Using HIPAA Privacy and Security Standards to Protect Your Agency

Presented by:
Jason Karn
Chief Compliance Officer
Total HIPAA Compliance

July 2018

This compliance corner is sponsored by the LPRT Committee

The View from the Top is Great….So are the benefits of being there!

Find out more on NAHU's website, search "LPRT"

Encouraging excellence in health and benefits insurance professionals since 1942

Sponsored by LPRT

What's the <u>BIG</u> deal?

- Profound Testimonial about YOU
- Distinguished
- Knowledgeable
- Successful
- The ELITE in your profession
- Motivation …

Circle of Excellence
SOARING EAGLE
NAHU Leading Producers Round Table

NAHU Leading Producers Round Table

QUESTIONS?

You may ask your question in the questions box at any time. Any questions that we do not answer during the webinar will be posted on the compliance corner webpage in the coming weeks.

The information herein should not be construed as legal or tax advice in any way. Regulations, guidance and legal opinions continue to change. The preparer has gathered public information and has attempted to present it in an easily readable and understandable format. Situations vary, technical corrections and future guidance may vary from what is discussed in the presentation.

This is meant for informational content only. The presenter makes no warranty of any kind concerning this information. You should seek the advice of your attorney or tax consultant for additional or specific information.

This presentation is not to be duplicated or distributed.

TODAY'S PRESENTER

Jason Karn
Chief Compliance Officer at Total HIPAA Compliance

Jason is a co-author of Total HIPAA's Training and Compliance Solutions, and a frequent national speaker on HIPAA and a regular HIPAA social media contributor.

As Chief Compliance Officer for Total HIPAA, Jason takes a hands-on approach to assisting clients with the details of developing a well-documented HIPAA compliance plan. He has been a featured speaker for the Georgia Association of Healthcare Underwriters (GAHU), National Broker's Association (NBA) at their annual conference, the Columbus Association of Health Underwriters (CAHU), and is the content creator and co-presenter of NueMD's 10-part webinar series on HIPAA Compliance. https://www.nuemd.com/webinars/hipaa

Total HIPAA is the preferred HIPAA provider of both NAIFA (National Association of Insurance and Financial Advisors) and NAHU (National Association of Health Underwriters).

An accomplished opera singer, Jason has performed around the world and recently made his New York City Opera debut. You can check him out on his opera website- www.jasonkarn.com

Housekeeping

This program is educational and does not constitute, and may not be construed as legal advice to, or creating an attorney-client relationship with, any person or entity.

The materials referenced here are subject to change, so frequent review of the source material is suggested.

AGENDA

- What are the carriers demanding?
- Why are carriers pushing compliance?
- How to use HIPAA to protect your business
- What are HIPAA and GLBA?
- State Privacy Regulations
- GDPR
- How an agency complies with HIPAA and GLBA
- HIPAA and GLBA fines and penalties
- Recent HIPAA and GLBA breaches
- 12 things you can do today to protect your business

New Carrier Requirements

- Blue Cross Blue Shield of Tennessee
  - SOC 2 Audit within 12 months or;
  - Signed attestation of HIPAA Compliance by C-Suite
- Blue Cross Blue Shield of South Carolina
  - SOC 2 or ISO 27001 Audit within 12 months or;
  - Signed attestation of HIPAA Compliance by C-Suite
- United Health Care of California
  - Online assessment questionnaire
  - Random online audits (We've seen agencies as small as 2 people selected for an audit.)
- Aetna
  - Install full disc encryption on all devices
  - Install Alert ACCESS software which monitors your encryption software

Why HIPAA?

- Meets All the Carrier Requirements!
- Faster to complete
- Cost-effective (affordable)
- Already required
- Meets other security requirements
  - GLBA
  - ACA
  - Individual state requirements

What is HIPAA

- Health Insurance Portability and Accountability Act
- Based on the National Institute of Standards and Technology Risk Management Framework 800-53 (NIST-RMF)
- Protected Health Information (PHI)
- Goal is to protect your client's information, but can be used to protect your business intelligence and comply with GLBA and State Privacy and Security Requirements

HIPAA Compliance is Required for:

- Medical Insurance
  - Medicare Supplement
  - Drug Coverage

- Dental Insurance

- Vision Insurance

- Long-Term Care Insurance
- Hearing
- Behavioral health
- Substance abuse
- Prescription drug coverage
- FSA or HSA coverage

The size of your agency or selling only a little of these insurances does not exempt you!

What is GLBA

Gramm-Leach-Bliley Act

- Applies to all financial products
- Protects Non-Public Private Information (NPPI)
- Requires an annual Notice of Privacy Practices (NPP)

State Security Laws

These states **require** a written security plan, agreements with contractors, and training of staff… sound familiar?

- Massachusetts's Written Information Security Program (WISP)
- California, Texas and Rhode Island Security Laws
- Oregon Identity Theft Protection Act

General Data Protection Regulation (GDPR)

- Went into affect May 25, 2018
- Protects EU citizens' Personally Identifiable Information (PII)
- Gives EU citizens control over their personal data
- Will become the defacto US standard for data protection because of major US corporations

HIPAA Provides A Protection Plan

- HIPAA is more than a group of Federal and State Privacy Requirements

It is WAR!

