Cloud-based systems can help secure patient information

Asaf Cidon, PhD

Dr. Cidon is CEO and Co-founder of Sookasa and holds a PhD from Stanford University, specializing in mobile and cloud computing, Stanford, California.

Disclosure
Dr. Cidon is CEO and co-founder of Sookasa.

Physicians hardly need the Health Insurance Portability and Accountability Act (HIPAA) to remind them how important it is to safeguard their patients' records. Physicians understand that patient information is sensitive and it would be disastrous if their files became public or fell into the wrong hands. However, the use of health information technology to record patient information, although beneficial for medical professionals and patients, poses risks to patient privacy.[1]

HIPAA requires clinicians and health care systems to protect patient information, whether it is maintained in an electronic health records system, stored on a mobile device, or transmitted via e-mail to another physician. The U.S. Department of Health and Human Services will increase HIPAA audits this year to make sure that medical practices have taken measures to protect their patients' health information. Physicians and other clinicians can take advantage of cloud-based file-sharing services, such as Dropbox, without running afoul of HIPAA.

Mobile computing, the cloud, and patient information: A risky combination

Although mobile computing and cloud-based file-sharing sites such as Dropbox and Google Drive allow physicians to take notes on a tablet, annotate those notes on a laptop, and share them with a physician who views them on his (her) desktop, this free flow of information makes it more difficult to stay compliant with HIPAA.

Dropbox and other file-sharing services encrypt documents while they're stored in the cloud but the files are unprotected when downloaded to a device. E-mail, which isn't as versatile or useful as these services, also is not HIPAA-compliant unless the files are encrypted.

Often, small psychiatric practices use these online services and e-mail even if they're aware of the risks because they don't have time to research a better solution. Or they might resort to faxing or even snail-mailing documents, losing out on the increased productivity that the cloud can provide.

Secure technologies satisfy auditors

A number of tools exist to help physicians seamlessly integrate the encryption necessary to keep their patients' records safe and meet HIPAA security requirements. Here's a look at 3 options.

Sookasa (plus Dropbox). One option is to invest in a software product designed to encrypt documents shared through cloud-based services. This type of software creates a compliance "shield" around files stored on the cloud, converting files into HIPAA safe havens. The files are encrypted when synced to new devices or shared with other users, meaning they're protected no matter where they reside.[2]

Sookasa is an online service that encrypts files shared and stored in Dropbox. The company plans to extend its support to other popular cloud services such as Google Drive and Microsoft OneDrive. Sookasa also audits and controls access to encrypted files, so that patient data can be blocked even if a device is lost or sto-

continued on page 52

continued from page 25

len. Sookasa users also can share files via e-mail with added encryption and authentication to make sure only the authorized receiver gets the documents.[2]

TigerText. Regular SMS text messages on your mobile phone aren't compliant with HIPAA, but TigerText replicates the texting experience in a secure way. Instead of being stored on your mobile phone, messages sent through TigerText are stored on the company's servers. Messages sent through the application can't be saved, copied, or forwarded to other recipients. TigerText messages also are deleted, either after a set time period or after they've been read. Because the messages aren't stored on phones, a lost or stolen phone won't result in a data breach and a HIPAA violation.[3]

Secure text messaging won't help physicians store and manage large amounts of patient files, but it's a must-have if they use texting to communicate about patient care.

DataMotion SecureMail provides e-mail encryption services to health care organizations and other enterprises. Using a decryption key, authorized users can open and read the encrypted e-mails, which are HIPAA-compliant.[4] This method is superior to other services that encrypt e-mails on the server. Several providers, such as Google's e-mail encryption service Postini, ensure that e-mails are encrypted when they are stored on the server; however, the body text and attachments included in specific e-mails are not encrypted on the senders' and receivers' devices. If you lose a connected device, you would still be at risk of a HIPAA breach.

DataMotion's SecureMail provides detailed tracking and logging of e-mails, which is necessary for auditing purposes. The product also works on mobile devices.

E-mail is a helpful tool for quickly sharing files and an e-mail encryption product such as SecureMail makes it possible to do so securely. Other e-mail encryption products do not securely store and back up all files in a centralized way.

File-sharing services encrypt documents while they're stored in the cloud but they are unprotected when downloaded to a device

References

1. U.S. Department of Health and Human Services. HIPAA privacy, security, and breach notification adult program. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit. Accessed February 12, 2015.
2. Sookasa Web site. How it works. https://www.sookasa.com/how-it-works. Accessed February 12, 2015.
3. TigerText Web site. http://www.tigertext.com. Accessed February 12, 2015.
4. DataMotion Web site. http://datamotion.com/products/securemail/securemail-desktop. Accessed February 12, 2015.

Discuss this article at www.facebook.com/CurrentPsychiatry