

Physician HIPAA Overview of Privacy at Mount Carmel



MOUNT CARMEL

A MEMBER OF  TRINITY HEALTH

HIPAA Regulations

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. The HIPAA Privacy Rules became effective in April 2003 and the HIPAA Security Rules became effective in 2005.

Amendments to the HIPAA Regulations – HITECH 2009

Major amendments to the original privacy and security rules were enacted into law in February of 2009 as part of the American Recovery and Reinvestment Act of 2009. The specific revisions are referred to as the Health Information Technology for Economic and Clinical Health Act or the HITECH Act. Some of the first provisions of the HITECH act to be enforced are those that strengthen the civil and criminal enforcement of the HIPAA rules and under certain circumstances, notification of patients if privacy rights have been violated.

Effective February 2009:

Enhanced Enforcement Provisions

1. HITECH provides that a person who has wrongfully obtained or disclosed PHI without authorization commits a criminal violation of HIPAA if the information is maintained by the covered entity. A “covered entity” as defined by HIPAA is a health plan, a healthcare clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction such as health care payment or remittance.
2. In cases where the U.S. Department of Justice does not prosecute an individual for alleged criminal violations of HIPAA, the Office of Civil Rights may investigate and impose civil and monetary penalties.
3. State attorney Generals can bring civil actions for criminal violations.

Effective September 2009 and enforcement/sanctions date February 2010:

Breach Notification Provisions - Prior to the HITECH breach notification requirements, HIPAA rules allowed Covered Entity’s some discretion in determining when to notify patient or the Department of Health and Human Services (DHHS) of a breach. Under the HITECH privacy and security provisions, there will be some situations where Covered Entities are mandated to notify the patient of the disclosure and report the disclosure to DHHS and local media outlets.

Patients

- Notification is required when unsecured Protected Health Information (PHI) – verbal, paper or electronic – is involved in an incident that meets the HITECH definition of a “breach”.

Prominent Media Outlets

- Prominent media outlets must be notified of breaches of unsecured PHI involving 500 or more individuals in a state or jurisdiction.

Notification and Reporting to the DHHS

- There must be immediate notification of breaches of unsecured PHI impacting more than 500 individuals. Additionally, covered entities must give a report to the DHHS on an annual basis listing all those individuals who were notified of breaches in the course of the previous year. This takes place in February each year.

As the HITECH laws are implemented, Mount Carmel will strive to keep physicians informed of the implications of the law. You may also contact the Privacy Official at 546-3284 with questions or concerns.

Mount Carmel and the Medical Staff jointly use and disclose patient's health information during the provision of services that we provide. Since we are both covered entities under HIPAA, we both have the same obligations and duties to protect information. Regardless of HIPAA, we both have a duty to:

- Protect and safeguard information;
- Educate patients on their rights regarding their information;
- Protect the patient's rights;
- Ensure their information is used and disclosed appropriately; and
- Ensure that appropriate administrative requirements are fulfilled.

The Privacy Official

Under HIPAA, each organization is required to select someone to serve as the Privacy Official. This person is responsible for developing and maintaining privacy related policies and procedures, providing training and overseeing the privacy functions at the facility. At Mount Carmel, the Privacy Official is Cathy McFaul who can be reached at 614-546-3284 or at cmcfaul@mchs.com

Origin and Purpose of HIPAA

One of the primary goals of the Health Insurance Portability and Accountability Act (HIPAA) was to help people obtain and maintain their health insurance benefits when they changed jobs.

HIPAA (also called Administrative Simplification Standards) also includes rules that are meant to:

- Make the management of healthcare information easier;
- Protect the privacy of patients' health information; and,
- Protect the security of patients' health information.

The major areas covered by the Administration Simplification requirements are:

- Transactions and Code Sets: Standards for the format and coding of billing-related electronic information that is sent and received by a facility. For example, electronic claims sent to third party payers.
- Privacy: Standards to protect the privacy of medical records and other specific information. These standards help to make sure protected health information (PHI) is properly handled by a facility.
- Security: Standards to protect the security, confidentiality, integrity (data-integrity), and availability of PHI. These standards address items such as sending electronic claims (billing) to payers and where and how you access electronic PHI.

This overview will focus on the privacy standards.