- In medieval times, each village had a strategy to protect themselves
  - Walls
  - Moats
  - Bridges
  - Towers
  - Soldiers

What You're Up Against

- Hackers
- Malware
- Ransomware
- Employee Mistakes
- Malicious Employees
- Disasters

Step 1- How Do You Prepare?

- Conduct a Risk Assessment
  - Administrative (who is in charge)
  - Physical (what physical protections will be in place)
  - Technical (how will you stop the enemy from crossing your wall)

Step 2 - Create a Plan

- Compliance Plan
  - Convert the information gathered in a Risk Assessment into a document (plan) that everyone can follow
  - Complete both parts of your plan
    - Privacy
    - Security

Step 3 - Reinforce Your "Wall"

- Network Security
  - Firewalls
  - Anti-Malware Software
  - Offsite Backups
- Electronic Device Security
  - Desktops
  - Laptops
  - Tablets
  - Smart Phones
- Facility Security
  - Fire Suppression
  - Security Alarms

Step 4 - HIPAA Compliant Communication

- Encrypted email
- HIPAA compliant faxing
- Texting
- Chat
- File sharing
- Video conferencing

Step 5 – Train Your Army

- Your plan is only as good as each soldier's preparation
- Staff needs to be trained on the Law and your agency's specific policies and procedures

Step 6 – Secure Your Assets

- Encrypt the information you hold to meet HIPAA standards so that it is protected
  - At rest
  - In transit
  - In storage

- Backup, Backup, Backup!

Real World Cost of a Breach

"2017 Cost of Data Breach Study: United States"

- **The Ponemon Institute** found that the average cost per breached record was **$221.00**
- Root causes of breaches
  - 50% Malicious or criminal attacks,
  - 27% System glitch,
  - 23% Human error

Ways to Decrease the Cost of Breach

- Have an incident response plan and team in place
- Implement extensive use of data encryption
- Train employees
- Use of data loss prevention software (Ex. firewalls, antivirus software)

Examples of data breaches

- Anthem Hack – $115 million settlement
  - Largest civil settlement for a consumer breach to date.
- Sony Hack – Estimated $15 million settlement
  - 435,000 employees were part of the class action suit.
  - Maximum of $10,000 paid per individual – most plaintiffs received $1-$3,000.
- Triple-S Management – $3.5 million fine
  - Investigations indicated widespread non-compliance throughout the corporation and its subsidiaries
- St. Joseph Health – $2.14 million fine
  - Reported that files containing ePHI were publicly accessible through internet search engines
- Advocate Health Care – $5.55 million fine
  - Three combined breaches affected the ePHI of approximately 4 million individuals

Who Regulates HIPAA and GLBA?

- HIPAA
  - Health and Human Services (OCR) regulates
  - State attorneys general
  - Legal action by affected clients or employees
- GLBA
  - Federal Trade Commission
  - FTC has brought almost 30 cases for violations of the GLB Act in 2017

Market forces can damage your business more than fines and penalties!

Penalties from Omnibus Ruling

Violation Category 1176(a)(1)	Each Violation	Maximum fine for an identical violation in a calendar year
(A) Did Not Know	$100-$50,000	$1,500,000
(B) Reasonable Cause	$1,000-$50,000	$1,500,000
(C)(i) Willful Neglect-Corrected	$10,000-$50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected	$50,000	$1,500,000

Criminal Penalties

Violation	Penalties
Knowingly obtaining or disclosing PHI	$50,000 + 1 year in prison
Offenses conducted under false pretenses	Up to $100,000 + 5 years in prison
Intent to sell, financial gain, harm	Up to $250,000 + 10 years in prison

GLBA Penalties

- You will lose your license
- You can be fined up to $100,000 per violation
- Officers and directors can be fined up to $10,000 per violation
- Fines will be doubled if GLBA is violated along with another federal law, or if there is a pattern of any illegal activity involving more than $100,000 within a 12-month period; offender can be imprisoned for up to 10 years
- Criminal Penalties include imprisonment for up to 5 years, a fine, or both

13 Steps You Can Take Today

1. Appoint HIPAA Privacy and Security Officer(s)
2. Turn on encryption and password protection for all digital devices
3. Turn on software firewall in computer operating system
4. Turn on Auto-Lock on all digital devices
5. Sign up for an email encryption program*
6. Sign up for encrypted file sharing*

*BA Agreements Required

13 Steps You Can Take Today, cont'd

7. Make a list of all Business Associates and Subcontractors your company uses
8. Sign Business Associate and Subcontractor Agreements with all vendors
9. Make a list of all places you have PHI stored in your company - physical and electronic
10. Change all weak passwords to difficult ones
11. Start using a password management program
12. Use 2-factor authentication
13. Train all employees

Questions

10% discount for NAHU Members, use the Coupon:

NAHU2018
www.TotalHIPAA.com/NAHU2018