# ASTRO'S APEX SURVEYOR HIPAA COMPLIANCE TRAINING

Welcome to ASTRO's APEx surveyor orientation covering HIPAA compliance training. HIPAA, which stands for the Health Insurance Portability and Accountability Act of 1996, was a broad statute that addressed a wide variety of topics. This training session will focus on the HIPAA requirements to protect the privacy and security of protected health information, which is referred to as PHI.

We will highlight the aspects of HIPAA that are most relevant to you in your role as a surveyor for the APEx program. In addition, you have received a copy of ASTRO's HIPAA Privacy and Security Policies and Procedures, which will also need to review and follow in the course of your work as an APEx program surveyor. If you have additional questions about HIPAA and how it affects your role as a surveyor for the APEx program, we encourage you to reach out to ASTRO's Privacy Officer at HIPAA@astro.org.

It is important to understand the requirements of the federal HIPAA regulations that protect the privacy and security of protected health information and what information must be protected. Additionally, as a surveyor you must understand how HIPAA regulations affect you and your job, and how you are expected to protect this confidential and sensitive information.

This course is designed to train APEx surveyors on the requirements of HIPAA privacy and security compliance prior to conducting facility reviews. In this course, you will review

- Important definitions in HIPAA;
- How you can and cannot use or disclose PHI;
- Individual rights that patients have with respect to their protected health information;
- How to address breaches of protected health information;
- Safeguards that are in place to protect the privacy and security of protected health information; and
- The requirement to mitigate the harmful effects of any impermissible uses or disclosures of PHI.

## INTRODUCTION

The federal requirements that govern protected health information have evolved through a series of statutes and regulations, beginning with the Health Insurance Portability and Accountability Act of 1996 (or HIPAA). As a health care professional, you are likely aware of the federal requirement to protect the privacy of patients' health care information, which has been in effect since April of 2003. In April of 2005, specific requirements relating to the security of health care information maintained in electronic form were put in place.

The most recent changes to these requirements went into effect in September of 2013 as a result of Congress's passage of the HITECH Act in 2009. These changes were implemented by a regulation that is referred to as the "Omnibus Rule."

Changes enacted as part of the Final Omnibus Rule include changes to HIPAA governing:

- Marketing using protected health information;
- The sale of protected health information;
- Fundraising using protected health information;
- A patient's right to request restrictions on the use or disclosure of his or her protected health information;
- A patient's right to electronic access of his or her protected health information; and
- Most relevant to the APEx program, changes in how business associates are treated under the HIPAA rule.

When the Privacy Rule became effective on April 14, 2003, the goal was to provide a federal rule that established a "floor" with respect to privacy protection for health information. States can always provide stronger protections for patient information. The HIPAA privacy rule limited the ability to use a patient's PHI, except for:

- Uses related to treatment, payment and healthcare operations;
- Uses pursuant to an authorization, which is a specific written statement signed by the patient; or
- Uses for certain other limited circumstances, such as uses that are required by law and uses for certain public policy reasons.

It also provided individuals with certain rights relating to their protected health information.

The HIPAA Security Rule, which became effective in April 2005, established national standards to protect individuals' electronic protected health information. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

HIPAA is enforced by the Department of Health and Human Services' Office for Civil Rights. In general, the government seeks civil monetary penalties for violations of HIPAA, which we will discuss in more detail on the next slide.

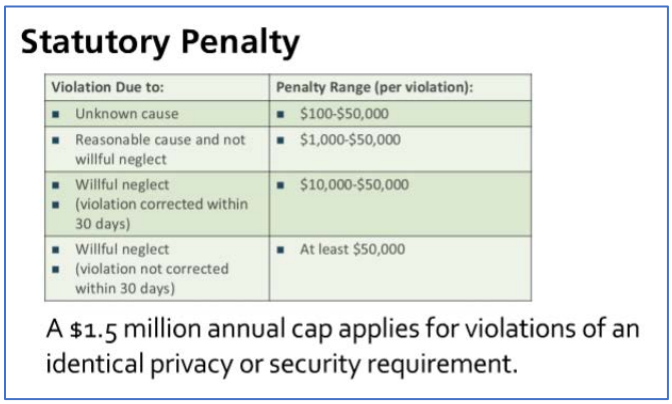
Congress has directed HHS to share penalties with the individuals whose protected health information has been improperly disclosed. This program is not yet in place but was included as part of the HITECH Act.

