SOOKASA WHITEPAPER | **HIPAA COMPLIANCE**

www.sookasa.com

Demystifying HIPAA Compliance in the Cloud

Healthcare's challenges

There's no shortage of signals that the healthcare industry is under pressure: To do more with less, to provide higher quality care, to offer services more cheaply—all while remaining HIPAA compliant.

There's a stunning confluence of factors shifting healthcare's priorities, all part of a trend toward reducing costs and improving outcomes.

- **Payments:** Move away from fee-for-service models in favor of capitated contracts and / or bundled payments.
- **Coordination:** Increased focus on care coordination between different providers.
- **Insurance:** Growth in insured due to Obamacare and the rise of high-deductible plans means people are taking on more risk.
- **Reimbursement:** Paying for successful outcomes.
- **Compliance:** Greater emphasis on compliance, privacy, and fraud detection. HIPAA fines are huge, and reporting and notification is required.
- **Consumerization:** More apps mean more data—and more choices.

The increasingly mobile nature of medical services as well as the need for rapid, convenient, and high-volume data sharing means that healthcare professionals increasingly want to access data on-the-go. High volumes are being shared among organizations, including large images, medical bills, and scanned patient records.

Pair that with the advent of mobile devices, and the demand for ubiquitous data has boomed. So, too, have cloud file sharing services, which answer the call to make information available anywhere. In recent years, market leaders such as Dropbox (400 million users), Google Drive (240 million users), and Box (41 million users) have seen dramatic growth in the number of users and devices they serve.

Innovations like the cloud are supposed to address this demand for data, making it easier than ever for healthcare professionals to keep clinical data at their fingertips, coordinate care among providers, share information with patients, and pass on data to billing and insurance companies. The cloud offers a low-cost, user-friendly alternative to complex, expensive and hard-to-support legacy systems.

But when it comes to dealing with patient health information, that's easier said than done, often leaving professionals forced to suffer a tradeoff between privacy and productivity. Security and HIPAA compliance are essential, and recently, file sync-and-share providers like Dropbox and Google Drive took a step in the right direction by signing Business Associates' Agreements that let healthcare organizations use their services to store and share PHI while maintaining HIPAA compliance. But while these providers support compliance for files on their servers as part of the BAA, users still have to hold up their end of the bargain by protecting the way they work with data.

Compliance challenges

Cloud file sharing services conveniently synchronize files on any device, but they also scatter files across a large number of employees, mobile devices, and external partners. This, in turn, dramatically increases the risk of a HIPAA breach.

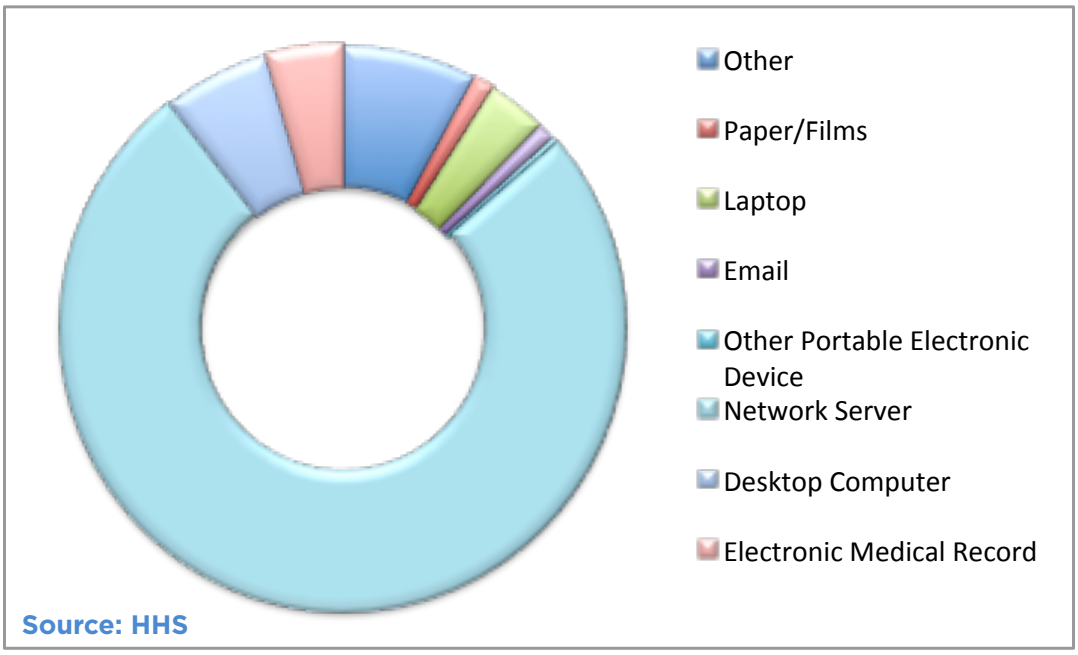
HIPAA breaches related to cloud file-sharing services can generally be attributed to two issues:

1. **Proliferation—and loss—of devices:** The increase in the number and usage of mobile devices significantly increases the risk of loss. According to Consumer Reports, more than 5.2 million smartphones were lost or stolen in the U.S. in 2014, up from 4.5 million in 2013. File sharing applications enable each device to tap into a large number of unprotected files. The loss of a single device that contains unprotected Personal Health Information (PHI) constitutes a HIPAA breach.
2. **Accidental sharing:** In this way, the simplicity of sharing is actually a hindrance. With "one-click" features for sharing files, folders, and full directories with individuals and groups, it's easier than ever to share thousands of files—and to mistakenly send this information to an unauthorized person.

