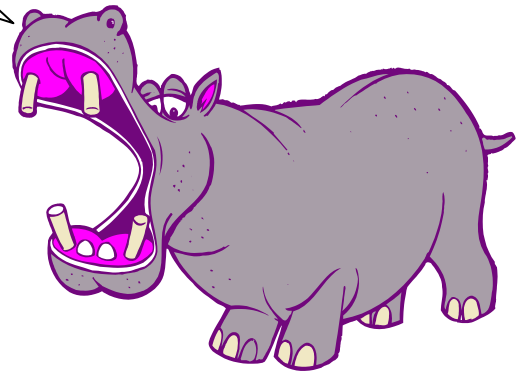




HIPAA Privacy Rule Training Materials

Protecting our patients' privacy is EVERYONE'S responsibility!



The HIPAA Privacy Regulations went into effect in April 2003. Generally speaking, protecting the privacy of a patient is not a new concept for those working in the health care industry. Professional standards have always promoted confidentiality as a critical aspect of the patient/care giver relationship. HIPAA now makes this longstanding practice a conscious effort because it requires formalized policies and procedures as well as training.

Introduction to ENT and Allergy Associates Privacy Training

The objective of this training session is to give you an overview of our regulatory obligations and policies governing patient privacy. It will help you to understand our expectations for maintaining our patients' privacy and give you some common sense guidelines to help you apply the policies to your work.

At the end of the lesson there is a short quiz to assess your understanding of the privacy rules.

What is HIPAA?

Health Insurance Portability and Accountability Act of 1996

The Federal regulations generated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) give patients more control over their health information by establishing certain rights related to their health information and setting limits on how we can use and disclose that information.

USE: the sharing, employment, application, utilization, examination or analysis of individually identifiable health information **within** an entity that maintains that information.

DISCLOSURE: the release, transfer, provision of access to, of divulging in any other manner of information **outside** the entity maintaining the information.

Who Does it Affect and Who is Accountable?

Individuals and entities that are covered by the HIPAA privacy regulations are defined as "Covered Entities." There are three types of Covered Entities regulated by the HIPAA rules:

- Health Plans- who pay for medical care and/or services (including Medicare & Medicaid)
- Healthcare Providers who provide medical care and submit claims for payment electronically
- Clearinghouses- we use one to facilitate the movement of electronic claims from our billing system to the payer.

Anyone who has access to or knowledge of PHI is accountable under HIPAA. As employees of a physician practice we are ALL accountable under HIPAA to protect individually identifiable health information. Under HIPAA this is called "Protected Health Information" or PHI.

Protected Health Information (PHI): In general, means individually identifiable health information that is:

- Transmitted by electronic media (claims submissions)
- Maintained electronically (billing system, EMR)
- Transmitted or maintained in any other format (charts, EOBs)

PHI comes in many forms, many of which will be found outside of the patient's medical record.

Examples of PHI include:

- **Clinical Information** – test results, diagnoses, progress notes, images, names and specialties of physicians or other care providers.
- **Financial Information** – health insurance coverage, itemized bills and charges, EOBs.
- **Demographic Information**- Name, address, social security number, dates of service, date of birth, age.

Uses and Disclosures of PHI

1. General Rule

A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by a covered entity. In general, we may not use or disclose PHI except as permitted or required by the privacy regulations. There are several general categories of required and permitted uses and disclosures which are also explained in the Notice of Privacy Practices.

a. Required Disclosures

- i. To an Individual who is the subject of the PHI.
- ii. Upon request to the Department of HHS when conducting an investigation or compliance review.

b. Permitted Uses and Disclosures

- i. **Treatment, Payment and health care Operations (TPO).** Either for our own or for another health care provider's treatment and payment activities provided that provider has a relationship with the patient at issue and the PHI pertains to that relationship.
- ii. Pursuant to a valid authorization unless use or disclosure is otherwise permitted by the privacy regulations.
- iii. To persons involved in the individual's care (family members, relatives and close personal friends) only the PHI directly relevant to their involvement with the individual's care or payment for such care.
- iv. Miscellaneous uses and disclosures. There are several situations listed in the Notice of Privacy Practices in which PHI may be used or disclosed without an authorization or the agreement of the individual (i.e. required by law, for public health purposes, health oversight by a public agency, certain legal proceedings).