For egregious behavior, such as selling protected health information, HHS may impose criminal penalties, including potential prison terms.

In addition, State Attorneys General now have the power to enforce HIPAA if they feel that their citizens' rights are being violated under HIPAA.

Finally, HHS has an audit program to audit covered entities and business associates. The audit program is funded by the civil penalties the agency collects for HIPAA violations.

HIPAA violations carry federal civil monetary penalties that vary based on the intent of the person or entity committing the violation. These penalties range from $100 to more than $50,000 per violation with a maximum annual penalty of $1.5 million for identical privacy or security violations.




As you can see from this chart, violations on the low end of the scale are violations for "unknown causes" – in other words, if you did not know or reasonably had no basis for knowing that a HIPAA violation had occurred. On the high end of the scale are violations due to willful neglect, meaning the violation was made as a result of a conscious, intentional failure or reckless indifference to the obligation to protect patient information.

While the penalties are capped at $1.5 million per violation of an identical requirement, keep in mind that a violation of one provision of HIPAA may also be a separate violation of another provision of HIPAA, which can lead to aggregate penalties for the same activity above the $1.5 million annual cap.

In recent years, HHS has increased its enforcement of HIPAA violations. In addition to penalties imposed by the government, HIPAA violations can affect a health care provider's or business associate's professional reputation and business. They can also undermine a patient's trust in their health care provider. The government takes these violations seriously and you should, too.

## DEFINITIONS

The following slides provide definitions for key terms used in HIPAA.

A **covered entity** is:

- Any health care provider who transmits health information electronically in connection with certain transactions, many involving billing and claims;
- Health Plans (including public, private, self-insured or insured plans); and
- Health care clearinghouses (including billing services, repricing companies, and other health information systems).

A **business associate** is an entity that creates, receives, maintains or transmits protected health information on behalf of a covered entity.

Certain types of service providers are specifically enumerated in the regulations, including lawyers, actuaries, consultants and accrediting bodies. Subcontractors of business associates are also considered to be business associates under HIPAA.

ASTRO, as an accrediting body, is a business associate of each of the covered entities it accredits. ASTRO's surveyors are subject to the requirements of HIPAA as members of ASTRO's workforce. Additionally, as a surveyor, you are subject to ASTRO's HIPAA privacy and security policies and procedures. This training is aimed at helping you understand your obligations under HIPAA. Additional information about your duties and obligations under HIPAA are included in APEx's Surveyor Manual, ASTRO's HIPAA policies and procedures – which you received prior to beginning this training – and in the provisions of your Surveyor Agreement with ASTRO.

The relationship between a covered entity and a business associate is spelled out in a contract referred to as a "business associate agreement." The contract specifies and limits how a business associate can use and disclose protected health information. A business associate may ONLY use or disclose protected health information as permitted or required by its business associate agreement with the covered entity or as required by law.

The HIPAA privacy and security rules require you to protect a patient's protected health information, or PHI.

**PHI** is defined as individually identifiable health information which is in the possession of a covered entity or business associate. This is health information (which includes demographic information like date of birth or address) relating to:

- An individual's past, present or future physical or mental health conditions;
- The provision of health care; or
- Payment for the provision of health care.

The information is of the type that does - or may - identify the individual.

It can be maintained in any form, including oral, written or electronic. Electronic protected health information includes electronic storage media (such as computer hard drives and removable digital memory media) as well as transmission media such as the internet. Protected health information can also be contained in items such as videos, photographs, and x-rays.

As mentioned above, this is information in the possession of a covered entity or business associate. If, for example, a doctor's note is in the hands of a patient's employer to verify a leave of absence, it is not protected health information because it is not maintained by a covered entity or business associate.

