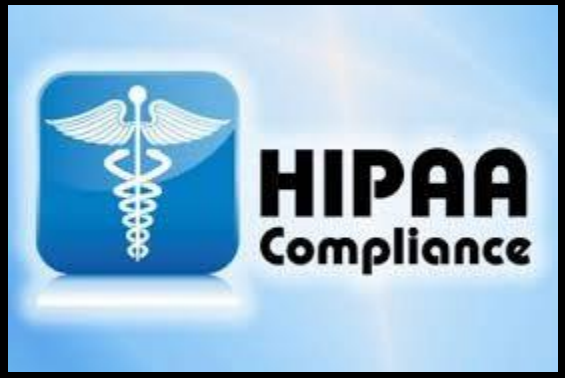
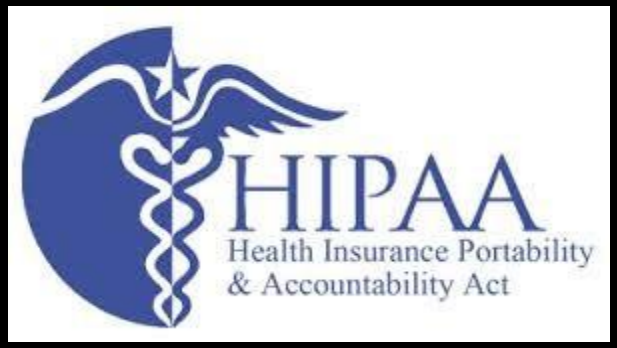
HIPAA Training for Independent Contractors and Temporary Employees



Training Objectives

- Review pertinent HIPAA Privacy & Security Rule requirements
- Know how these Rules affect **YOU** and **YOUR** contract with Alabama Health Guidance
- Know **YOUR** obligation to protect all forms of PHI/PII
- Know the consequences of HIPAA breaches
- Know **YOUR** obligation to report HIPAA incidents

PART 1:
HIPAA DEFINITIONS



HIPAA Definitions

- **Business Associate (BA)** – an enrollee or entity contracted with a covered entity (CE) to perform a function on the CE's behalf that involves Protected Health Information (PHI). You, or the organization you are affiliated with, are considered a BA and are bound to the terms listed in the Business Associate Agreement (BAA) with AHG. The BAA establishes your responsibility for complying with HIPAA Privacy and Security.

HIPAA Definitions

- **Covered Entity (CE)** – the entities listed below that are required to comply with HIPAA:

Health plans (includes HMOs, government health plans like Medicare, Medicaid, VA Programs, self-insured employer groups, etc.)

Providers (doctors, labs, dentists, home health companies, etc.)

Health care clearinghouses (that process data and create standardized formats)

You, as a Business Associate (BA), are also required to comply with HIPAA you are working on behalf of another HIPAA Covered Entity (CE).

HIPAA Definitions, cont.

- **Health Insurance Portability and Accountability Act (HIPAA) of 1996** – a federal law addressing various topics including the privacy and security of Protected Health Information (PHI). Privacy Rules were adopted in 2003 and Security Rules in 2005 that specifically require **you** to:
  - Protect PHI
  - Secure electronic PHI (e-PHI) both physically and electronically
  - Provide enrollees with specific rights related to their PHI

You are independently and directly liable for your compliance with HIPAA!

HIPAA Definitions, cont.

- **Personally Identifiable Information (PII)** – information used to distinguish or trace an enrollee's identity (e.g., SS#, enrollee #, Medicare #, Medicaid #, Name, etc.).
  - May be used alone or combined with other identifying information linked to a specific enrollee (date and place of birth, mother's maiden name, etc.).

- **Protected Health Information (PHI)** – individually identifiable health information related to the past, present or future physical and/or mental health condition of a enrollee, the past, present or future provision of care to a enrollee, or the payment for the provision of healthcare to the enrollee.
  - Health information + a PHI data element = PHI (see next slide for PHI data elements).
  - PHI **excludes** de-identified data, employment records held by a covered entity in its role as an employer, and health information about a decedent for 50 years following death are **not** considered PHI.

The same requirements that apply to PHI also apply to PII!!!

