



The Challenges of Applying HIPAA to the Cloud



#PrivacyAcademy

#CSACongress

Adam Greene, Partner
Davis Wright Tremaine LLP

SEPTEMBER 17-19 • SAN JOSE



AGENDA

- Key Concepts Under HIPAA
- HIPAA Obligations for a BA
- Questions Remain
- Reaching Answers
- Resources



#PrivacyAcademy



#CSACongress

KEY CONCEPTS UNDER HIPAA

Covered Entity:

- Health care provider who electronically conducts certain administrative transactions with health plans
- Health plan
- Health care clearinghouse



#PrivacyAcademy



#CSACongress

KEY CONCEPTS UNDER HIPAA

Business Associate (“BA”):

- Person or entity who creates, receives, maintains, or transmits protected health information (“PHI”) on behalf of a covered entity or another business associate for a HIPAA-regulated activity
- No notice or business associate agreement is required to be a BA



KEY CONCEPTS UNDER HIPAA

Protected Health Information

Individually identifiable health information, including merely demographic information that is in a context that indicates an individual is/was a patient/enrollee of a health care provider or health plan.



#PrivacyAcademy



#CSACongress

CHANGE TO DEFINITION OF BA

- Business associate originally defined as person who uses or discloses individually identifiable health information
 - Some cloud providers interpreted that they did not use or disclose the information or fell under “conduit exception”
- 1/25/13 HIPAA rule revised definition to include entity that maintains PHI
 - BA compliance required by 9/23/13
 - Conduit exception limited to transmission services (with only incidental, temporary storage and random/infrequent access)



HIPAA OBLIGATIONS FOR A BA

Limits on uses and disclosures of PHI

- May not use or disclose PHI other than as permitted or required by business associate agreement (“BAA”)
- Generally may not use or disclose PHI in manner that is impermissible for covered entity under HIPAA
 - Exception for administration/mgmt of BA if permitted by BAA



HIPAA OBLIGATIONS FOR A BA

Assist with Patient Privacy Rights

- Patient right of access to certain PHI
- Patient right of amendment of certain PHI
- Patient right to an accounting of disclosures



#PrivacyAcademy



#CSACongress

HIPAA OBLIGATIONS FOR A BA

Must comply with the Security Rule

- Includes administrative, physical, and technical safeguards
- Requires documentation of policies, procedures, and basis for not implementing “addressable” specifications



HIPAA OBLIGATIONS FOR A BA

Pass on BAA obligations to subcontractor BAs

- Limits on uses and disclosures must be at least as restrictive
- Must require subcontractor BA to comply with the Security Rule



#PrivacyAcademy



#CSACongress

HIPAA OBLIGATIONS FOR A BA

Reporting obligations

1. Any impermissible use or disclosure (timing and content governed by BAA and state law)
2. Any security incidents (timing and content governed by BAA and state law)
3. Any “breach of unsecured PHI” (timing and content governed by HIPAA, BAA, and state law)



HIPAA OBLIGATIONS FOR A BA

- If business associate takes on covered entity's Privacy Rule compliance obligation, must comply with applicable requirements
- Must make internal records available to U.S. Dept. of Health and Human Services upon request



#PrivacyAcademy



#CSACongress

HIPAA OBLIGATIONS FOR A BA

- Must permit termination for breach of BAA
- Must return or destroy PHI if feasible; continue to protect PHI and limit use/disclosure if return or destruction infeasible



#PrivacyAcademy



#CSACongress

Questions Remain



#PrivacyAcademy



#CSACongress



Your poll will show here

1



Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or

[Open poll in your web browser](#)



If a cloud provider maintains only encrypted PHI and does not have a decryption key, then:

- A. It is a BA because it is maintaining PHI, even though the PHI is encrypted.
- B. It is not a BA because it does not have access to any PHI.



#PrivacyAcademy



#CSACongress



Your poll will show here

1


Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or

[Open poll in your web browser](#)



If a cloud provider contractually prohibits customers from storing PHI on its servers but a customer does so anyway, then:

- A. It is not a BA because it has no knowledge of maintaining PHI.
- B. It is a BA but has an affirmative defense to any penalties because of a lack of knowledge.
- C. It is a BA and is subject to millions in penalties if it has failed to comply with the Privacy, Security, and Breach Notification rules.