As the result of a new change to the HIPAA requirements, protected health information does not include individually identifiable health information about individuals who have been deceased for more than 50 years.

As a surveyor, you may be exposed to various types of PHI through your work with medical records and as you spend time observing the operations of a health care provider. The information provided in this training is intended to help you understand the rules governing how you can use and disclose protected health information.

## USE AND DISCLOSURE

There are several ways that a covered entity or business associate may use and disclose protected health information.

Protected health information can always be shared with the individual who is the subject of the PHI.

It can also be used to carry out treatment, payment or health care operations. The term "health care operations" covers a broad range of activities, including quality assessment and improvement activities, patient safety activities and accreditation.

In carrying out treatment, payment and health care operations, a covered entity may share protected health information with a business associate and members of the business associate's workforce. For example, health care providers that are being surveyed by ASTRO as part of the APEx program can disclose PHI to ASTRO and members of its workforce, including surveyors, because the purpose of the disclosure is for accreditation, which is part of the provider's health care operations.

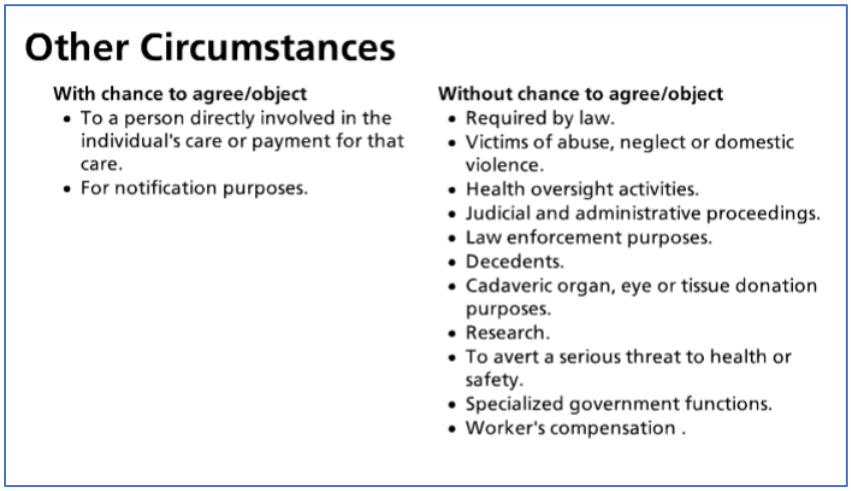
A covered entity or business associate may use or disclose PHI "incident to" an otherwise permitted use or disclosure. For example, while you are performing an on-site survey, you may be exposed to protected health information unrelated to your role as a surveyor. This could include overhearing conversations or viewing protected health information in the location where you are

working. Under HIPAA, this is still considered a permitted use as long as the covered entity is complying with its obligations to put in place safeguards to protect its patients' protected health information and to limit your exposure to protected health information to the minimum necessary to perform your job (as discussed later in this training). Keep in mind, however, that as a business associate of the covered entity, you are obligated to keep that information confidential and to not use or further disclose the information.

Protected health information may also be used or disclosed pursuant to an authorization signed by the patient who is the subject of the PHI.

In addition, there are a number of other specific circumstances in the HIPAA law and regulations where protected health information may be used or disclosed.

Those specific circumstances (listed below) include disclosures required by law or those related to public health or safety.




If you have any questions relating to uses or disclosures of protected health information in your role as a surveyor, please contact ASTRO to discuss the matter further.

As referenced previously, the **"minimum necessary standard"** in HIPAA is an important concept. It states that, in general, disclosures of protected health information must be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Covered entities must develop policies and procedures to implement the minimum necessary standard for routine uses and disclosures of PHI.

"Minimum necessary" policies must address ways to limit the scope of information used or disclosed and the individuals who may use or disclose PHI. Access to PHI should be limited to workforce members who need access to carry out their duties. For example: a billing clerk may need to know what laboratory test was done in order to properly submit the claim for payment, but would not need to know the result of the test.

If possible, uses and disclosures of PHI should be limited to a "limited data set," which is PHI stripped of specific direct identifiers.