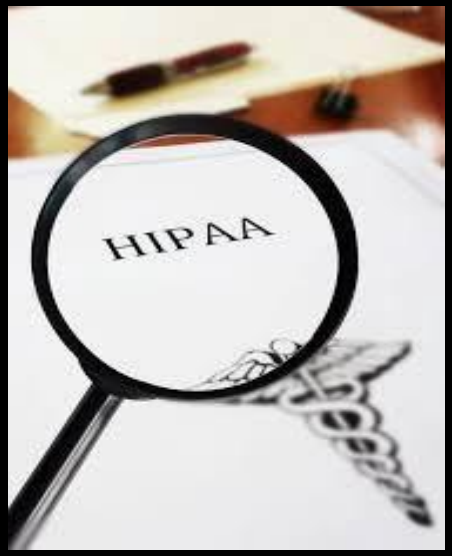
HIPAA Definitions, cont.

- **<u>Protected Health Information (PHI) Data Elements</u>** – identifiers of an enrollee or of relatives, employers or household enrollees of the enrollee including the following:

  - Names
  - Postal addresses smaller than state
  - All elements of dates (except year) such as birth date, admission/discharge date, date of death and all ages over 89
  - Telephone numbers
  - Fax numbers
  - Email addresses
  - Social security numbers
  - Medical record numbers
  - Health plan ID numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers including license plates
  - Device identifiers and serial numbers
  - Web Universal Resources Locators (URLs)
  - Internet Protocol (IP) address numbers
  - Biometric identifiers, including finger and voice prints
  - Full face photographic images and any comparable images
  - Any other unique identifying numbers, characteristics, or codes

To de-identify PHI, all 18 identifiers must be removed and there cannot be <u>any</u> information that can be used alone or combined with other information to identify an enrollee!

PART 2:
HIPAA BASICS



When Can You…

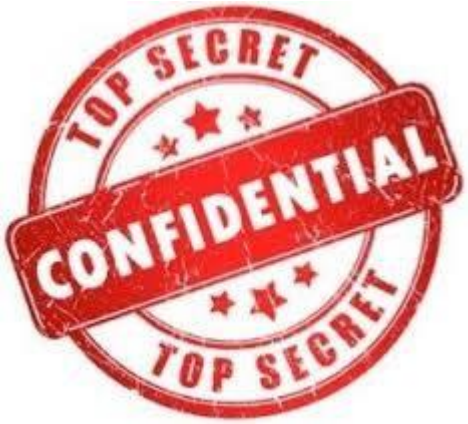
- Access PHI?
- Use PHI?
- Disclose PHI?

ONLY WHEN REQUIRED AS PART OF YOUR CONTRACT WITH AHG!

Accessing or disclosing PHI without a work- related need to know is a violation of HIPAA and carries heavy penalties discussed later in this presentation.

PHI is Highly Confidential!

- PHI can only be accessed, used or disclosed for **Treatment, Payment or Healthcare Operations** (TPO) without an enrollee's authorization.
- Do not discuss PHI with others who do not need to know the information to perform their jobs.
- Do not discuss a enrollee's PHI with your family and friends.
- Do not use your access to look at PHI of a family enrollee/friend unless this is a function of your job.



Treatment, Payment or Healthcare Operations (TPO)

- PHI uses and disclosures allowed for TPO do not require a enrollee's authorization. TPO includes:
  - **T**reatment: Provision, coordination or management of health care for a patient by one or more healthcare providers.
  - **P**ayment: Activities by a health plan to determine responsibilities for coverage under the health plan policy. Also, activities by healthcare providers to obtain reimbursement for the provision of healthcare. Examples of payment include risk adjustments, utilization review activities, reporting to consumer reporting agencies, etc.
  - Healthcare **O**perations: Certain administrative, financial, legal and quality improvement activities of a covered entity (CE) necessary to run the CE's business and to support the CE's core functions of TPO.

Purposes Other Than TPO

- Unless permitted or required by law, any other use or disclosure of PHI requires the enrollee's authorization.
- Examples of uses or disclosures requiring authorization:
  - Disclosures to attorneys/law offices.
  - Requests from medical record companies.
  - Requests from vendors or providers wanting to market their products.
  - Requests from employers.
  - Requests from family enrollees/friends except for the special conditions noted later.

Minimum Necessary Standard

- HIPAA requires that you only ask for, use and disclose the minimum information necessary to accomplish a TPO task.

- This means:
  - Only ask for what you need (be specific - don't ask for all records unless all are required).
  - When disclosing information, only include what is absolutely necessary.
  - When responding to a request for PHI (for a permissible disclosure), only include the specific information

NOTE: Disclosures for treatment of the enrollee are not limited to the minimum necessary standard.

