



HIPAA / HITECH

Agent Understanding And Compliance

Presented By:
Ed Massey
Affiliated Marketing Group

AMIG

brokerage general agency
713.977.0611
www.affiliatedmarketing.com



It's The Law

On February 17, 2010 the Health Information Technology for Economic and Clinical Health Act (HITECH) became law.

It impacts not only carriers, but the insurance agents who represent them as it broadly expands the scope of privacy Law under HIPAA.

This course will deal with the legal responsibility and rules governing the control of consumer's personal information that is under the control of independent insurance agents.



What is HIPAA?

- HIPAA is a federal law that was enacted for the purpose of increasing access to health Insurance products.
- However, the term "HIPAA" is primarily associated with two of its Regulations - the HIPAA Privacy Rule and the HIPAA Security Rule.



What is the HIPAA Privacy Rule?

The HIPAA Privacy Rule has two basic purposes:

- It regulates the use and disclosure of health information by insurance companies (and self-funded health plans) and health care providers, and
- It gives individuals certain rights about their own health information, such as a right know how their health data is being used, as we have the right to access and correct health records maintained by insurance companies (and self-funded health plans) and health care providers.
- Under both HIPAA and HITECH, organizations that perform services for customers on behalf of insurance carriers-such as independent insurance agents and outside service providers have to comply with the Privacy Rule requirements for use and disclosure of health information.



What is the HIPAA Security Rule?

- The HIPAA Security Rule governs health records and related information that is (or ever was) stored electronically. It is structured as a set of standards that are required to be met by insurance companies (and self-funded health plans) and health care providers. In turn, each standard is achieved by implementing a comprehensive set of safeguards covering physical, administrative and technical security.
- For example, an organization's strong-password policy is an example of an administrative safeguard for electronically-stored customer information.



What is HITECH?

HITECH is a new federal law that expands our responsibilities regarding our customers' medical-related information.

It significantly increases penalties associated with privacy and security violations, and expands our customers' privacy rights in five areas



The Five Parts of HITECH?

- Data breach notification requirement - If we use or disclose protected health information in a way that is not permitted by HIPAA, we must notify the individual and the federal government. Also, we must carefully document all situations that have the potential of constituting a data breach.
- Directly applies certain privacy and security requirements to other organizations we contract with to service our customers, such as staff and outside service providers.
- Allows privacy and security complaints to be brought by state as well as federal regulators
- Provides new limits on how we can use and disclose protected health information
- Gives individuals new rights over their protected health information



What do we mean by “Privacy”?

- The term "privacy" has different meanings in different contexts.
- In a business context, the term privacy generally means the legal protections given to certain pieces of data belonging to human beings.
- The rise of criminal identity theft has been a significant driver in the increase of data protection laws in the U.S. and around the world.



What laws regulate data privacy?

Data privacy laws represent a complex and growing body of law at the state and federal level. HIPPA – HITECH are just two of many.



What categories of data are protected?

- **Medical information is protected** by federal law ("HIPAA") as well as similar laws enacted in each state.
- **Insurance transaction information is protected by federal law ("GLBA") and enforced by state insurance departments.**
- **Social Security numbers are protected** by laws in each state, by GLBA and by HIPAA if combined with health information.
- **Banking account and credit or debit card information is protected** by laws in each state, GLBA and by HIPAA if combined with health information.
- **Adverse underwriting information is protected** by state laws.
- **Consumer credit information is protected** by federal and state laws.
- **Driver's license numbers are protected** by federal and state laws.



How do privacy/data protection laws affect me?

- As a representative of Insurance Companies, your job responsibilities require you to come into contact with the personal information of your customers and in many cases share that information with other organizations.
- As such, **you play an important role** in preventing breaches of customer data.



What are my responsibilities?

Remember that the customer's information belongs to them - they trust you to be responsible stewards of their information.

As an associate conducting business with insurance carriers, we are subject to compliance with HIPPA/HITECH

Failure to comply can result in termination of your contract with the carrier



Areas to Consider

- You should have privacy and security policies that address administrative, physical and technical safeguards
- Privacy and security training programs
- Confidentiality and/or nondisclosure agreements
- Return/destruction of information
- Process for providing an accounting of disclosures when requested or required;
- Limiting the use, disclosure and request of PHI to the minimum necessary



What is "protected health information" or PHI?


- "Protected health information" or PHI is a defined term used primarily in connection with HIPAA and HITECH. It means:
- Information that reasonably identifies an individual and that relates to either the individual's health status or condition, or payment for health care services for the individual.
- While a person's name is a clear example of data that identifies an individual, there are many types of information that are reasonably identifiers of an individual. For example, addresses and telephone numbers, social security numbers, insurance policy numbers, etc.
- When any of these "identifiers" are combined with either information about an individual's health status or condition or information about payment for health care services for the individual, then all of the information is considered PHI.



Are we still required to protect personal information even if it is not PHI?

The answer is yes.

While HIPAA - HITECH specifically governs PHI, there are many, many other privacy and data protection laws that require us to safeguard personal information that is not related to health and medical matters.



A list of all the types of personal information we should protect?

