



HIPAA Compliance and Health Insurance Agents

TOTALHIPAA
COMPLIANCE

Jason Karn
Chief Compliance Officer
Total HIPAA Compliance

January 2020

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 BIG deal?

- Profound testimonial about YOU
- Distinguished
- Knowledgeable
- Successful
- The ELITE in your profession
- Motivation...




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, a frequent national speaker on HIPAA, and a regular HIPAA social media contributor.

As Total HIPAA's CCO, 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 Brokers' 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.

Total HIPAA is the preferred HIPAA provider for NAHU.

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



AGENDA

- What is HIPAA
- What is GLBA
- State Privacy Rules
 - CCPA
 - WISP
 - NY DFS
- GDPR
- Carrier Audits
- It's War!
- Real World Cost of Breach
- How to Decrease the Cost of a Breach
- Who Regulates HIPAA and GLBA
- HIPAA Fines and Penalties
- GLBA Penalties
- 12 Steps You Can Take Today

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
 - Medicare Supplement
 - Drug Coverage



- Dental



- Vision



- Long-Term Care Insurance



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

What is GLBA

- Gramm-Leach-Bliley Act
- Applies to all financial products (life, Workers' Comp, commercial liability, etc.)
- Protects Non-Public Private Information (NPPI)
- Requires an annual Privacy Notice

State Security Laws

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

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

NY Department of Financial Services

- Regulated entities and licensed persons must file the Certification of Compliance for calendar year 2019 between January 1, 2020, and April 15, 2020
- File compliance online: www.dfs.ny.gov
- Exemptions:
 - Fewer than 10 employees
 - Less than \$5M gross income last 3 years in NY State
 - Less than \$10M in year-end total assets
 - You are an employee, agent, or representative under another Covered Entity, and follow their plan
 - Do not operate, maintain, utilize or control any IT systems, nor required to access, generate or receive NPPI
 - A captive insurance company that does not, and is not required to control, own, access, generate, receive or possess NPPI
- **Even if you qualify for an exemption you still need to file online**

California Consumer Protection Act

- CCPA doesn't apply to information that is subject to federal regulations
 - HIPAA and GLBA are exempt
 - *(c) This act shall not apply to protected or health information that is collected by a covered entity governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56 of Division 1)) or governed by the privacy, security, and breach notification rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996. For purposes of this subdivision, the definition of "medical information" in Section 56.05 shall apply and the definitions of "protected health information" and "covered entity" from the federal privacy rule shall apply.*

General Data Protection Regulation (GDPR)

- Effective as of May 25, 2018
- Protects EU citizens' Personally Identifiable Information (PII)
- Gives EU citizens control over their personal data
- Even insurers with no operations or presence in the EU are subject to the GDPR to the extent that they offer services to individuals located in the EU
- Breach notification rules different for any EU residents
 - Each country has its own supervisory authority
 - 72 hours “where feasible” to notify supervisory authority and affected persons
 - If you go beyond 72 hours, you must explain why there was a delay in reporting

Carrier Requirements... So Far

- 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 audits)
- More to come...

It's War!

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

What You're Up Against

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

Step 1 – How to 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 Walls

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

Step 4 – Communication

- Encrypted email
- HIPAA compliant faxing
- HIPAA compliant text and chat
- File sharing
- Video conferencing

All 3rd party software that has access to PHI requires a BA Agreement!

Step 5 – Train Your Army

- Your plan is only as good as each employee's preparation
- Your staff must be trained on HIPAA and your agency's specific policies and procedures

Step 6 – Secure Your Assets

- Encrypt the information you hold so that it is protected
- Backup! Backup! Backup! !

Real World Cost of a Breach

- On average, it takes **245 days** to identify and contain a breach
- Healthcare: highest industry average for breaches
- Lost business is the BIGGEST contributor to data breach costs!
- Small businesses face higher costs relative to their size to mitigate a breach

“Cost of a Data Breach Study.” IBM, <https://www.ibm.com/security/data-breach>

Decrease the Cost of a Breach

- “An ounce of prevention is worth a pound of cure!”
- Have a plan and a team in place
 - Test that plan
- **ENCRYPTION!**
 - Reduces breach costs on average by \$360,000
- Strong passwords
 - 2-factor authentication
- Train employees
- Use data loss prevention software

“Cost of a Data Breach Study.” IBM, <https://www.ibm.com/security/data-breach>

Who Regulates HIPAA and GLB

- HIPAA
 - Health and Human Services (OCR)
 - Individual State Attorneys General
- GLBA
 - Federal Trade Commission

Market forces can damage your business more than the 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	\$25,000
(B) Reasonable Cause	\$1,000-\$50,000	\$100,000
(C)(i) Willful Neglect - Corrected	\$10,000-\$50,000	\$250,000
(C)(ii) Willful Neglect - Not Corrected	\$50,000	\$1,500,000

Criminal Penalties

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

GLBA Penalties

- You will lose your license to practice
- 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 there's a pattern of any illegal activity involving more than \$100,000 within a 12-month period, he or she can be imprisoned for up to 10 years
- Criminal Penalties include imprisonment for up to 5 years, a fine, or both

12 Steps You Can Take Today

1. Appoint a HIPAA Privacy Officer and Security Officer
 - These may be the same person at a small agency
2. Turn on encryption and password protection for all digital devices
3. Turn on Auto-Lock on all digital devices
4. Implement an email encryption program*
5. Implement encrypted file sharing*

*BA Agreements Required

12 Steps You Can Take Today

6. Enable software firewall in computer operating system
7. Create a list all Business Associates your company uses
8. Sign Business Associate Agreements with all vendors
9. Create a list 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. Train all employees

RESOURCES

“Cost of a Data Breach Study.” IBM, <https://www.ibm.com/security/data-breach>



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.

Continuing Education



<https://nahu.org/professional-development/courses/hipaa>

NAHU's HIPAA Privacy and Security Training 2.0 Certification Course thoroughly explains the HIPAA laws in a multi-media format. This course is approved for three continuing education credits and is delivered online at the student's own pace.

See the handouts section for more information!