


CHAMBLISS

fiercely loyal.

October 22, 2014

Time to Take Another Look: HIPAA Likely Applies to You



James L. Catanzaro, Jr.
Chambliss, Bahner & Sopher, P.C.
Liberty Tower • 605 Chestnut Street, Suite 1700 • Chattanooga, TN 37450
chamblisslaw.com

CHAMBLISS

fiercely loyal.

I. Privacy in the News

Russian Hackers Steal
1.2 Billion Usernames and Passwords

CHAMBLISS

fiercely loyal.

I. Privacy in the News

P. F. Chang's:
33 Restaurants Affected in Data Breach

CHAMBLISS
fiercely loyal.

I. Privacy in the News

Super-Valu
Becomes Latest to Suffer Data Breach

CHAMBLISS
fiercely loyal.

I. Privacy in the News

Community Health
says Data Stolen in Cyber Attack from China

CHAMBLISS
fiercely loyal.

I. Privacy in the News

Your Medical Records
are Worth More to Hackers
than Your Credit Card


CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 1:

HIPAA's privacy/security requirements apply only to health care providers.



CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

These requirements apply directly to any service provider using PHI for a health care provider or a health plan, and any subcontractor of the service provider.

These entities are called "*Business Associates.*"

CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

Example:

Steel Inc. Health Plan hires law firm.

Law firm as a Business Associate for Steel Inc. subcontracts accountant to help with benefit work.

Accountant is Business Associate subject to HIPAA!

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 2:

PHI only includes medical records.

10

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

PHI includes Covered Entity information relating to health condition, treatment, or billing for treatment that identifies individuals.

11


CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 3:

I am not a Business Associate if I do not sign a business associate agreement.

After DSI



12

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

If you create, receive or have access to PHI on behalf of a Covered Entity, you are a Business Associate.

13

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 4:

Once I sign a business associate agreement, nothing further is required.

14

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

The business associate agreement is only the beginning.

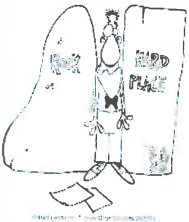
Be careful to understand key terms. Indemnity, LOL, breach response.

Business associates must also comply directly with the law!

15

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths



Example:

Accountant hired to help Steel Inc. must have security and privacy policies and training.

Make sure policies and BAA obligations consistent.

16

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 5:

Health records/information have no real value so I don't need to worry about the integrity of such information.


17

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

Medical records are worth more to hackers than credit card info.



18

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 6:

All I need are written policies to comply.

19

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

Policies are an important component.
However, there is a need to do a system risk assessment, train on breach protocols, and implement actual physical and technical safeguards.

20

CHAMBLISS
fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 7:

HIPAA penalties are minimal.

21

CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

HIPAA penalties were greatly increased in 2013 and are scaled based on compliance efforts.

"Willful neglect" or no effort risks \$50,000 per violation up to \$1.5M per year.

22

CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

MYTH # 8:

Could an accountant or "downstream" vendor ever get in trouble?

23

CHAMBLISS

fiercely loyal.

II. HIPAA Coverage and Dispelling Myths

TRUTH:

HIPAA complaints are on the rise.

State laws now supplement.

Data shows most breaches come from Business Associates!

24

CHAMBLISS
fiercely loyal.

III. Risks Areas to Consider

1.

From a practical standpoint, how do you handle protected health information?

It is a good idea to trace the receipt, creation and handling of protected health information within your organization.

15

CHAMBLISS
fiercely loyal.

III. Risks Areas to Consider

2.

To whom do you disclose the protected health information and why?

From whom do you need to secure BAAs?

16

CHAMBLISS
fiercely loyal.

III. Risks Areas to Consider

3.

Do workforce members have remote access to PHI or use remote devices to handle same?

17

CHAMBLISS
fiercely loyal.

III. Risks Areas to Consider

4.

Do your practices satisfy applicable business associate agreement requirements?

Do you have consistent obligations?

28

CHAMBLISS
fiercely loyal.


III. Risks Areas to Consider

5.

Do your workforce members understand when a breach occurs and what to do when that happens?

29

CHAMBLISS
fiercely loyal.



Disclaimer

This presentation is provided with the understanding that the presenter is not rendering legal advice or services. Laws are constantly changing, and each federal law, state law, and regulation should be checked by legal counsel for the most current version. We make no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained in this presentation. Do not act upon this information without seeking the advice of an attorney.

This outline is intended to be informational. It does not provide legal advice. Neither your attendance nor the presenter answering a specific audience member question creates an attorney-client relationship.

30