Your poll will show here

1



Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or

[Open poll in your web browser](#)



A colocation service maintains customers' servers in locked cabinets in its data center. The customers' servers include PHI. The colocation service:

- A. Is a BA because it maintains PHI on behalf of a covered entity.
- B. Is not a BA because it is analogous to a landlord, merely renting physical space to someone who maintains PHI.



“Security incident” is defined as including “attempted or unsuccessful” unauthorized access, use, disclosure, modification, or destruction of systems with electronic PHI.

A covered entity must include in its BAA a requirement to report any security incidents.



#PrivacyAcademy



#CSACongress



Your poll will show here

1



Install the app from
pollev.com/app

2

Make sure you are in
Slide Show mode

Still not working? Get help at pollev.com/app/help
or

[Open poll in your web browser](#)



If a cloud provider routinely experiences unsuccessful attempts to get past its security controls:

- A. It must log and report all unsuccessful attempts.
- B. It only must report non-routine attempts that pose a high risk.
- C. It may proactively report such unsuccessful attempts in its BAA.
- D. No reporting of such unsuccessful attempts is required.



OTHER REMAINING QUESTIONS

- Is a BA required to report impermissible use or disclosure of *encrypted* PHI?
- How can a BA provide access, amend, and account for disclosures of encrypted PHI when it does not have the encryption key?
- Does the health care entity, SaaS provider, and IaaS provider each have a separate obligation to encrypt and backup any electronic PHI?
- How does a SaaS reconcile a health care entity and an IaaS each requiring the use of their form BAAs, and such BAAs are inconsistent?



Reaching Answers



#PrivacyAcademy



#CSACongress



- Non-profit trade association created to:
 - **Reduce obstacles** to the health care sector leveraging cloud computing technology.
 - **Promote innovation** by reducing health care compliance burdens on health care technology companies.



#PrivacyAcademy



#CSACongress



Objectives:

1. Understanding – Create an accepted framework and tools for health care and cloud computing
2. Trust – Build trust in cloud computing and regulatory compliance through an accepted accreditation/certification process or other programs.
3. Government Outreach – Seek regulatory guidance from HHS and other relevant agencies. Maintain outreach and transparency with the government.



IMPROVING UNDERSTANDING

Promote a common framework:

- Providing access to cloud services satisfies access and amendment requirements.
- Accounting of disclosures need not identify type of PHI disclosed if unknown to cloud provider.
- Reporting requirements do not encompass encrypted PHI or routine unsuccessful security incidents.
- Identify cloud configurations that are appropriate for electronic PHI (e.g., dedicated instance).



#PrivacyAcademy



#CSACongress

IMPROVING UNDERSTANDING

Create helpful tools:

- Self-audit tool for SaaS, PaaS, and IaaS providers maintaining ePHI
- Model notice for cloud provider to notify customer of how privacy and security responsibilities are delegated
- Model BAA provisions specific to cloud computing providers



#PrivacyAcademy



#CSACongress

BUILDING TRUST

Work with other stakeholders (e.g., CSA, HIMSS) to identify and promote common means of demonstrating HIPAA compliance and good privacy and security:

- Identify what existing programs (e.g., SSAE 16 SOC 2, CSA STAR, FedRamp, etc.) best address health care and cloud issues
- Ensure scalability to allow innovation among small SaaS companies
- Promote common security questionnaires



GOVERNMENT OUTREACH

- Maintain transparency with government stakeholders such as HHS Office for Civil Rights, Office of the National Coordination for Health IT
- Seek clarification on ambiguities
- Consider seeking statutory fixes (e.g., affirmative defense for BAs who had no notice of PHI)



#PrivacyAcademy



#CSACongress

RESOURCES

- HIPAA regulations at www.dwt.com/hipaaregs
- HIPAA Omnibus Rule at <http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf> (pp. 5571-72 discuss “data storage” companies)
- HHS Office for Civil Rights at www.hhs.gov/ocr/privacy
- CSA Health Info. Mgmt. at <https://cloudsecurityalliance.org/research/him/>
- HIMSS Cloud Security Toolkit at <http://www.himss.org/library/healthcare-privacy-security/cloud-security/toolkit>
- 2014 HIMSS Cloud Analytics Survey at <http://www.himss.org/library/healthcare-privacy-security/cloud-security/security-survey>



QUESTIONS?



Adam H. Greene, JD, MPH

 **Davis Wright
Tremain** LLP

adamgreene@dwt.com

202.973.4213



#PrivacyAcademy



#CSACongress