2. Minimum Necessary Rule (P&P RA007)

We are required to make reasonable efforts to limit PHI used or disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This rule does not apply to:

- disclosures to or requests by *a healthcare provider for treatment*;
- uses or disclosures *to the individual*;
- uses or disclosures made *pursuant to a HIPAA compliant authorization*;
- disclosures made *to the Secretary of HHS*;
- uses or disclosures that *are required by law* (i.e. in response to a court ordered subpoena); and
- uses or disclosures as required for *compliance* with the HIPAA Privacy Rule.

Role based access to the computer network and billing system. Role based access means that each workforce member is only provided access to the minimum level necessary to perform his or her job duties. That is one reason why it is important that users do not share their passwords and that they either log off, or lock, their computer when stepping away for any extender period of time.

Minimum Necessary Rule: Reasonable efforts must be made to limit the amount of protected health information (PHI) to the minimum necessary to accomplish the stated purpose of the use, disclosure or request unless the use or disclosure is exempt from the minimum necessary policy.

3. Authorizations (P&P RA002)

Authorizations to release PHI must be reviewed to ensure that they contain the core items and statements as required by the privacy regulations. Authorizations that contain all of the necessary items and statements but are incomplete are not valid and cannot be acted upon. The HIPAA Authorization Checklist provides guidance for ensuring an authorization is valid.

Each practice location has a person designated to review authorizations received and to ensure that any use or disclosure of PHI is consistent with the authorization. Any question regarding the validity of a specific authorization should be directed to the Privacy Officer.

4. Telephone Disclosures

There are many times in which it is necessary to communicate with a patient or to respond to requests for a patient's PHI using the telephone. Therefore, it is necessary to make a reasonable effort to confirm the identity of the people to whom PHI is disclosed over the telephone.

- a. Limit, to the extent practicable, the PHI communicated over the telephone.
- b. If the caller is stating he/she is the patient and is requesting PHI about himself/herself confirm the identity by:
 - Asking the caller to confirm at least three items from the verification list below; or
 - Place a return call to the patient using the telephone number documented in the patient's file.

- c. If the caller is not the patient and states he/she is an immediate family member (i.e. father, mother, child, sibling) use professional judgment to discern whether any disclosure is appropriate. Also,
 - Ask the caller to confirm at least three items from the verification list below; or
 - When necessary, ask the physician to advise whether disclosure is approved.
- d. If the caller states he/she is a friend, relative or acquaintance of the patient, or if the caller is unrelated to the patient (employer, policeman) do not disclose PHI without the patient's authorization.

Verification List:

This list includes, but is not limited to, information about a patient that can be requested from a caller to confirm their identity as a patient. At least three of these items should be requested from the caller to reasonably confirm his/her identity.

- Date of Birth
- Telephone Number
- Address
- Social Security Number
- Insurance information (name, ID #, group #)
- Date of Service
- Physician Name
- Services Received

Administrative Requirements

In response to the HIPAA regulations, ENT and Allergy has implemented or updated policies to meet the requirements, many of which relate to the Administrative Requirements. These policies will be revised as necessary to comply with changes in relevant law and, if changes also affect the practices stated in our Notice of Privacy Practices, this will be changed as well. The Administrative Requirements address the following areas and policies:

1. Designation of a Privacy Officer.

ENT and Allergy Associates has designated the Director of Regulatory Affairs as the Privacy Officer. Any questions or concerns regarding how ENT and Allergy Associates complies with the HIPAA Privacy Regulations should be directed to this person. The Privacy Officer will conduct investigations on any reports of non-compliance with either HIPAA regulations or the policies and procedures of the Compliance Program.

2. Complaint Process (P&P RA006)

HIPAA establishes the right of any person to file a complaint either directly with ENT and Allergy Associates (a covered entity) or with the Secretary of Health and Human Services. We have a written policy that provides direction to employees in the event that a patient does want to make a complaint. In general, patients should be directed to speak to the Privacy Officer who will document and investigate the complaint to ensure resolution where necessary.