Benefits

Taking the steps to follow the HIPAA standards and develop the needed procedures can result in many benefits. For example:

Benefits to the Patient

Patients receive several benefits under the privacy rules of the Administrative Simplification requirements. Some of these benefits include:

- An understanding of how their protected health information (PHI) may be used by the Mount Carmel and/or the Medical Staff.
- The ability to approve who may use or disclose their PHI.
- A right to access and amend PHI.

Benefits for Mount Carmel and the Medical Staff

- Enhance patient confidence and develop a positive public image in the community as a result of efforts taken to protect patient information in compliance with the privacy and security standards.
- Minimize the potential for civil and/or criminal penalties and fines.

Benefits to the Industry

- Establish minimum standards and requirements that all covered entities must follow related to privacy and security of patient information.

- Allows facilities to continue to disclose PHI needed for certain activities such as law enforcement and public health activities.

Failure to Comply

Compliance with HIPAA and the Administrative Simplification requirements is very important. A facility or provider that does not follow the rules may:

- Be responsible for civil penalties and fines that can quickly add up to thousands of dollars.
- Be accused of criminal violations that can result in even larger penalties and fines, along with possible jail time.
- Be excluded from participation in the Medicare program.

Civil and criminal penalties and fines are not the only problems. A failure to comply may also hurt the reputation of Mount Carmel and associated providers, put accreditation status at risk and result in costly lawsuits.

By understanding the requirements related to privacy and security, you can help Mount Carmel comply with HIPAA. Together, we can continue to provide the level of quality, care and service that our patients have come to expect.

Privacy Rules

Starting on April 14, 2003, the privacy rules set the minimum standards that all providers must follow to protect patients' health information. The key term that you will hear when discussing the privacy rules is Protected Health Information:

Protected Health Information (PHI): Information in any format related to any healthcare provided to a person. This includes demographic information that can be used to identify the patient. Information that can be used in some manner to identify the person (e.g. social security number) is also considered PHI.

For example, the privacy standards cover PHI that can be found in:

- Information used within the facility
- Verbal or written information
- Information stored in computer files
- Information stored in paper patient files
- Information shared with other healthcare providers, payers or third parties (e.g., consultants, attorneys, etc.)

Patient Specific Identifiers

HIPAA has identified the following items as patient specific identifiers:

- Name
- Address, including street, city, county, precinct, zip code or the equivalent geographic codes
- Names of relatives
- Names of household members
- Name of employers
- Age (if greater than 90)
- Social Security Number
- Telephone and fax numbers
- E-mail addresses
- Medical record number
- Admission/Discharge dates
- Date of death
- Health plan identification/beneficiary number
- Account number
- Certificate/license number
- Any vehicle or device serial number including license plate number
- Web addresses
- Internet Protocol (IP) addresses (information that is able to identify an individual computer on the Internet)
- Biometric identifiers such as finger or voice prints
- Photographs
- Any other unique identifying numbers, characteristics or codes (e.g. a tattoo)

Patient Rights

Notice of Privacy Practices

Patients have the right to receive a Notice of Privacy Practices (NPP) which describes patient rights under the privacy rule as well as how the covered entity (health care provider, payer/health plan, health care clearing house) will use and disclose their information. The document must be given to the patient at the first encounter to the covered entity.

The covered entity must make every effort to have the patient sign a written acknowledgement that the NPP was offered. The notice must provide the name or title and phone number of a contact person in the event the patient wishes to file a complaint. The NPP must be easy to read and understandable. It also must be prominently posted in the facility.

At Mount Carmel, the NPP is available in English, Spanish, Russian and Somali.

Patient Rights

Patients have several basic rights regarding their protected health information or PHI such as:

- The right to a **Notice of the Privacy Practices** of Mount Carmel and the Medical Staff (discussed in the previous section)
- The right to **Request Additional Privacy Protections and Confidential Communications**. Patients may request that additional steps be taken to protect their PHI. Patients can also request that PHI be provided in a different, confidential manner (e.g. mailing PHI to a different address or sending information to an e-mail address instead of the patient's home address, etc.).
- The right to obtain **Access to their PHI**. With certain exceptions, patients have a right to review and copy their PHI.
- The right to **request an Amendment to their PHI**. Patients can request that Mount Carmel make changes or updates to their PHI if needed. Certain rules and exceptions apply here too.
- The right to an **Accounting of the Uses and Disclosures of their PHI**. This includes how certain PHI has been disclosed for certain reasons, for a period of up to 6 years, as well as who has received those disclosures. For example, a patient may be informed that his or her PHI was disclosed to the public health department in response to an inquiry related to a communicable disease.
- The right to **agree or object** to specific disclosures of their PHI, for example, from a facility directory, for disaster relief purposes, or to family or friends involved in their care.
- To **file a complaint** with Mount Carmel or directly to the Department of Health and Human Services. Mount Carmel must promptly investigate and respond to complaints.

Policies and procedures regarding patient rights are in place.

Authorization

Authorization: This is a form signed by the patient for the use and disclosure of specific PHI. Authorizations are obtained for uses and disclosures that are not related to treatment, payment, and healthcare operations. For example, releasing medical records to attorney at the patient's request would require an authorization.

A valid HIPAA authorization must contain certain elements which are outlined in the HIPAA Administrative Simplification Regulation Text. The authorization document used by Mount Carmel contains these elements.

You should be aware that there are some uses and disclosures where an authorization is not required. For example, uses or disclosures required by law or for public health purposes.

An authorization allows the use and disclosure of very specific PHI. Authorizations are required for many uses or disclosures of PHI for purposes other than treatment, payment or healthcare operations. Authorizations are obtained on a case-by-case basis and are needed each time a different use or disclosure is desired. .

Mount Carmel may not condition treatment on receipt of a valid authorization. One exception is for patients that want to participate in research studies where treatment will be provided (e.g. clinical trials). If the patient refuses to sign a required Authorization, he or she can be excluded from the study.

Once authorization is provided, the patient can revoke or cancel the authorization. The request to revoke or cancel an authorization must be in writing. The patient must be told how to revoke or cancel the authorization. Information should be provided to the patient regarding any exceptions. You should be familiar with this process in order to answer any questions the patient may have.

An authorization is considered invalid if it has expired, does not contain the required elements, is incomplete, has been revoked, or is known to contain false information.

Using and Disclosing PHI

Ohio Laws Regarding Privacy

In Ohio, many of Ohio laws are more stringent than HIPAA. In other cases, it is possible to comply with both the Ohio law and HIPAA. There are a few exceptions where HIPAA is more stringent than Ohio law.

Authorization for Fundraising/Marketing

In order to make contact with patients for the purpose of marketing activities, an authorization must be obtained. Two specific exceptions have been identified. These include:

- Marketing that occurs during face-to-face physician treatment encounters with the patient; such as recommending a drug of choice and,
- Marketing resulting from promotional gifts of nominal value (e.g.; pens or calendars).

Marketing and Fundraising Activities

Under HIPAA, marketing is defined as “a communication about a product or service that encourages the recipients of the communication to purchase or use

the product or service.” The Planning and Marketing Department at Mount Carmel review all Marketing initiatives. All Fundraising activities are coordinated through the Mount Carmel Foundation.

Types of communications that are not considered “marketing” include the following:

- To describe healthcare provider networks and any descriptions of products, services (or payments for products or services) that are or may be provided by Mount Carmel.
- For the treatment of the individual.
- For case management or care coordination for an individual patient.
- To direct or recommend alternative treatments, therapies, healthcare providers or care settings for an individual patient.

For example, some common communications that would not be considered marketing activities would include:

- Disease Management Programs
- Wellness Programs
- Prescription Refill/Appointment Reminders

It is anticipated that the HITECH regulations will require “clear and conspicuous” opt-out language to all fundraising materials given to patients.

Use of PHI: Emergent and Public Health Situations

Often, PHI must be used in certain emergent and public health situations. For example:

- Public health activities such as preventing or controlling disease or injury (e.g. a tuberculosis outbreak in the community)
- Reporting of child abuse and neglect
- Reporting to the Food and Drug Administration (FDA)
- Reporting of vital events such as births and deaths
- Disclosures to prevent a serious threat to health or safety

In these situations, Mount Carmel does not need to obtain authorization. In addition, the patient does not have the ability to agree or object to the disclosure.