Criteria must be established to evaluate non-routine requests for protected health information. In such cases, these requests should be addressed in consultation with an organization's HIPAA Privacy Officer.

There are a number of important exceptions to the minimum necessary requirement. Most importantly, it does not apply to uses or disclosures of protected health information for treatment purposes. In addition, it does not apply to disclosures to the individual who is the subject of the protected health information, disclosures made pursuant to a valid authorization, or other disclosures to the Department of Health and Human Services, those required by law or by other provision of the Privacy Rule.

As a surveyor abstracting data from medical records, you should only be looking for the specific information needed to fulfill your obligations as a surveyor, as spelled out in your Surveyor Manual. Be aware that each facility may have additional minimum necessary policies and procedures that may affect your activities on-site. These policies and procedures should be discussed in your pre-survey teleconference.

The HIPAA regulations allow uses or disclosures of protected health information that are not otherwise permitted or required by HIPAA as long as the uses or disclosures are pursuant to a valid authorization.

The authorization must be signed by the patient and meet other specific requirements spelled out in the regulations. As a surveyor, this aspect of the HIPAA regulations is unlikely to affect you or your work.

HIPAA prohibits the sale of protected health information, which is broadly defined to include disclosures where a covered entity or business associate directly or indirectly receives remuneration in exchange for disclosing PHI.

There are a number of exceptions to this rule. Most relevant for APEx and its surveyors, the sale of protected health information does not include payment to a business associate for activities it undertakes on behalf of a covered entity.

As an APEx surveyor, you should not be in a position to receive payment in exchange for protected health information. If any situations arise that raise questions about this topic, please contact ASTRO's Privacy Officer.

## INDIVIDUAL RIGHTS

The HIPAA rule outlines a number of rights available to individuals with respect to their protected health information. These right generally place obligations on health care providers that are covered entities. While they will not be directly applicable to you in your role as an APEx surveyor, individual rights are an important part of HIPAA. If you encounter an individual trying to exercise his or her rights in the course of your work with APEx, you should direct them to the covered entity.

An individual may request to **inspect or copy** their protected health information. Under limited circumstance, the covered entity may deny a patient's request, but in general, such requests will be granted. The protected health information should be produced in the form and formatted requested by the patient. If it is not readily producible in the requested form or format, the organization must provide the patient with a readable hard copy form, or other form as agreed to by the organization and the patient. If the information is maintained electronically and the patient requests an electronic copy, the covered entity is required to produce it electronically, either in the form and format requested by the individual if it is readily producible and, if not, in a mutually agreed upon electronic form and format. A reasonable, cost-based fee can be charged for copies of protected health information.

An individual also has the right to have a covered entity **amend** protected health information – for example, to correct incorrect information. A covered entity may deny an individual's request in certain circumstance but the individual must be allowed to submit a statement disagreeing with the denial to be included in their record.

An individual has the right to receive a **list of certain disclosures** of their protected health information made by a covered entity and its business associates over the prior 6 years. However, covered entities and business associates do not need to account for or report certain disclosures, including:

- Disclosures for treatment, payment, and health care operations;
- Disclosures made pursuant to an authorization; and
- Incidental disclosures.

Eventually, individuals will be entitled to receive an accounting of all disclosures of their protected health information made through electronic health records in the prior 3 years, including disclosures for treatment, payment and health care operations. The regulations implementing that right have not yet been finalized.

An individual also has a right to request that the use or disclosure of their protected health information **be restricted**. For example, a patient may request that their PHI be communicated in an alternative way or to an alternative location. In general, a covered entity is not required to agree to this type of restriction but if it does agree, the restriction must be honored.

Under new rules that went into effect in September of 2013, health care providers are generally required to grant a request for restriction when it relates to disclosure of protected health information to a health plan for payment or health care operations and the individual has chosen to pay for the service in full out of pocket.

## BREACHES

HIPAA requires covered entities and their business associates to provide notification to certain parties following a breach of unsecured protected health information.