As a matter of legal compliance and best practices, we should be responsible custodians of any information about a customer that is personal to that individual especially, if the information if misused or wrongfully disclosed could result in reputational or financial harm.



Defining "Personal" Information

- An individual's name (either first and last name, or first initial and last name) and/or address/telephone number when combined with one or more of the following:
 - Date of birth
 - Social Security number
 - Drivers license number
 - Passport - Visa number
 - Insurance policy number
 - Banking information -routing and/or account numbers
 - Credit - debit card information
 - Health information
 - Net worth information
 - Adverse underwriting information
 - Consumer credit information
 - Log-in credentials for customer-accessible web sites
 - Images of customer signatures



Example Documents Containing Consumer Protected Information

- Others documents that should be protected:
- Health, Life or other Insurance Applications
- Emails
- Attending Physician Statements
- Medicals
- Bank draft instructions

Quote Your Client

The following form uses our Health Analyzer. Fill out all of the information requested below to get the most accurate quote available without going through full underwriting.

▶ Basic Quote Information:

State of Residence
Guaranteed Term
Coverage Amount
Payment Mode
Income / Liability Analysis
Minimum Needs Analysis

▶ Information About The Proposed Insured:

Gender: Male Female
Date of Birth: / /
Height/Weight: ft. in. lbs.

▶ Tobacco: Have you ever used tobacco products? Yes No

▶ Blood Pressure Information: Have you ever been treated for high blood pressure? Yes No

▶ Cholesterol Information: Have you ever been treated for high cholesterol? Yes No

▶ Driving History Information: Do you have a driver's license? Yes No

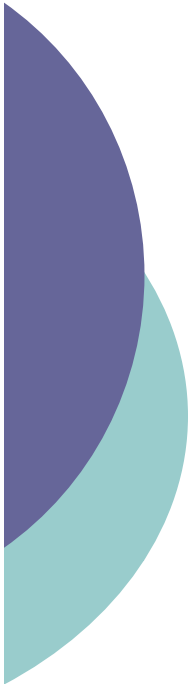
▶ Family History Part A: Family Related Death

Please indicate the total number of family members (parents or siblings) who have died from cardiovascular disease (heart attacks and strokes), cancer, diabetes or kidney disease before the age of 70:

▶ Family History Part B: Family Related Occurrence of Disease

Not including those who died, please indicate the total number of family members (parents or siblings) who have contracted a cardiovascular disease (heart attacks and strokes), cancer, diabetes, or kidney disease before the age of 70:

[Check Rates](#)



Online Application

*denotes a required field

Insured Information:	First Name:*	<input type="text"/>
	Middle Name:	<input type="text"/>
	Last Name:*	<input type="text"/>
	Birth Place:*	<input type="text"/> i.e. State or Country
	Gender:	<input checked="" type="checkbox"/> M <input type="checkbox"/> F
	Driver's License:*	<input type="text"/>
	Driver's License State:*	Select State <input type="text"/>
	SSN:*	<input type="text"/> i.e. 123-45-6789
	Residency Status:	Citizen <input checked="" type="checkbox"/> <input type="checkbox"/> Non-Citizen
	Address:	Street Address:*
Address Line 2:		<input type="text"/>
Address Line 3:		<input type="text"/>
City:*		<input type="text"/>
State:		Texas <input type="text"/>
Zip Code:*		<input type="text"/>
Contact Information:		Home Phone:*
	Cell Phone:	<input type="text"/>
	Work Phone:	<input type="text"/>
	Fax:	<input type="text"/>
	Best Time To Contact:*	Morning <input checked="" type="checkbox"/> <input type="checkbox"/> Afternoon <input type="checkbox"/> <input type="checkbox"/> Evening
	Email Address:*	<input type="text"/>
Other Information	Reason for Insurance:*	Family Protection <input checked="" type="checkbox"/> <input type="checkbox"/> Other
	Occupation:	<input type="text"/>
	Annual Income:	<input type="text"/>
	Net Worth:	<input type="text"/>

Existing Coverage: Do you have any existing insurance policy(s)? Yes No

Primary Beneficiary (At least one primary beneficiary is required)

Name:*	SSN/Tax ID:	Gender:*	Relationship:*	Date of Birth:*	Percent:*
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Check box if primary beneficiaries get equal shares.

Contingent Beneficiary

Name:*	SSN/Tax ID:	Gender:*	Relationship:*	Date of Birth:*	Percent:*
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	Male <input checked="" type="checkbox"/> Female <input type="checkbox"/>	Spouse <input checked="" type="checkbox"/> Other <input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Check box if contingent beneficiaries get equal shares.