Mount Carmel has detailed written procedures available for staff to review and follow. This will help to make sure any disclosures performed without authorization or the ability for the patient to agree or object are in compliance with the privacy rules. Mount Carmel will properly document the uses and disclosures of PHI made in these situations in case the patient requests an accounting of disclosures.

Releases of PHI Required By Law

Mount Carmel may release PHI without an Authorization when required by law to do so. Even then, the facility must be sure that:

- The release is within the extent of the law that requires the release
- The release of PHI complies with the requirements of the law
- The release is limited to the relevant requirements of the law

Complex and specific requirements of HIPAA must be met when the disclosure required by another law is in one of the following categories:

- Disclosures about adult victims of abuse, neglect or domestic violence
- Disclosures for judicial and administrative proceedings
- Disclosures for law enforcement purposes

Mount Carmel does have specific policies and procedures in place to handle disclosures for these purposes. These policies and procedures should be consulted and followed each time such a disclosure is considered.

Releases of PHI Permitted By HIPAA

In addition to releases required by law, HIPAA permits certain other releases of PHI without a specific authorization. Such releases include:

- Disclosures for public health activities
- Disclosures for health oversight activities
- Disclosures about decedents (to Coroners, Medical Examiners, Funeral Directors)
- Disclosures for cadaver organ, eye or tissue donation purposes
- Disclosures for research purposes
- Disclosures to avert a serious threat to health or safety
- Disclosures for specialized government functions (e.g., Military, National Security, Presidential Protection)
- Disclosures for workers' compensation

The determination of whether or not such disclosures can be made in a specific circumstance can be complicated. To help make sure any disclosures for these purposes are in compliance with the privacy rules, written policies and procedures are available for all Mount Carmel staff and the Medical Staff to help them understand what is required.

Administrative Requirements

There are many administrative requirements that Mount Carmel must put in place under the privacy rules. For example, Mount Carmel has met all of these administrative requirements:

- Selected a **Privacy Official**. For larger health systems, a single Privacy Official may be selected to oversee multiple facilities.
- Developed policies and procedures related to **PHI** and defined a process to update the policies and procedures as needed.
- Performing monitoring and auditing to make sure PHI is properly handled.
- Developed and taking corrective actions for people that do not follow the privacy policies and procedures.
- Ensure there is no **retaliation against individuals** who report potential privacy violations in good faith.
- Providing required training and education on the privacy rules.
- Developed a process for receiving and handling privacy related complaints.
- Taking steps to minimize any harm that may be caused by the improper use or disclosure of PHI.
- Ensuring documentation and record keeping processes are in place to demonstrate compliance.

With the administrative requirements, Mount Carmel does have policies and procedures in place to cover each of these areas.

Privacy Policies and Procedures

As part of the privacy practices, Mount Carmel is required to have written policies and procedures relating to PHI and information practices. Below is a general listing of some of the types of policies and procedures:

- Confidentiality policy
- Records retention policy
- Employee training policy
- Employee termination policy
- Release of information policy

Safeguards and Sanctions

Mount Carmel must develop the necessary administrative, technical and physical safeguards for PHI. Mount Carmel must also reasonably protect PHI from intentional or accidental use or disclosure, or other possible violation of the rules. But what happens when a patient's PHI is accidentally or intentionally disclosed?

Mount Carmel, in coordination with the Medical Staff (when appropriate) must identify what happened and those responsible for the improper disclosure. Disciplinary actions must be taken as appropriate. These actions, or sanctions,

should consider the severity and intent of the violation. They should also consider if there is a pattern or practice of improper use or disclosure of PHI. Disciplinary actions could range from a warning to termination.

Mount Carmel must try to minimize any adverse effects the disclosure may have. For example, a patient requests that his records be sent to Dr. John Smith. The records are prepared, however, they are accidentally sent to Dr. Jon Smith who is in the same building, but in a different suite. Mount Carmel has an obligation to contact Dr. Jon Smith and retrieve the information.

Beginning in September of 2009, the new HITECH requirements require that under certain conditions, patients are notified of a breach in their PHI. At Mount Carmel the Privacy Official will work with Mount Carmel Legal Counsel and the HIPAA Director at Trinity Health to determine if the violation meets the breach notification requirements. Additionally, depending on the nature and the magnitude of the breach, the United States Department of Human Services and Media outlets may need to be notified.

