Protecting Patient Privacy at the Touch of a Button

By Heather Bremner Claverie

NOT LONG AGO, file cabinets and fax machines were the high-tech vehicles used to store and share medical records. Then, healthcare providers began moving records to in-house servers. But, these days, most medical records are stored in the metaphorical sky or, in technological terminology, the cloud. In other words, electronic health records (EHRs) now live in web-based servers and are maintained by companies that provide the security and other administrative tools necessary to maintain patient privacy.

Storing medical data in electronic databases has its advantages. Physicians claim it helps reduce medication errors and enables them to quickly and easily send records. In addition, the cost to pay a cloud computing company is usually more affordable than hiring in-house personnel.

Yet, while paper files could be protected by alarms, security guards and lock and key, EHRs are susceptible to cybercriminals who can hack into the systems and steal this private information. Fortunately, companies that provide medical data storage are tightening their cybersecurity. In fact, a variety of storage options are available depending upon the healthcare company, hospital or physician's needs.

Storing Patient Data: The Regulations

There is no single format for EHRs that healthcare providers are required to use. However, there are security measures they must take. And, if auditors determine they failed in this respect, they can be fined.

The U.S. Department of Health and Human Services (HHS) has extended the medical privacy act known as the Health Insurance Portability and Accountability Act (HIPAA) to include specific cybersecurity regulations for cloud-computing databases. Any healthcare provider, from a small-town doctor to a medical HMO to a billing company, must follow HIPAA guidelines. In addition, under the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, anyone, even a subcontractor such as a cloud-computing company, that creates, receives, maintains or transmits protected health information falls into the covered-entity category. This act also significantly increased the penalties from a previous rate of $100 per violation and a maximum of $25,000 to a range of $100 to $50,000 per violation and a maximum of $1.5 million depending on the severity of the claim and the determined liability of the institution.

Cloud Computing

With the widespread proliferation of cloud computing, HHS has enacted specific rules to ensure entities strive to maintain secure patient medical data and limit breaches. HIPAA requires that when physicians or other covered entities use companies to store their medical data, they must enter into a contract with the business associate that specifies the safeguards they must follow to protect patients' health information:

- Covered entities must identify and analyze any potential risks to the security of the documents.
- Measures to address any identified risks must be implemented.
- A designated security official must be appointed to develop and implement all security measures.
- Covered entities should not use or disclose protected health information, unless permitted by their agreement or are legally required to do so.
- They must use all appropriate safeguards to comply with the privacy act with respect to electronic medical records.
- If a breach is discovered, the entity must disclose the incident.

The Good News

In the old days when paper was king, transmitting and receiving healthcare documents often took weeks or longer. With the use of technology, medical records can now be sent to various sites and to patients, healthcare workers and hospitals immediately. Also, with the popularity of mobile access, many companies now offer packages that allow access on devices such as iPads and iPhones.

Many of the HIPAA violations boil down to improperly executed or nonexistent business associate agreements. Therefore, when signing up with a medical data storage company, make sure the agreements are properly executed to protect all parties.

HEATHER BREMNER CLAVERIE is a contributing writer for *IG Living* magazine.

Shopping Guide to Medical Data Storage

Key for Convenience

One of the major benefits of Microsoft's OneDrive is that many healthcare organizations are already using Microsoft Office. The software company's enterprise cloud services are HIPAA- and HITECH-compliant and are billed as one of the most secure in the industry. Prices start at $35 a month for the Enterprise E5 system, which includes storing 1 terabyte of files and advanced security management that assesses risks and threats.
onedrive.live.com/about/en-us/business

Sky's the Limit

CareCloud was established as an electronic medical record application for the healthcare industry in 2009. At a beginning rate of $628 a month, this company is pricier than its competitors, but many users give it high marks for versatility and ease of use. It's designed to meet a variety of practices, from a one-physician office to a large hospital.
www.carecloud.com/ehr

Just Drop It

Dropbox is a familiar brand name to many healthcare workers, and since becoming HIPAA- and HITECH-compliant in 2015, it can now be used for confidential medical records. Customers who are already using Dropbox Business can sign a business associate agreement electronically. Prices vary depending upon the package.
www.dropbox.com

Boxing Day

Box for Healthcare, a cloud storage company, began marketing its services in the healthcare sector six years ago when they became HIPAA- and HITECH-compliant. Doctors can use Box to store a patient's medical records or clinical summary in the cloud, and share clinical documents, images and medical records with other healthcare providers and patients. Contact them for pricing.
www.box.com/industries/healthcare

Just Google It

Google has jumped into the medical sector with its G Suite for healthcare businesses by Google Cloud. Customers can now opt to store their patient data in a HIPAA-compliant sector of Google Drive. The company offers mobile device management and specialty encryption software for its service. The enterprise account, which includes all the necessary security measures and unlimited storage, is $25 a month per user. Potential customers can sign up for a trial run.
gsuite.google.com/industries/healthcare

Back It Up

Carbonite for Office users can enjoy perks like backup recovery for disasters and compliance with the Massachusetts Data Security Regulation, which they claim offers the most secure data nationwide. Carbonite offers data encryption in both the cloud and locally. Plans range from $269.99 to $1,299.99 per year. The first two include 250 GB of storage and the enterprise version has 500 GB of storage.
www.carbonite.com/backup-software/buy-carbonite-safe