



Understanding HIPAA, Compliance and Implications

- *Wendy Gittleson*

The American Health Insurance Portability and Accountability Act of 1996, or HIPAA, is a broad reaching law that affects every aspect of the health care industry. Title I of HIPAA specifically affects the health insurance industry and has little to no impact on records management procedures. Title II was written to protect patients from fraud and abuse of privacy. Failure to comply with Title II of HIPAA can result in civil and even criminal penalties. It's important that medical professionals become well versed in Title II. It's also important that medical professionals establish a relationship with a records management company that helps its practice comply with HIPAA. GRM's integrated medical records management solutions have a multi-tiered approach to help a medical practice become compliant and remain compliant throughout the life of a record.

The intent of HIPAA Regulations is twofold. It is designed to protect patient privacy while simultaneously allowing sharing of patient information among hospitals, physicians, pharmacists and other health care professionals. By April of 2006, all medical entities were required to be compliant. Failure to comply can result in loss of Medicare and Medicaid payments as well as fines. Fines can range from \$100 to \$50,000 per incident, depending on a company's track record on compliance.

Fine collection is up to each state's Attorney General. When a breach occurs, it is up to the Attorney General to determine the most probable cause of that breach. If the breached records follow a chain of custody as with all Covered Entity/Business Associate relationships, in our opinion, the Attorney General will seek to find the weakest link with the deepest pockets.

HIPAA compliance is a requirement of all office sizes and of all healthcare vendors. Covered entities should be particularly careful to check individual state regulations. You will be required to adhere to the stricter of the two regulations.

An effective records management system won't guarantee absolute compliance, but it can help keep your company in the \$100 per breach category instead of the \$50,000 category.

A HIPAA compliant records management program should look at three aspects; integrity, confidentiality and availability, and lastly, you will need proof of compliance. In this white paper, we will look at each aspect and how GRM can be a valuable partner in a fully HIPAA compliant records management system.



Integrity:

Integrity means that a company's data is dependable and accurate. The data must also be available and must not be altered or destroyed. Integrity can be breached in a number of ways, including data entry errors, mechanical errors, human error, poor integration or encryption, computer viruses and system hackers. It's imperative that a company is able to show that all precautions were taken to protect the integrity of its data, beginning with encryption of all digital data.

GRM Digital offers a variety of solutions to assist with data integrity. The GRM Online Record Center has redundant data centers to ensure that documents are safe from disaster and available to users via the internet or a private intranet 24/7. We offer intrusion detection, monitoring, encryption and physical security to protect information and comply with regulations.

Confidentiality and Availability:

The HIPAA Privacy Rule regulates the use and disclosure of certain information held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers.) It establishes regulations for the use and disclosure of medical records and payment history. A covered entity has 30 days to disclose information to facilitate treatment, health care operations or payment. They may also be required by law in cases such as abuse. They can also disclose information with patient consent. When disclosing information, covered entities must make reasonable efforts to only disclose the minimum amount of information.

GRM's eAccess Technology gives a complete chain-of-custody record. It will give a real time record of all transactions, allowing medical professionals and government regulators to see the precise information that was disclosed and when.

Proof of Compliance:

The definition of proof of HIPAA compliance is rather vague; however the burden of proof will always fall upon the healthcare provider. There are steps that must be taken including organized record keeping, encryption of all data, proper firewalls and chain-of-custody tracking.

GRM Document Management and some other records management vendors offer integrated solutions that can help with all aspects of records compliance. A web based database like GRM's eAccess can consolidate all patient records, including billing records into a web based database. A portion or the entirety of the file can be shared upon your discretion and with strict password protected access.

eVaulting technology will ensure that your data is deduplicated, encrypted, compressed and transmitted to one of our top tier data centers.