

Free Tech Report
Executive IT Info Series

*"Virtual CTO" Tim Gillen reports on
current business technology issues*

Staying HIPAA Compliant with Online Data Storage

Keeping patient records secure and private is the concern of every hospital and health care provider, but they are often overwhelmed with years and years of patient information and the lack of adequate storage space. Destroying these health records in order to make room for more storage is often not an option. Patients want access to all of their health care records, and physicians need them in order to better diagnose patients.

Online data storage is a way to satisfy all of these issues. Using online storage for these records allows easier access for patients, and offers easier sharing of patient information from hospital to physician, as well as from physician to physician. Storing health records online isn't, however, without security concerns. Patients, hospitals, and physicians want assurance that these confidential records will remain safe, private, and secure, and will only be accessed by those authorized to do so.

What is HIPAA?

HIPAA or the Health Insurance Portability and Accountability Act of 1996 was created in order to protect health information and give patients certain rights regarding their private health information. It also allows for disclosure of health information necessary for patient care. This act specifies safeguards necessary for administrative, and physical and technical handling of patient health information.

According to the U.S. Department of Health and Human Services (HHS.gov) HIPAA has many requirements and restrictions. It requires safeguards for:

- Access Control
- Audit Controls
- Person or Entity Authentication

Access control is defined in the HIPAA Privacy Rule as "the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource." It should allow authorized users to only access the minimum amount of information necessary to complete job functions. The Access Control specification also requires the implementation of an exclusive user identification or user ID, and immediate access in case of an emergency.

What Type of Security is Necessary?

When dealing with patient records in an office, maintaining privacy and security usually involves storing patient files in locked cabinets where the files can be physically secured and visibly monitored at all times. When you are storing patient information online, certain precautions must be met in order to maintain the same security and privacy guaranteed each patient.

While HIPAA permits patient records to be transmitted over the Internet, businesses will want a service that offers file encryption, authentication and password protection in order to secure the information. Although HIPAA does not require online data storage services to have encryption, it does require that patient information be adequately protected and accessible only to authorized persons. Encryption is the best way to protect that information and ensure authorized access to those records. It is also important to offer backup services in case of a virus attack, flood, or fire. Finally, the service must offer a method of tracking any security breach, as well as the ability to lock out former employees after they have left or been terminated.

When storing patient information, it is important to stay HIPAA compliant, as the fines for not doing so are expensive. While online storage for health care businesses guarantees less worry, work, and expense for health care providers, the service is only as good as the security offered. Remaining HIPAA compliant is vital in order to continue a good business relationship with the health care industry.

Timothy Gillen CNE | MCP
CEO & President
"Virtual" CTO

AskTim@terrapiIT.com