Who Can You Disclose PHI to?

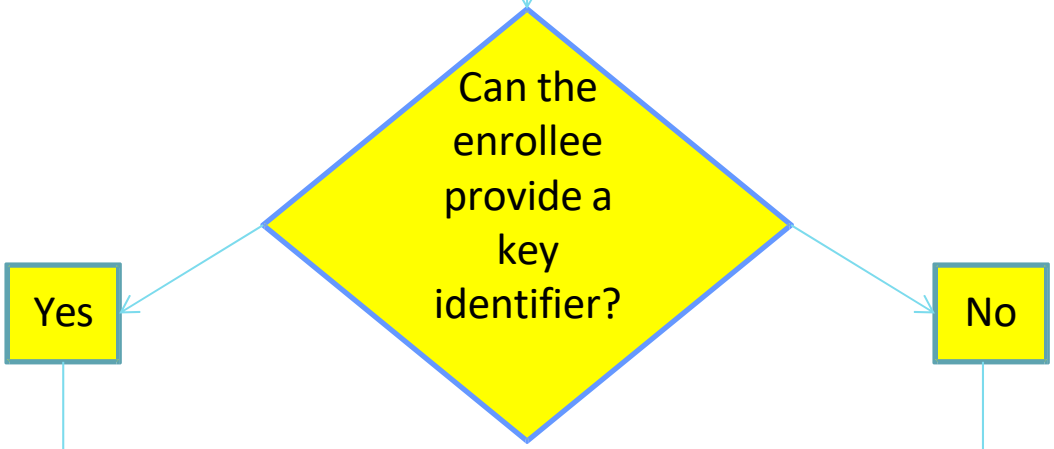
- The enrollee (who is the subject of the PHI).
- The enrollee's Power of Attorney (POA) or Legal Guardian (ordered by the court or protective order).
  - PHI can be disclosed once proof of legal authority is obtained and that specifically authorizes health disclosures.
- The enrollee's Appointed Personal Representative

NOTE: It is important to document ALL PHI disclosures you make!

Always ask for a "key identifier" and at least three (3) forms of identification about the enrollee before disclosing PHI (see next slide).

Trust, But Always Validate!

Before disclosing PHI, always ask for a key identifier about the enrollee and validate the information against what is known to you about the enrollee (e.g., enrollee #, Medicare#, etc.)



Ask the enrollee to <u>also</u> provide the enrollee's:

1. Name;
2. Full mailing address; **<u>AND</u>**
3. Phone number.

Ask the enrollee to <u>also</u> provide the enrollee's:

1. Name;
2. Full mailing address;
3. Phone number; **<u>AND</u>**
4. **<u>Date of birth</u>.**

Remember: Don't disclose the information above, ask for it, then validate it against what you know about the enrollee.

Who Else Can You Disclose PHI to?

If your contract permits, you can also disclose to:

- Providers involved in the enrollee's treatment.
- Public health and governmental agencies, law enforcement officials and other authorities as required by law.

Remember: The enrollee requesting PHI must pass the validation checks mentioned in the previous slide.

Enrollee Permission to Disclose

- You can disclose PHI to anyone the enrollee authorizes in advance as follows:
  - Verbal authorization – must be documented (and documentation must be saved to later to prove that authorization was obtained).
    - Verbal authorizations should be time limited and do not provide a "blanket authorization."
    - You must only disclose what the enrollee authorized and nothing more.
  - HIPAA Authorization Form – the enrollee can complete an authorization form to specify the terms of the authorization. This is not a commonly used form, but is available if a enrollee does not want to appoint a Personal Representative.

What About Emergencies?

- You can disclose PHI to an enrollee's family/friends involved in the enrollee's care in ***emergency situations*** where the enrollee is temporarily incapacitated or unable to agree or object.
- Use your best judgment!
- Document all emergency disclosures (and save the documentation for future reference).

What about Long-Term Incapacity?

- In the event a enrollee becomes long-term incapacitated, PHI can be disclosed to the enrollee's **family** when:
  - The disclosure is to the enrollee's spouse, parent, child, brother, sister or next of kin that is over age 19
  - Requires proof of long-term incapacity (usually, written documentation from the enrollee's PCP)
  - Creates a "blanket authorization"
  - Discuss with the insurance company contact if you have questions!