Unsecured protected health information is PHI that has not been rendered unusable, unreadable or indecipherable. HHS considers protected health information to be secured – and therefore not to trigger the breach notification requirements – if it has been encrypted or destroyed consistent with federal guidelines. An improper use or disclosure of PHI that has not been encrypted or destroyed should be analyzed as a potential breach.

A breach is, generally, an impermissible use or disclosure of protected health information under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

The following types of uses or disclosures of protected health information are specifically excluded from the definition of a breach:

- An unintentional acquisition, access or use of protected health information by a workforce member, if the access or use was in good faith and within scope of authority, and no further use or disclosure is made. For example, if a workforce member inadvertently views the wrong patient's medical record but does not further use or disclose that information, a breach has not occurred. If, however, a workforce member intentionally snooped in the medical record of a patient, that may be a breach.
- It is also not a breach when an inadvertent disclosure of protected health information is made to a colleague who is also authorized to access the PHI, and the PHI is not further used or disclosed.
- Finally, it is not a breach when protected health information is disclosed where there is a good faith belief that the person receiving the PHI would not be reasonably able to retain the information disclosed.

When a breach does occur, it is the business associate's duty to notify the covered entity.

- Depending on the business associate agreement between the covered entity and the business associate, the business associate may notify individuals of the breach.
- Certain information about the breach must be provided to the individuals and other parties who must receive notice
- **As an APEx surveyor, if you suspect that protected health information may have been breached, please notify the ASTRO Privacy Officer immediately.**

The covered entity is responsible for notifying certain parties, including:

- The individuals affected by the breach. However, as already mentioned, the business associate agreement between the covered entity and business associate may require the business associate to notify the individuals about the breach instead of the covered entity.
- The covered entity must also notify the Department of Health and Human Services.
- If the breach affects fewer than 500 individuals, the covered entity can report it to HHS annually. Notification is required within 60 days after the end of the calendar year.
- If the breach affects 500 or more individuals, the notification to HHS will be at the same time the covered entity notifies the individuals. For these bigger breaches, HHS will post information about the breach on its website.
- Finally, when the breach affects more than 500 residents in the same jurisdiction, the covered entity is also required to notify the media.

Notice to individuals affected by a breach must include:

- A brief description of the breach, including the date of the breach (if it is known)
- A description of the types of protected health information that were involved in the breach
- The steps that affected individuals should take to protect themselves from potential harm
- A brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as
- Contact information for the covered entity (or business associate, as applicable) where individuals affected by the breach can ask questions or learn additional information.

Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

In certain circumstances, the notice may need to be translated into the patient's native language.

The breach notification rule requires covered entities to notify individuals of a breach without unreasonable delay and no later than 60 days after discovery of the breach, even if the investigation is ongoing.

As a business associate, ASTRO is required to notify the sites of any breach under the same standard, without unreasonable delay and no later than 60 days after discovery of the breach, even if the investigation is ongoing.

Discovery is the first day on which the breach is known – or by **exercising reasonable diligence** would have been know – to an employee, officer or agent.

As a surveyor for ASTRO, you will not be providing notification of a breach directly to a covered entity. If you suspect that protected health information may have been breached, please notify ASTRO's Privacy Officer immediately.

## SAFEGUARDS

As required by the HIPAA privacy rules, ASTRO has put in place a number of requirements to safeguard PHI.

ASTRO has appointed a Privacy Officer to develop and implement ASTRO's privacy policies.

ASTRO trains its workforce and certain other parties on these policies, including you as a surveyor for the APEx program.

As part of its policies, ASTRO has incorporated administrative, technical and physical safeguards to protect the privacy of protected health information that may be received by ASTRO.

ASTRO will not retaliate against or intimidate any individual who exercises his or her rights under HIPAA or brings a complaint against a covered entity or business associate.

- Applies to PHI that is transmitted or maintained in electronic media (ePHI)
- Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of ePHI
- Flexible approach
- Facility-specific polices will be discussed prior to on-site survey
- Data surveyors enter into the APEx portal is de-identified PHI, meaning key patient identifiers have been removed
- Surveyors must not enter individually identifiable patient information into the APEx portal.

