HIPAA Cloud Burst

New Guidance Proves Cloud Services Are Business Associates

By Mike Semel

It's over. New guidance from the federal Office for Civil Rights (OCR) confirms that cloud services that store patient information must comply with HIPAA.

Many cloud services and data centers have denied their obligations by claiming they are not HIPAA Business Associates because:

a. They have no access to their customer's electronic Protected Health Information (ePHI),
b. Their customer's ePHI is encrypted and they don't have the encryption key,
c. They never look at their customer's ePHI,
d. Their customers manage the access to their own ePHI in the cloud,
e. Their terms and conditions prohibit the storage of ePHI, and
f. They only store ePHI 'temporarily' and therefore must be exempt as a 'conduit.'

Each of these excuses has been debunked in HIPAA Cloud Guidance released on October 7, 2016, by the Office for Civil Rights.

The new guidance clearly explains that any cloud vendor that stores ePHI must:

a. Sign a HIPAA Business Associate Agreement,
b. Conduct a HIPAA Security Risk Analysis,
c. Comply with the HIPAA Privacy Rule,
d. Implement HIPAA Security Rule safeguards the ePHI to ensure its confidentiality, integrity, and availability.
e. Comply with the HIPAA Breach Reporting Rule by reporting any breaches of ePHI to its customers, and be directly liable for breaches it has caused.

The OCR provides examples of cloud services where clients manage access to their stored data. It discusses how a client can manage its users' access to the stored data, while the cloud service manages

the security of the technical infrastructure. Each needs to have a risk analysis that relates to its share of the responsibilities.

OCR also recently published guidance that cloud services cannot block or terminate a client's access to ePHI, for example, if they are in a dispute with their customer or the customer hasn't paid its bill.

As we have been saying for years, the 2013 HIPAA Omnibus Final Rule expanded the definition of HIPAA Business Associates to include anyone outside a HIPAA Covered Entity's workforce that "creates, receives, maintains, or transmits PHI" on behalf of the Covered Entity. It defines subcontractors as anyone outside of a Business Associate's workforce that "creates, receives, maintains, or transmits PHI on behalf of another Business Associate."

'Maintains' means storing ePHI, and does not distinguish whether the ePHI is encrypted, whether the Business Associate looks at the ePHI, or even if its staff has physical access to the devices housing the ePHI (like servers stored in locked cabinets in a data center.)

A small medical clinic was fined $ 100,000 for using a free cloud mail service to communicate ePHI, and for using a free online calendar to schedule patient visits. Recently the OCR issued a $ 2.7 million penalty against Oregon Health & Science University (OHSU) partly for storing ePHI with a cloud service in the absence of a Business Associate Agreement.

"OHSU should have addressed the lack of a Business Associate Agreement before allowing a vendor to store ePHI," said OCR Director Jocelyn Samuels. "This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously."

So what does this mean to you?

If you are Covered Entity or a Business Associate…

- A common myth is that all ePHI is in a structured system like an Electronic Health Record system. This is wrong because ePHI includes anything that identifies a patient, nursing home resident, or health plan member that is identifiable (many more identifiers than just a name) and relates to the treatment, diagnosis, or payment for health care.

  EPHI can be in many forms. It does not have to be in a formal system like an Electronic Health Record (EHR) system, but can be contained in an e-mail, document, spreadsheet, scanned or faxed image, medical images, photographs, and even voice files, like a patient leaving a message in your computerized phone system requesting a prescription refill. During our risk analyses we find ePHI everywhere- on servers, local devices, portable media, mobile devices, and on cloud services. Our clients are usually shocked when we show them where their ePHI is hiding.

- Never store ePHI in any cloud service without first knowing that the service is compliant with HIPAA and will sign a HIPAA Business Associate Agreement.

  This automatically disqualifies:
  - The free texting that came with your cellular phone service;
  - Free e-mail services like Gmail, Yahoo!, Hotmail, etc.;
  - Free e-mail from your Internet service provider like Cox, Comcast, Time Warner, Charter, CenturyLink, Verizon, Frontier, etc.;
  - Free file sharing services from DropBox, Box.com, Google Drive, etc.
  - Consumer-grade online backup services.

- Another common myth is that if data is stored in the cloud that you don't have to secure your local devices. This is wrong because if someone can compromise a local device they can gain access to your data in the cloud. Be sure the mobile devices and local devices you use to access the cloud are properly protected, including those on your office network, and at users' homes. This means that all mobile devices like phones and tablets; PCs; and laptops should be secured to prevent unauthorized access. All devices should be constantly updated with security patches, and anti-virus/anti-malware software should be installed and current. If ePHI is stored on a local network, it must be a domain with logging turned on, and logs retained for six years.