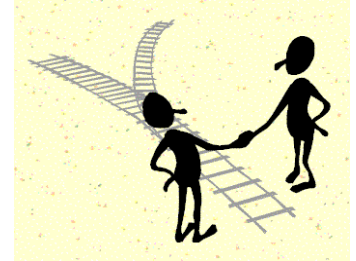
3. Documentation



ENT and Allergy Associates has documented all policies and procedures related to the HIPAA Privacy Rule in writing and/or electronic form. All documentation related to compliance with the HIPAA Privacy Rule must be maintained for a minimum of six years. This includes any changes to policies, procedures or practices. The policies and procedures are identified by the prefix “RA” and are located in each office location.

4. Mitigation (P&P RA008)

ENT and Allergy Associates will mitigate, to the extent practicable, any harmful effect that is known to us of a use or disclosure of PHI in violation of any policies and procedures or any other requirements under the HIPAA Privacy Rule. It is our responsibility to mitigate regardless of whether the privacy breach was caused by a workforce member, a contractor, or business associate since the potential harm to the individual is the same in all cases.



5. Sanctions (P&P RA014)



All workforce members are required to abide by the policies and procedures that ensure compliance with the HIPAA Privacy Rule as well as any other laws or regulations relevant to our practice. Failure to do so will result in disciplinary action as described in the Employee Handbook. The nature and severity of the discipline will be determined by ENT and Allergy Associates in its sole discretion and will reflect the severity of the violation, the employee’s past record, and other individual circumstances.

Additionally, employees have a duty to report any perceived or known violation of the HIPAA Privacy Rule, Compliance Program or other relevant policies and procedures. The Compliance Hotline provides a mechanism for employees to make such reports anonymously. Employees making good-faith reports will not be retaliated against. Furthermore, ENT and Allergy Associates will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual and others who:

- file a complaint with the Secretary of HHS;
- testify, assist, or participate in an investigation, compliance review, proceeding, or hearing related to a violation under HIPAA;
- oppose any act or practice made unlawful by the HIPAA Privacy Rule, provided the individual or person has a good faith belief that the practice is unlawful, and the manner of the opposition is reasonable and does not involve disclosure of PHI in violation of the HIPAA Privacy Rule.

6. Safeguards (P&P RA013)

Administrative, technical and physical safeguards are utilized to reduce the risk of unintended disclosures of PHI. As a consequence of other permitted uses and disclosures there is some risk of secondary uses and disclosures that may occur. These are permitted as long as reasonable safeguards have been undertaken to limit the secondary use and disclosure to the minimum necessary.



Incidental Disclosures: Secondary uses & disclosures that cannot reasonably be prevented, are limited in nature, and that occur as a byproduct of an otherwise permitted use and disclosure.

Such uses and disclosures are **permitted as long as reasonable safeguards have been undertaken** to limit the use and disclosure of the PHI to the minimum necessary.

Risks:

- Conversations at nurse's stations, front desks, hallways, etc.
- Documents containing PHI in view
- Computer monitors in view

- Printers in public view

- Fax machines

- Disposal of documents and electronic media

Safeguards to Reduce Risk:

- ✓ Lower voice, better manage patient flow
- ✓ Keep documents in folders
- ✓ Turn monitors away or use privacy screen
- ✓ Keep printers in secure area
- ✓ Call ahead before faxing, check fax number before dialing, review fax confirmation sheet.
- ✓ Shred documents and dispose of electronic media appropriately

Disposal of PHI (P&P RA004)



All workforce members need to take reasonable precautions to dispose of any PHI securely regardless of its format. This includes a Post-it note with a patient name and date of service or account number on it. Shredders and/or shredder bins are located in all office locations. **All PHI maintained in paper format must be shredded before disposal. PHI should NEVER be discarded in trash bins.**

PHI that is maintained in electronic format (i.e. CD, floppy disk or PC) must be securely destroyed before disposal. The IT Department will advise as to the proper method of destruction of PHI maintained in this format.

Fax Transmittals (P&P RA005)

One might expect fax transmittals are relatively benign and simple tasks but there is some degree of risk of an unauthorized disclosure of PHI when sending a fax. It is important to take reasonable safeguards to ensure that the faxed PHI is received by the intended person. This can be done following some simple precautionary measures.

- All faxes containing PHI must be sent with a FAX Cover Sheet that includes the Approved Confidentiality Notice even if faxed within the practice.
- Preprogram frequently used fax numbers in the fax machine to prevent misdialing numbers.
- Periodically check that preprogrammed fax numbers are current.
- Verify the fax number of the recipient before faxing.
- Check the fax confirmation sheet to ensure the correct number was dialed.