XRAE - Build A Quote - Windows Internet Explorer

http://www.xrae.com/questions.aspx?quote=1335&guid=02fb302c-c079-4bcb-af52-d2ba19eebdf3&... Google

File Edit View Favorites Tools Help

XRAE - Build A Quote

Medical Questions

11. Q What is the client's cholesterol ratio? (example: 4.5)
A
12. Q Has the client EVER been treated (medications) for blood pressure?
A
13. Q What is the client's SYSTOLIC blood pressure reading? (Number on top, example: **135/75**)
A
14. Q What is the client's DIASTOLIC blood pressure reading? (Number on bottom, Example: **135/75**)
A
15. Q Has the client EVER been convicted of a DWI, DUI, reckless driving, moving violation, license revocation or suspension?
A
16. Q Has the client EVER participated in any hazardous avocations? (Aviation, Climbing/Mountaineering, Gliding, Motor Sport, Parachuting, Scuba Diving, etc.)
A
17. Q Does the client plan on traveling outside of the US or Canada? (**Travel Warnings**)
A
18. Q Has the client ever had or been treated for any other medical conditions? If yes, check all that apply:
A
19. Q List all other details, considerations, APS summaries or quote related information not previously provided.

Internet 100%

start Presentation1 HIPPA HITECH Cours... XRAE - Build A Quote ... 12:06 PM



What is a "data breach" law or a "data breach notification" law?

- Nearly every state requires that businesses notify customers whose protected data has been "breached". State laws differ, however, in many respects. State laws differ widely in what types of personal information is "protected" under the state's data breach law.
- In addition, some laws require notification only for breaches of electronic information or if a large number of individuals are affected.
- The HITECH data breach regulation requires individuals are notified in the event of any data breach that involves health information.



If Security Is Breached

In contrast to the previous version of HIPAA, covered entities must now notify individuals whose health information has been breached. Business associates must notify covered entities of any breaches; the covered entity must then notify the individual.



A Two-Part Inquiry

Does it qualify as a breach?

Was the information protected by encrypted technology? No notification to individuals is required if the breached information was covered by an encryption system approved by the U.S. Department of Health and Human Services (HHS). Those systems render the information “unusable, unreadable or indecipherable to unauthorized individuals,” using technologies or methods approved by HHS.

Notice must occur no later than 60 days after discovery of the breach—when at least one employee of the entity knows or should have known of the breach. Notice is also required to be provided to media outlets if the information of more than 500 individuals has been compromised. Notification must also be forwarded to HHS.



Examples Of Possible Breaches

A lost or stolen laptop, PDA, or flash drive that is used to store PHI.

Examples of paper breaches that must be reported include faxing PHI to an incorrect number or person, mailing PHI to the wrong address or person, or failing to shred paper PHI records prior to disposal.

Breaches that happen by word of mouth include releasing PHI over the telephone or in person to an unauthorized individual.

These are only a few examples of possible breaches of PHI. If you are unsure whether a breach has occurred, report it!



The Impact of Violations

The Health Information Technology for Economic and Clinical Health (HITECH) Act provides a tiered system for assessing the level of each HIPAA privacy violation and, therefore, its penalty



Tier A Violations

- Tier A is for violations in which the offender **didn't realize** he or she violated the Act and would have handled the matter differently if he or she had.
- This results in a **\$100** fine for **each violation**, and the total imposed for such violations cannot exceed **\$25,000** for the calendar year.



Tier B Violations

- Tier B is for violations due to **reasonable cause**, but not **“willful neglect.”**
- The result is a **\$1,000** fine for **each violation**, and the fines cannot exceed **\$100,000** for the calendar year.



Tier C Violations

- Tier C is for violations due to **willful neglect** that the organization **ultimately corrected**.
- The result is a **\$10,000** fine for **each violation**, and the fines cannot exceed **\$250,000** for the calendar year.



Tier D Violations

- Tier D is for violations of **willful neglect** that the organization **did not correct**.
- The result is a **\$50,000** fine for **each violation**, and the fines cannot exceed **\$1,500,000** for the calendar year.



State Recovery

The HITECH Act also allows states' attorneys general to **levy fines and seek attorneys fees** from covered entities **on behalf of victims**.

Courts now have the ability to **award costs**, which they were previously unable to do.



First Lawsuit Filed

On January 13, 2010 the Connecticut Attorney General's Office sued Health Net for failure to encrypt data on a portable electronic device.

A notebook computer disappeared from the offices of Healthnet. It contained health and financial data of 440,000 clients.

The filing indicates that Healthnet did not adequately protect the data and failed to notify authorities of the loss as required by law.



Applying Penalties

HHS will not impose the maximum penalty in all cases, but base the penalty on the nature and extent of the violation and resulting harm with consideration for the compliance history.

A Covered Entity may not assert an affirmative defense that it did not know and reasonably should not have known of a violation unless it also corrects the violation during the 30-day period beginning on the first date it learned of the breach.



What to Do if there is a Breach or Suspected Breach

- **Contact** and file a **police** report
- **Notify** the **carrier** compliance department of all carriers affected
- If required, work with the compliance department to **notify** all **clients** who have or may have had their personal information compromised
- **Notify state and federal agencies** as advised by the carriers involved



Summary

- Privacy Laws affect each of us in the conduct of our business.
- A **privacy and security policy** for protecting client information must be an integral part of office procedures. This should include but not be limited to computer and office file access.
- **Timely reviews** should be done to insure compliance with those procedures and to adjust the protocol to reflect changes in technology.
- **Respond quickly** if there is a breach or suspected breach of client information