- Use an e-mail service that complies with HIPAA. Microsoft Office 365 and similar business-class services advertise that they provide secure communications and will sign a HIPAA Business Associate Agreement.

- You may be using a vendor to remotely filter your e-mail before it arrives in your e-mail system. These services often retain a copy of each message so it can be accessed in the event your mail server goes down. Make sure your spam filtering service secures your messages and will sign a HIPAA Business Associate Agreement.

- Never send or text ePHI, even encrypted, to a caregiver or business associate at one of the free e-mail services.

- Never use the free texting that came with your cell service to communicate with patients and other caregivers.

- If you have sent text messages, e-mails, or stored documents containing ePHI using an unapproved service, delete those messages now, and talk with your compliance officer.

- Review your HIPAA compliance program, to ensure it really meets all of HIPAA's requirements under the Privacy, Security, and Data Breach Reporting rules. There are 176 auditable HIPAA items. You may also need to comply with other federal and state laws, plus contractual and insurance requirements.

If you are a cloud service, data center, or IT Managed Service Provider …

- If you have been denying that you are a HIPAA Business Associate, read the new guidance document and re-evaluate your decisions.
- If you do sign HIPAA Business Associate Agreements, you need to review your internal HIPAA compliance program to ensure that it meets all of the additional requirements in the HIPAA Privacy, Security, and Data Breach Reporting rules.
- Also become familiar with state regulations that protect personally identifiable information, including driver's license numbers, Social Security numbers, credit card and banking information. Know which states include protection of medical information, which will require breach reporting to the state attorney general in addition to the federal government. Know what states have more stringent reporting timeframes than HIPAA. You may have to deal with a large number of states with varying laws, depending on the data you house for customers.

- Make sure your Service Level Agreements and Terms & Conditions are not in conflict with the new guidance about blocking access to ePHI. Compare your policies for non-payment with the new guidance prohibiting locking out access to ePHI.
- Make sure your Service Level Agreements and Terms & Conditions include how you will handle a breach caused by your clients when they are using your service. Everyone should know what will happen, and who pays, if you get dragged into a client's data breach investigation.
- Make sure all of your subcontractors, and their subcontractors, comply with HIPAA. This includes the data centers you use to house and/or manage your infrastructure, programmers, help desk services, and backup vendors.
- Learn about HIPAA. We see many cloud vendors that promote their HIPAA compliance but can seldom answer even the most basic questions about the compliance requirements. Some believe they are compliant because they sign Business Associate Agreements. That is just the first step in a complex process to properly secure data and comply with the multiple regulations that affect you. We have helped many cloud services build compliance programs that protected them against significant financial risks.

- If you have administrative access to your client's networks that contain ePHI, you are a Business Associate. Even if your clients have not signed, or refused to sign, Business Associate Agreements, you are still a Business Associate and must follow all of the HIPAA rules.
- If you are reselling hosting services, co-location services, cloud storage, file sharing, online backup, Office 365/hosted Exchange, e-mail encryption, or spam filtering, you need to make sure your vendors are all compliant with HIPAA and that they will sign a Business Associate Agreement with you.
- Look at all the services your regulated clients need. Include in your project and managed service proposals clear links between your clients' needs and your services. For example, when installing replacement equipment, describe in detail the steps you will take to properly wipe and dispose of devices being replaced that have stored any ePHI. Link your managed services to your client's needs and include reports that directly tie to your clients' HIPAA requirements.

Talk to Semel Consulting about your needs. The OCR guidance validates what we have been saying and writing about cloud services since 2013. We have helped many HIPAA Covered Entities and Business Associates, including cloud services and IT Managed Service Providers, build effective HIPAA compliance programs, secure data, and protect their investments and reputations.

We give independent advice and training based on over 30 years in IT and over 12 years in HIPAA and other compliance requirements. Our founder and lead consultant is a recognized thought leader in the healthcare and IT industries. He has been the Chief Information Officer for a hospital and a K-12 school district, was the Chief Operating Officer for a cloud service, and has owned or managed MSP businesses for over 25 years. He has written HIPAA certification courses, had numerous articles published in magazines and on websites, and has spoken to many health care and IT technology groups. Visit www.semelconsulting.com for more information.

Mike Semel is the President and Chief Compliance Officer for Semel Consulting. He has owned IT businesses for over 30 years, has served as the Chief Information Officer for a hospital and a K-12 school district, and as the Chief Operating Officer for a cloud backup company. Mike is recognized as a HIPAA thought leader throughout the healthcare and IT industries, and has spoken at conferences including NASA's Occupational Health conference, the New York State Cybersecurity conference, and many IT conferences. He has written HIPAA certification classes and consults with healthcare organizations, cloud services, Managed Service Providers, and other business associates to help build strong cybersecurity and compliance programs. Mike can be reached at 888-997-3635 x 101 or mike@semelconsulting.com .