In the event that a fax is misdirected it is imperative that the unauthorized disclosure be mitigated. The goal is to ensure that the unintended recipient destroys the information. Fax Shredders and/or shredder bins are located in all office locations. a note to the unintended recipient requesting that the entire content of the misdirected fax be destroyed.

7. Training

Training will be provided to all members of the workforce to allow for them to appropriately carry out their functions. New employees will be provided training within a reasonable time after joining ENT and Allergy Associates. Documentation of training is kept on file in the Department of Regulatory Affairs.



Individual Rights

HIPAA provides patients certain rights which are reflected in ENT and Allergy Associates policies and procedures. These rights are discussed briefly below. Please refer to the relevant policies for more specific information.

1. Inspect and Copy

Individuals have the right to inspect and obtain a copy of PHI about the individual for as long as the PHI is maintained by ENT and Allergy Associates. In general this right is also granted by both New York and New Jersey law. ENT and Allergy Associates will provide such access to patients' while abiding by the limits of the relevant state and federal laws.



2. Receive a Notice of Privacy Practices. (P&P RA009)



ENT and Allergy Associates provides all new patients with a copy of the Notice of Privacy Practices upon their first visit. We make a good faith effort to receive written acknowledgement of receipt of the Notice. The Notice is provided in English and Spanish in all office locations as well as our website.

3. Request for Amendment (P&P RA010)

An individual has the right to request an amendment to their PHI. Individuals making such requests are to be referred to the Privacy Officer. All such requests must be made in writing. We may deny an individual's request for amendment if it is determined that the PHI or record that is the subject of the request:

- was not created by ENT and Allergy Associates (unless it is reasonable to believe the creator is no longer available to act on the request)
- is for information that is not a part of the designated record set;
- would not be available for inspection under state or federal law;
- is accurate and complete.

4. Request for Confidential Communications (P&P RA011)

ENT and Allergy Associates will accommodate any reasonable request for confidential communication. We will not require an explanation of the reason for the request. We can only require that the request be reasonable, that is it in writing and that it specify an alternative address or method of contact.



The reasonableness of the request must be determined solely on the basis of administrative difficulty or complying with the request. A request will not be refused based on our perception of the merits of the individual's reason for making the request.

5. Request for Restriction of Uses and Disclosures (P&P RA012)

Individuals have the right to request a restriction of the use or disclosure of PHI for treatment, payment or health care operations. We are not required to agree to a restriction, however, if we do agree the restriction must be honored practice wide with two exceptions:

- it is terminated by either party. If the individual agrees to terminate the restriction, we may use or disclose the PHI as otherwise permitted under HIPAA. If the individual disagrees to the termination, we may only terminate the restriction with respect to PHI created or received after the date the individual is informed of the termination.

- In an emergency treatment situation we are allowed to use or disclose PHI to a health care provider for providing treatment.

6. Accounting of Disclosures (P&P RA001)

Individuals have the right to request a log of all tracked disclosures made by ENT and Allergy Associates. This includes within the six years prior to the date of the request. Requests for an accounting of disclosures should be submitted in writing to the Privacy Officer.

A form titled 'ENT and ALLERGY ASSOCIATES, L.P. Accounting of Disclosures of Protected Health Information'. It includes a header with the company name and a date field. Below is a table with columns for 'Date', 'To Whom Disclosed', 'Purpose of Disclosure', 'Requester's Name', 'Requester's Address', and 'Requester's Phone Number'. The table has several rows for data entry. At the bottom, there is a section for 'Requester's Signature' and 'Date'.

The accounting may exclude disclosures made by the covered entity to carry out treatment, payment and health care operations which constitute an overwhelming majority of uses and disclosures. The burden is further lessened with the exclusion of disclosures made to the individual, pursuant to an authorization, and that were incidental.

The Bottom Line

The most effective way you can protect our patients' privacy is by considering their prospective when making decisions about using or sharing their information. If you were the patient, how would you expect your information to be handled? Whenever possible give patients control over how their information is shared and avoid sharing information in ways that might prompt patients to object.

Privacy is everyone's responsibility. Policies and protocols will not be effective unless everyone is committed to protecting our patients' privacy.