Written facility policies and procedures should provide information on disciplinary processes and the steps to take to minimize the impact of improper disclosures.

Limits on the Use and Disclosure of PHI

So far, we have reviewed what is required to use or disclose a patient's PHI.

Notices inform patients how their PHI may be used.

Authorizations are for uses and disclosures of specific PHI for purposes other than treatment, payment or **healthcare operations**.

Next, we are going to review what information should be released. Here is an example:

Ms. Jenkins arrives at Mount Carmel for treatment of Spinal Meningitis. A Public Health official, concerned about the possible spread of disease, requests copies of all information the hospital has concerning Ms. Jenkins.

This situation falls within one of the exceptions that allow information to be released without a specific authorization. However, is there anything else that you must consider before turning over all of the records Mount Carmel may have on Ms. Jenkins?

The answer is yes! When you disclose or request PHI, it is important that you only access, disclose or request the minimum amount of information necessary to perform or complete the task. This is known as the minimum necessary standard. This formalized the processes for, "Need to Know" for internal and external uses of PHI. In some cases, there are exceptions to this requirement.

In most cases, providers can rely on the requests received from other providers and authorized officials as being the minimum necessary required. However, if Mount Carmel believes the request is in error or is improper, the facility may restrict the amount of information disclosed. In our example, it would not be appropriate to send information related to past hospitalizations or other information not relevant to the spinal meningitis. Such information would be more than the “Minimum Necessary Disclosure” to accomplish the purpose for which the health official is seeking information.

When disclosing PHI, you must also make sure that the person requesting the PHI is authorized to receive the information and that you verify the person’s identity and authority.

Written procedures are in place to help you determine what information is necessary for the tasks that you perform. These procedures can also provide you with information on how to determine who is authorized and who is not and the steps to take to verify the identity of the person.

Incidental and Oral Communications

The Privacy Standards apply to PHI that is oral, written, stored in computer files, and stored in paper medical records.

Many patient complaints lodged with the **Office of Civil Rights (OCR)** – the Department of Health and Human Services entity that oversees HIPAA Privacy and Security – involve the inappropriate disclosure of **oral PHI**.

HIPAA does allow for incidental disclosures, BUT PHYSICIANS MUST TAKE REASONABLE SAFEGUARDS, to prevent others from overhearing or seeing protected health information.

Do not discuss results of surgery in a surgery waiting area. Take the family to a less public location.

Always request the patient’s permission prior to sharing any PHI in front of other individuals present in the room. This includes immediate family members. Another option is to request that all leave the room while you update the patient. This takes the burden off the patient to ask visitors to leave.

The goal of the privacy rule is not to prevent needed discussions related to patients, but to make sure that when discussions need to take place, Mount Carmel and the Medical Staff are doing what is reasonable to protect a patient’s PHI. If a facility/provider does not take reasonable steps to protect patient privacy, it could be found in violation of the privacy rule.

It really means using your best judgement, for example:

- Discussions in busy hallways and elevators mean that anyone around can overhear the conversation. It would be better to find a place where fewer (or no) people could overhear the conversation
- Use overhead paging, only when absolutely necessary
- Cafeterias and halls are often busy with patients, their families and employees. If you are discussing the details of a particular patient, it may be best to have the conversation in a more isolated location
- Patient information that is visible on computer screens should be kept confidential. Unless impossible to accomplish, screens should be located to avoid access or viewing by unauthorized users. Log off applications when you have completed your business.
- When phoning patients, messages should be kept to a minimum when the patient cannot be reached directly. Leave only your name and number, not diagnostic information, or the reason you are calling.
- Replace patient information in a secured location when not in use. Secure information that you carry on your person. Use the appropriate document destruction bins to dispose of information that has PHI on it.

Verification Requirements

Mount Carmel has received a request for disclosure of PHI. You've followed all of the procedures. You have made sure that only the PHI necessary to complete the task is provided. But is the person requesting the PHI authorized to receive it?