Enrollee Rights

- Enrollees have the following HIPAA rights and can make the following requests:
  - For confidential communications
  - To access their PHI (in electronic and/or paper form)
  - To amendment to their records
  - For an accounting of disclosures you or AHG has made about the enrollee (excludes disclosures for TPO)
  - To restrict how you and AHG use and disclose their PHI
  - To have a contact assist them with privacy related issues
  - To file a complaint about how you or AHG handled their PHI

PART 3:
HIPAA SAFEGUARDS

What Information Must be Protected?

- All forms of information including:
  - Paper (enrollment forms, copies of Medicare/Medicaid cards, etc.)
  - Electronic data (stored on a laptop, computer, flash drive, - even a cell phone, etc.)
  - Spoken word (voicemail messages, conversations with others, phone calls and discussions in public locations, etc.)
  - Photographs, x-rays, digital images, etc.

PHI must be protected from start (creation/receipt) to finish (storing, saving, transmitting, destruction, etc.)!

Safe Handling of PHI

- **YOU** are responsible for how you handle PHI!
- **YOU** are responsible for your own actions, and will be accountable for how you access, use and share PHI.
- Use good common sense with day-to-day activities. For example:
  - Verify email addresses, fax numbers, and addressed to be sure PHI is sent to the correct recipient!
  - Don't leave PHI unattended and expose PHI to others who may not need to see the information.

Workstation Safeguards

- Lock your screen before walking away from your device!
- Put away PHI at the end of the work day (such as in a locked cabinet) to keep unauthorized individuals from seeing the information.
- Store electronic PHI (e-PHI) on a secure network drive – **not** in a location that is not backed-up (i.e., on your computer's hard drive).

Remember, **you** are responsible for PHI in your possession at all times!

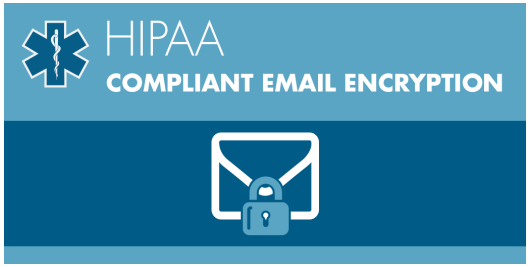
Password Safeguards

- Never share your login or password with anyone (don't ask others for their login or password).
- Use strong passwords that include alphanumeric characters, upper/lower case letters, + special symbols.
- Keep passwords secure.
- Notify AHG immediately if you think your login or password has been compromised.

Remember, **<u>you</u>** are responsible for what happens under your login!

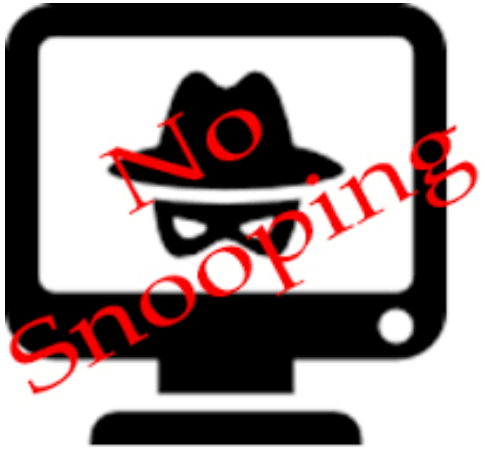
Email Requirements

- Emails with enrollee information MUST be encrypted!
- Avoid emailing large amounts of PHI – use a secure FTP site instead, when possible.
- Phishing emails are one of the biggest threats to organizations…**do not** open, forward or reply to suspicious emails – especially those that have attachments or links!



Access Reminders

- Always be sure you are only accessing records you are permitted to view.
- Accessing PHI or PII without a permissible business reason is a HIPAA violation and results in fines, penalties and contract termination.



Devices MUST be Encrypted

- All devices utilized to transmit or store enrollee information MUST be encrypted

PHI/PII Disposal

- PHI/PII must be disposed of securely when no longer needed.
- Use a HIPAA-compliant shredder that cross-shreds.
- Never dispose of enrollee information in a regular trash bin.

