perform a function on behalf of the covered entity (includes lawyers, vendors, subcontractors, experts, court reporters), except for employees of the covered entity.

4. WHAT IS A BUSINESS ASSOCIATE AGREEMENT? – A required contract that provides compliance with HIPAA security rule provisions mandating administrative, physical, and technical safeguards for PHI. A BAA must include restrictions on use and disclosure of PHI and set forth mandatory notification requirements to the Department of Health & Human Services (HHS) if a PHI security breach occurs.

5. HOW IS PHI "SECURED"? – PHI can be secured by destroying it (which renders it unusable) or complying with the encryption guidance standards set by HHS. Proper encryption ultimately avoids the breach notification obligations in event of unauthorized use or disclosure of PHI.

6. WHAT CONSTITUTES "UNSECURED" PHI? – PHI contained in hard copy form, as well as electronic storage or transmission of non-encrypted PHI.

7. WHAT IS A PHI "BREACH"? – Any impermissible disclosure of PHI is a breach unless "low probability that PHI was disclosed."

8. ARE PEER REVIEW ACTIVITIES SUBJECT TO HIPAA? – Peer review conducted through the proper channels falls into the exception for "health care operations." But common pitfalls (see reverse) exist that may expose physicians to HIPAA liability, so be cautious whenever transmitting PHI to any third party.

9. WHAT PENALTIES EXIST FOR HIPAA VIOLATIONS? – Criminal/civil penalties include fines ($100 to $50,000) and prison terms (1 year to 10 years). Intent is considered.

10. USE GOVERNMENT RESOURCES FOR COMPLIANCE – Find sample BAA contract language, notices of privacy practices, security compliance guidance, mobile device security compliance, and more by exploring the HHS's web site.

For additional tips visit The Doctor's Advocate blog, www.doctor-advocate.com.

AVOIDING COMMON HIPAA PITFALLS: TOP 10 TIPS

1. **BE AWARE THAT PHI IS EVERYWHERE** – PHI's incredibly broad definition (see reverse, Tip No. 1) includes many common identifiers such as name, address, birth date, and social security number if they can be associated with health data content, which is usually the case in a health care environment.

2. **REVIEW OF ANOTHER PHYSICIAN'S PATIENT, REQUESTED OR NOT** – Collegiality is not an exception under HIPAA. Except in formally conducted peer review or quality assurance meetings, be very careful when another physician requests that you review PHI. Unless you are a treating or consulting physician for that patient (and the medical record reflects that status) do not access PHI.

3. **ACCESSING PHI WHEN NOT TREATING PATIENT** – As a physician, you may find yourself in health care environments (whether physically or virtually) in which you are not treating a patient. Medical records systems may contain PHI for patients that are not yours. You may be present in a health care facility where you do not have clinical privileges. Be aware that these situations pose risk and avoid them.

4. **DON'T DO IT BECAUSE OTHERS DID IT** – HIPAA implementation is far from perfect. As a physician, make sure you are safeguarding PHI of your patients and not accessing PHI of patients that are not yours, even if others do so, as that will not provide you a defense.

5. **AUDIO OR VIDEO RECORDING OF EVENTS** – While it may not be illegal in your state to record a conversation over the phone or in person if you are a party to it (check state law), surreptitious audio or video recording in health care environments should be absolutely avoided.

6. **USE APPROPRIATE LOCKS AND SAFEGUARDS** – Whether PHI is in electronic form or hard copy, it must be secured pursuant to HIPAA's specific requirements. Hard copies should be locked in a file cabinet or desk drawer in a locked office while unencrypted electronic information should be password protected and properly safeguarded with firewalls. HIPAA compliant policies and procedures must be observed at all times.

7. **MOBILE DEVICES POSE SPECIAL RISK** – Physicians should strictly observe certain protocols (see www.healthit.gov/mobiledevices) with any mobile devices that contain PHI, including maintaining physical control at all times, using encryption and passwords, installing firewall and remote disabling software, using adequate security when using public Wi-Fi networks, and deleting all PHI before discarding any device.

8. **FORWARDING PHI FOR BUSINESS, LEGAL, OR ANY REASONS** – Attorneys, accountants, and business advisors are business associates (see reverse, Tip No. 3). If you forward PHI in any form, you must sign an appropriate BAA with them and comply with it. Also, unless an employee, any third-party/vendor who has access to PHI is a business associate, including copy services, experts, storage facilities, and other third parties. Janitorial services that "incidentally" have contact with PHI do not require a BAA.

9. **FORMAL HEALTH CARE OPERATIONS (INCLUDING PEER REVIEW) ARE EXEMPTED** – But a physician must operate within these formal channels and privileges by complying with all policies and procedures, and not outside of them. If you are the subject of the peer review, get the advice of a health care attorney to make sure you are able to defend yourself without violating HIPAA.

10. **DON'T BE A TARGET** – HIPAA violations have now become the focus of many health care entities, especially given visible public enforcement efforts and current technology that makes them easier to prove. Avoid even the appearance of HIPAA a violation and consult with a health care attorney if any issues arise.

ZANER LAW

KARIN ZANER, ATTORNEY AT LAW
ZANER LAW PC
8117 PRESTON RD., SUITE 300 · DALLAS, TX 75225
1800 LAVACA ST., SUITE 502 · AUSTIN, TX 78701
214·363·5036 O · 214·363·5046 F · 214·236·9956 C
KARIN@ZANER.LAW