Before any PHI is released, you must follow Mount Carmel's procedures for verifying the identity of the person requesting the information. If the request is from a person that is not known to us, or is not acting on behalf of the government, it is up to the facility to determine what is considered proper identification. **Mount Carmel accepts a driver's license or other state-issued photo ID for personal requests.**

For requests made by public agencies (e.g., state or federal government agencies, legal copy services, etc.), you should require verification of identity through an employment badge or photo ID. You may also verify authority by accepting a written statement, on letterhead from the agency that lists the legal authority (i.e. the specific code or law) or other support for the request.

You should make sure that you follow the procedures to verify the identity of any individual or agency before PHI is disclosed.

Business Associates

We must work with other facilities and organizations to provide patients services. A Business Associate is “a person or organization that uses or receives PHI from the facility in order to perform or assist the facility with some activity or function.” The Regulatory Compliance Department through the Privacy Official handles all Business Associate Contracts.

Some of the more common Business Associates may include:

- Independent Contractors
- Consultants
- Lawyers
- Auditors
- Information System/Data Processing Vendors
- Billing Companies

Due to the complexity of services provided by us, there may be many Business Associates. For example, some possible Business Associates related to Medical Staff functions are:

- External Peer Reviewers
- Consultants to improve processes
- Attorneys to obtain legal advice

In some situations, businesses involving physicians may be a Business Associate of Mount Carmel.

Business Associates may or may not be covered entities under HIPAA. A Business Associate is only required to follow the HIPAA rules if it is considered a covered entity. To be sure to protect patient’s PHI regardless of whether the Business Associate is a covered entity or not, Mount Carmel must be sure each Business Associate’s written contract requires that certain rules be followed to protect the privacy and security of PHI. For example, the contract cannot allow the Business Associate to make any use or disclosure of PHI that the facility is not allowed to make.

Reporting Concerns and Violations

The Privacy regulations are complex, and you may have questions from time to time. To seek answers to questions or concerns, including possible violations of the law, or policies and procedures it is recommended that:

1. Call the Privacy Official directly at 546-3284, or report your concern anonymously at 546-3292.
2. If you still are not satisfied, call the toll-free, 24-hour Integrity Alertline at 1-866-477-4661.

De-identification and Re-identification

At times, Mount Carmel or members of the Medical Staff may want or need to de-identify health information. For example, a pharmacy is doing a study to determine how many patients with a specific condition have been admitted to a local hospital. The results of the study will help the pharmacy budget their inventory for a very expensive drug that is used to treat that condition. By obtaining de-identified health information, the pharmacy will be able to maintain the necessary supply of the drug and the hospital will be able to help make sure patients receive the treatment they need.

HIPAA lists specific information that must be removed for PHI to be considered de-identified. We can remove, code or encrypt the information to create de-identified information. In any of these processes, we must be reasonably sure that the remaining information cannot identify the person, either by itself or in combination with information from another individual or organization.

When we de-identify information by using codes or other methods to allow for re-identification of the information, we must make sure that:

- The code or other identifier assigned to the record is not a part of or related to the information. For example, you would not want to list the initials of the patient's first and last name followed by the last four digits of the social security number.
- The code or other identifier cannot be translated to identify the patient. For example, the code should not be like a puzzle where the letter "A" equals "B", "B" equals "C", etc.
- We do not use or disclose the code or other identifier for any other purpose.
- We do not disclose the method used for re-identification of PHI.

Limited Data Sets

In addition to de-identified information, HIPAA provides an alternative method that Mount Carmel may follow for the use and disclosure of PHI for research, public health or healthcare operations. This alternative is known as a limited data set.

In order to qualify as a limited data set we must:

- Use or disclose information only for research, public health or healthcare operations purposes.
- Remove direct identifiers from the information to be used or disclosed.
- Obtain a data use agreement that:
 - Specifies the permitted uses and disclosures of the information;
 - Identifies who can use the information;
 - Includes an agreement that the recipient of the information will not re-identify the information or contact the individual; and,

- Provides that the recipient of the information has appropriate safeguards in place to prevent use or disclosure of the information other than for the intended purpose, or otherwise allowed under the privacy rule.

Use or disclosure of limited data set PHI for purposes other than those specifically identified in the privacy rules would be considered a violation.

Last Thoughts

Providers are already protecting information. With a few exceptions, HIPAA did not create new principles, or new ideas. It attempted to have a set of standards for all providers, across all practice settings. It also provides each of us an opportunity to improve the ways that we utilize and disclose information.