Physical Safeguards

- When presenting to one of our enrollees, wear a badge to clearly identify yourself.
- Take **<u>extra</u>** precautions to protect PHI/PII in the field!
  - Never leave PHI/PII unattended
  - Never store a device containing enrollee information visible in a vehicle (instead, lock it up in the trunk where it is out-of-sight).
  - Always be certain to ask for the enrollee's permission to discuss PHI if others are present and can hear the conversation.
- You must ensure all PHI/PII is protected from being seen or heard by unauthorized enrollees.
  - Unauthorized enrollees includes your family, friends, the general public and any other enrollee not legally authorized to access the PHI/PII.
  - Beware of your surroundings – do not discuss PHI/PII in public locations whenever possible (find a private area instead or lower your voice).

Be Careful Where You Send/Leave PHI

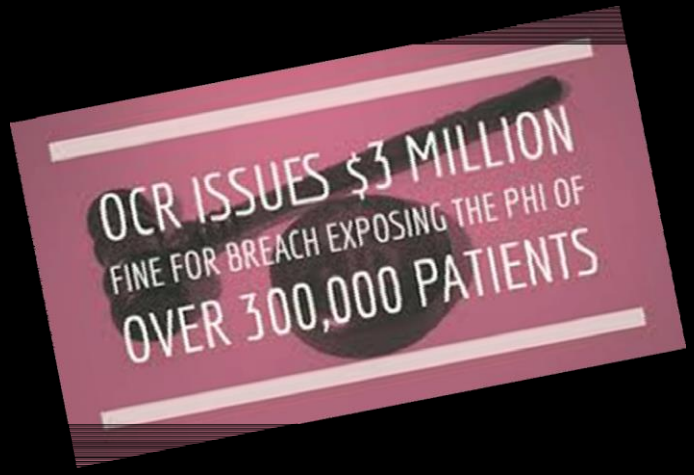
- Slow down!!!
- Misdirected emails and fax numbers can cause a HIPAA breach!
- If an email address or fax number is not clear, verify it first – **do not assume**!

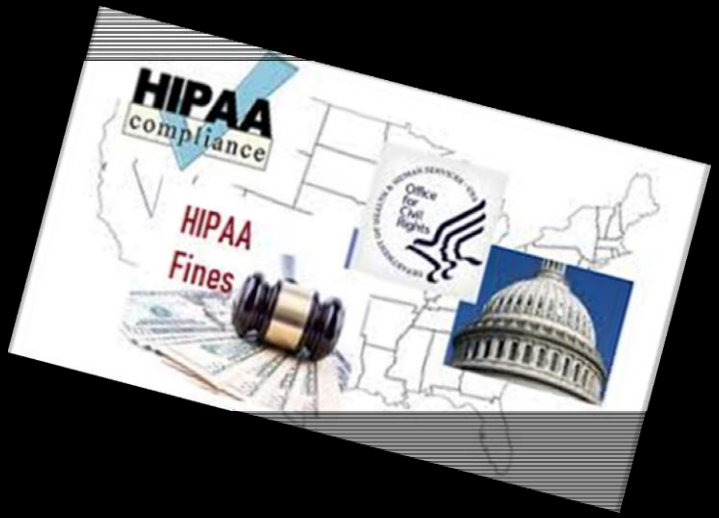
Pictures and Text Messaging

- Do not take pictures of any PHI/PII – this includes pictures on a cell phone, iPad, etc.
- Do not communicate PHI/PII via text messaging.
  - PHI/PII should never be stored locally on your device.

Remember, **<u>you</u>** are responsible for PHI in your possession at all times!

PART 4:
HIPAA INCIDENTS, REPORTING AND PENALTIES

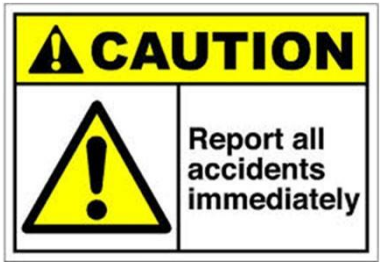




HIPAA Incidents, Reporting and Penalties

- **You** are obligated to take actions to avoid HIPAA incidents.
- **Your** are obligated to **immediately** report any incident that "may" compromise PHI.
  - To report a HIPAA incident or to get help or advice, talk to:
    - Your organization's Privacy Officer, if applicable
    - Your Insurance Carrier contact
    - Insurance Company Privacy Officer
    - Insurance Company Data Security Officer

Incidents must be investigated to determine if the incident is a HIPAA reportable breach.