An analysis of all reported HIPAA breaches since 2006 revealed that more than 70 percent of all breaches resulted from the loss or theft of unencrypted storage devices.

According to the Department of Health and Human Services' data, there were 115 data breaches that affected more than 500 people last year, prompting many to call 2014 the year of the breach.

HIPAA Breaches Affecting 500+ Records 2009-2015



Source: HHS

Growing risks

As federal agencies step up their oversight, the stakes when it comes to HIPAA compliance are higher than ever. Patient trust has always been on the line. Failing to ensure privacy and gain patients' trust can erode the care providers are able to deliver. What's more, with breach notification laws and a new national standard on the way, HIPAA violation don't exist in a vacuum. Health entities who have breached HIPAA must notify patients—and also have their names published on HHS' Data Breach Notification website, also known as the "Wall of Shame," which can have devastating effects.

But under the Health Information Technology for Economic and Clinical Health Act, the financial penalties are also searing, reaching the millions of dollars depending on the level of culpability. Though small entities are also subject to audits, OCR is focused on rooting out major breaches, such as the $4.8 million settlement with New York Presbyterian Hospital and Columbia University after the healthcare system exposed 6,800 patient records.

And if recent cases are any indication, it's clear that OCR is on the lookout for all types of breaches. Running unsupported and unpatched software, as Anchorage Community Mental Health Services learned the hard way this year, can constitute a breach, as can leaving boxes of medical records unattended. Fragmentation continues to rule the way healthcare entities run their businesses, meaning there are more ways than ever for non-compliance to creep in.

What's more, HITECH also expands the scope of what sorts of entities can be found liable, applying to covered entities as well as their business associates, from billing and insurance companies to legal counsel.

Finally, HHS' Office of Civil Rights is stepping up random audits of major institutions and smaller providers to proactively bring violations to light. Every covered entity and business associate could be subject to an audit, which focuses on the following three HIPAA standards:

- **Security Rule:** Risk analysis and risk management
- **Privacy Rule:** Notice of privacy practices and access rights
- Breach Notification Rule Content and timeliness of breach notification

For Phase 1, which focused on covered entities, OCR audited 115 covered entities. It found the smallest players struggled with compliance under all three of the HIPAA Standards. More than 60 percent of the violation findings or observations were related to security standards, with 58 of 59 audited health care provider covered entities had at least one such finding.

Phase 2 of the audit program, which will encompass 400 business associates, began its preliminary surveying in 2015, with audits expected to occur in 2016.

Sookasa's patented HIPAA-compliant Dropbox solution

Given the importance of simplicity and synchronizing massive amounts of files across multiple devices, mainstream file-sharing providers like Dropbox and Google Drive are the preferred sync-and-share solutions for the healthcare space. In a survey conducted by The Compliancy Group, a HIPAA compliance consultancy, 55 percent of healthcare providers surveyed said they use Dropbox to store and share healthcare documents.

Many cloud providers have signed Business Associates Agreements, which render them HIPAA-compliant, but proper security measures are taken on the user's side as well.

Sookasa is the only solution that overlays these cloud providers' file sharing services with a complete set of HIPAA safeguards. Sookasa facilitates HIPAA compliance for cloud file sharing services without compromising the user experience. Sookasa preserves the providers' native user interfaces, including mobile access, sharing, and synchronization.

Once installed, Sookasa automatically creates a folder called "Sookasa" in each user's existing cloud provider's account. The Sookasa folder is a safe haven for all business-related or sensitive files. Any file that is placed inside the Sookasa folder is automatically encrypted, thereby giving the company full control over access to the file.

Sookasa's primary mechanisms to ensure HIPAA compliance include:

- **Device loss / theft protection:** Sookasa allows encryption and decryption of electronic protected health information via its PC, Mac, iOS, and Android clients as well as on its web browser interface. With Sookasa's device block feature, users can remotely wipe the keys associated with certain devices and users so that it will no longer be able to decrypt sensitive information.
- **Protection from accidental sharing:** By encrypting files and granting access based on authenticated credentials, Sookasa ensures only authorized people can access electronic protected health information. Sookasa users define a whitelist of authorized employees and partners. Sookasa also features real-time access revocation to terminated employees and business associates.
- **Full audit trail:** Sookasa tracks every encrypted file across team accounts. It logs every modification, copy, access, or share operation made to encrypted files and associates each with a user. With a simple reporting tool, Sookasa provides complete audit trails on all operations with encrypted files.
- **Business Associate Agreements:** Sookasa signs BAAs with customers to ensure that PHI is encrypted in the cloud and on connected devices, but does not itself hold any PHI.
- **Emergency access:** Sookasa allows administrative access to necessary electronic protected health information during an emergency through a centralized web-based dashboard.
- **Automatic logoff:** Sookasa terminates a session after a predetermined period of inactivity, the length of which administrators can customize.
- **Seamless encryption and decryption:** Sookasa allows encryption and decryption of electronic protected health information via its PC, Mac, iOS, and Android clients as well as on its web browser interface.

Sookasa is the only solution that provides end-to-end encryption for cloud file-sharing services. With Sookasa's file-level encryption approach, files remain encrypted and tracked by Sookasa—even if they are moved outside their primary cloud applications.