In addition to these policies addressed in the HIPAA Privacy Rule, ASTRO also has policies pertaining to the **Security Rule**. The Security Rule governs electronic protected health information, which is PHI transmitted or maintained in electronic media. Covered entities must implement administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic PHI.

The Security Rule will apply to your access to electronic health records at the facilities you survey. Each facility will have its own HIPAA Security policies and procedures.

Each facility's specific security measures that will affect your work as an APEx program surveyor at that facility, and should be discussed in your pre-survey teleconference.

ASTRO does not anticipate that any of the data you collect or store in the surveyor portal as part of your site visit will include electronic PHI subject to the Security Rule. This is because ASTRO limits the collection of data regarding patients of the facilities that apply for accreditation. As a surveyor, you will be answering "yes" and "no" questions about what you see in the facility's electronic health records. The information you will be recording in the portal is considered "de-identified information." In other words, under HIPAA, the data would not be considered PHI. You should not enter any individually identifiable patient information into the portal. Even though ASTRO does not anticipate that ePHI will be stored or transmitted in the APEx portal, ASTRO's policies were developed

to comply with the Security Rule. If you have further questions about the HIPAA Security Rule, you may contact ASTRO's HIPAA Security Officer at HIPAA@astro.org.

## MITIGATION

Covered entities and business associates have a duty to mitigate, "to the extent practicable," any harmful effects due to uses or disclosures of protected health information in violation of the regulations or their own policies.

After an investigation by the Privacy Officer, efforts will be made to mitigate the risk of the impermissible use or disclosures, which may include:

- Asking the inappropriate recipient to destroy the PHI;
- Informing the recipient and asking them to refrain from further disclosure – which may involve asking them for a confidentiality agreement;
- Notifying the individual who is the subject of the PHI; and
- In some cases, notifying the media.

All members of ASTRO's workforce, including surveyors, must fully cooperate with any investigation, corrective action, sanctions or efforts to mitigate.

## RETENTION AND DESTRUCTION

The HIPAA rules require that all of the documents required by HIPAA be retained for six years. This includes documents such as policies and procedures, business associate agreements and authorizations.

HIPAA does not dictate how long medical records must be retained. Medical record retention is governed by state law and other considerations.

HIPAA requires that the administrative, technical and physical safeguards that are necessary to protect the privacy of medical records or other protected health information be in place for as long as the information is maintained and through its disposal.

While the HIPAA rules do not require a particular method of disposal, HHS has provided guidance on appropriate methods. For paper records, appropriate disposal may be through shredding, burning, pulping or pulverizing the records.

For electronic media, appropriate disposal methods include clearing (meaning to overwrite the media with non-sensitive data), purging (meaning to degauss or expose the media to a strong magnetic field to disrupt the recorded magnetic domains) or destroying the media through disintegration, pulverization, melting, incinerating, or shredding.

ASTRO's HIPAA policies and procedures you received prior to beginning this training contain ASTRO's policy for destruction of electronic PHI.

## SANCTIONS

HIPAA requires covered entities and business associates to have a policy in place to sanction any employee or workforce member who violates the HIPAA Privacy Policies and Procedures.

Depending on the infraction, sanctions may include:

- Retraining;
- Warnings (verbal and/or written);
- Suspension;
- Demotion; and
- Termination.

No sanctions will be imposed on whistleblowers who come forward to report concerns about HIPAA compliance.

ASTRO's sanctions policy is included in the HIPAA policies and procedures you received prior to beginning this training.

## COMPLAINTS

Surveyors should feel comfortable reporting any concerns or complaints regarding health information privacy or security issues to ASTRO's Privacy Officer. The Privacy Officer will investigate all complaints that he or she receives, and will keep his or her investigation in confidence, to the extent possible.

## QUESTIONS?

Contact ASTRO's HIPAA Privacy Officer if you have any questions about HIPAA.

**ASTRO Privacy Officer**
251 18th Street South, 8th Floor
Arlington, VA 22202

HIPAA@astro.org
703-839-7300