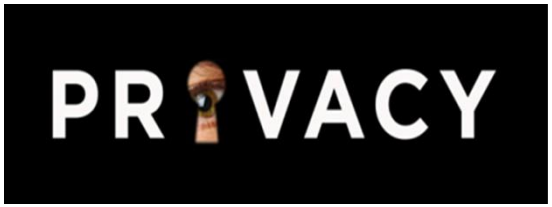
Types of Incidents to Report

- Lost or stolen PHI
- Misdirected mail, emails, faxes, etc. containing PHI
- Lost or stolen electronic devices – if the device contained any PHI/PII (devices should never store PHI/PII)
- Unusual messages shown on your computer that make you question your system's security
- Suspicion of others misusing/abusing PHI
- Any other incident that compromises any enrollee data!

Important: HIPAA laws require you to timely report incidents that could compromise PHI!

HIPAA Incidents Can Be Breaches

- HIPAA Breach - when PHI is “acquired, accessed, used or disclosed” in an unauthorized manner that compromises the security or privacy of the information.
- Breaches can result from:
  - Accessing PHI without a work-related need to know
  - Sharing PHI with those not needing to know
  - Sending emails/faxes/mail to the wrong recipient
  - Loss or theft of records containing PHI



Breaches can occur when you do not take the required precautions when handling enrollee information.

<u>Please handle all enrollee information with care!</u>

Breach Requirements

- If a HIPAA breach occurs, a Business Associate must coordinate with the Insurance Carrier to ensure notification is provided to:
  - Impacted enrollees within 60 days of discovery of the incident
  - The Department of Health and Human Services – HHS (annually or immediately – depending on the # of individuals involved)
  - The local media if 500 or more individuals are impacted
  - The Alabama Attorney General within 45 days of discovery if over 1,000 individuals are impacted

- HHS posts information about breaches at: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Handle all enrollee information with care!

HIPAA Penalties & Enforcement

- The Department of Health and Human Services (HHS) through the Office for Civil Rights (OCR) enforces tiered civil penalties for non-compliance with HIPAA.
  - Monetary penalties range from $117 per violation up to $1.7 million per calendar year
- State attorneys general can also pursue civil suits against persons violating HIPAA.
- The U.S. Department of Justice enforces criminal penalties for non-compliance with the HIPAA Privacy Rule.
  - Criminal penalties for “wrongful disclosure” include fines of $50,000 to $250,000 and up to 10 years in prison.

IMPORTANT: Penalties and fines for non-compliance apply to Agents too!!!

BUT THAT’S NOT ALL…

More Penalties & Enforcement

- **<u>The Privacy Act (5 U.S.C. § 552a)</u>** - a law that establishes controls over what personal information is collected, maintained, used and disclosed by federal agencies.
  - The Privacy Act requires protection of individually identifiable information held by federal and state agencies (e.g., names, social security numbers, or other identifying number or symbol assigned to an enrollee).
  - PII held by these agencies can only be accessed, used and disclosed for TPO purposes (as described previously).
- **<u>Privacy Act penalty:</u>**
  - Charge of a misdemeanor and fined up to $5,000.

IMPORTANT: The penalties above apply to **<u>YOU</u>** as a licensed agent!

More Penalties & Enforcement, cont.

- **Internal Revenue Code (IRC) at 26 U.S.C.A. §§ 7213, 7431 and 26 CFR 301.6103(n)** – Prohibits Social Security information from being willfully accessed or disclosed other than for a TPO function (as defined earlier).
- **IRC Penalties, if convicted:**
  - Unauthorized disclosure to someone not entitled to have it: Imprisonment for up to 5 years, and/or a fine of up to $5,000, plus the cost of prosecuting the case against you (§7213).
  - Unauthorized access: Imprisonment for up to 1 year and/or a fine up to $1,000, plus the cost of prosecuting the case against you (§7231 A).
  - Civil recourse: The person harmed can bring personal action against you. Penalties include a minimum of $1,000 per unauthorized access or unauthorized disclosure. If the person can show they had actual damages greater than $1,000, he/she can receive that plus punitive damages. You would also be responsible for the cost of the action and reasonable attorney fees (§7431).

IMPORTANT: The penalties above apply to **YOU** as a licensed agent!

HIPAA Resources

- Insurance Carrier Resources
  - Reach out to your insurance carrier contact for assistance or with questions
- HHS Resources
  - http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html

This concludes your HIPAA training.

Please contact with any questions.

Now, go and do good!