TRAINING MANUAL

HEALTH INSURANCE PORTABILITY &

ACCOUNTABILITY ACT OF 1996

HIPAA

Table of Contents

Introduction

What is HIPAA?
HIPAA is short for the Health Insurance Portability and Accountability Act of 1996. Through HIPAA, Congress provides federal protection for the privacy and security of patient health information. The HIPAA regulations provide guidance on privacy, security and transactions and code sets.

Privacy
The HIPAA Privacy Rule contains rules for the protection of patient health information and for patients' rights related to that information. HIPAA also requires us to implement policies for protecting patient health information and to permit patients to exercise their rights.

Security
The HIPAA Security Rule requires that we implement physical and technical safeguards to protect the security of electronic patient health information**.**

Transactions and Code Sets
The HIPAA Transactions and Code Sets Rule standardizes the way we send and receive billing information on the patients we treat.

Taken together, these three HIPAA Rules are designed to facilitate the development of a uniform computer-based health information system, while protecting the privacy and security of our patients**'** health information**.**

What is Covered
HIPAA requires covered entities, including certain health care providers such as EmCare and other health care companies**,** to protect the privacy and security of Protected Health Information (PHI). This type of information can be in oral, written or electronic form. PHI includes demographic or other identifying information that:

- is created or received by covered entity;
- relates to the past, present or future physical or mental health condition of an individual**,** provision of care to an individual; or the past, present or future payment for the provision of care to an individual**; and**
- identifies the individual; **or**
- provides a reasonable basis to believe the information can be used to identify the individual.

Administrative Requirements

Privacy Officer

To help ensure compliance with the HIPAA Privacy Rule, we have a Privacy Officer who is responsible for developing and implementing our HIPAA compliance program. The Privacy Officer is responsible for developing and implementing privacy policies and procedures, receiving complaints regarding our privacy practices and providing further information about our privacy practices.

Privacy Policies and Procedures

If you have any questions regarding our privacy practices, please contact the Privacy Officer or a member of the Ethics & Compliance Department.

You may also call the toll-free HIPAA Helpline number: (877) 835-5267.

We have established a comprehensive set of HIPAA policies and procedures to guide all employees and to ensure compliance with HIPAA and its regulations. These policies are available to review on the EmCare website.

Enforcement and Compliance

Any employee who violates HIPAA may be subject to sanctions, up to and including termination of employment. If you have a good faith belief that the HIPAA regulations may have been violated, you have an affirmative obligation to report any suspected violation to the Privacy Officer or a member of the Ethics & Compliance Department. Anyone, including our patients, who believe that we are not complying with the applicable requirements of HIPAA, may file a complaint with the Department of Health and Human Services ("DHHS"). HIPAA establishes civil and criminal penalties for violations of HIPAA**.** Criminal penalties include up to $250,000 for each violation and up to 10 years in prison.

We will not take any retaliatory action against any individual who in good faith reports a potential HIPAA violation.

Preemption

The HIPAA Privacy Rule establishes a uniform "floor" for protecting the privacy of PHI. The HIPAA Privacy Rule preempts, or overrides, state laws that are contrary to, and that are less protective than the HIPAA Privacy Rule**.** State laws related to the privacy of health information that are more protective than the federal rule will remain in effect. Generally, a state law is "more protective" when it provides greater privacy protection for the individual who is the subject of the information or provides the individual with greater rights in his or her PHI.

Patient Rights

Notice of Privacy Practices and Patient Rights

The HIPAA Privacy Rule gives individuals the right to be informed of our privacy practices and their privacy rights. It requires that we provide patients with a written notice describing our privacy practices.

We must make a good faith effort to obtain a written acknowledgement from the patient of receipt of the notice. In the event that the patient is unable to sign or we are otherwise unable to obtain a written acknowledgment, we must document the reason why we were unable to obtain the acknowledgment from the patient.

EmCare physicians who work at contracted facilities will distribute the facility's Notice of Privacy Practices.

Q & A: Privacy Practices and Patient Rights

Q. Are we required to provide the Notice of Privacy Practices to patients even during emergency treatment situations?

A. No. The HIPAA regulations do not require healthcare providers to distribute the Notice of Privacy Practices to patients during emergency treatment situations. However, we must document why we could not provide the Notice to the patient at the time of treatment. In addition, once the patient has been stabilized we must make a good faith effort to provide the patient with the Notice. We must also obtain a written acknowledgment from the patient of the receipt of the Notice.

Right to Access

The HIPAA Privacy Rule gives individuals the legal right to see and obtain a copy of their own PHI for as long as we maintain the information. In general, we must follow these rules:

- Allow an individual to inspect or obtain a copy of the PHI no later than 30 days after receiving the request.
- All requests for access to PHI must be made in writing.
- All written requests for access to PHI must be kept with the medical record for as long as we maintain the record.

Right to Amend

The HIPAA Privacy Rule gives individuals the right to amend their own PHI. For example, an individual who learns that someone else's health information is mistakenly in her chart may request that the record be amended to note that this information is not hers**.** The individual has this right for as long as the covered entity maintains the information.

We may deny an individual's request for amendment; for example, if we determine that we did not create the information, that the information would not be available for inspection because the individual does not have a right to access it, or that the record is accurate and complete**.**

- All requests for amendments must be submitted in writing.
- The Medical Director for each operational area or region will be responsible for reviewing the request and will make the final determination to accept or deny the request.
- The Medical Director will then provide the patient with a written explanation of our decision**.**
- We must respond to an amendment request within 60 days after receiving the request**.**
- The patient has the right to appeal the decision.

Q & A: Right to Amend

Q. Who is responsible for deciding if we will amend a patient's medical record?

A. When a patient requests an amendment to his or her medical record, it is the responsibility of the Medical Director to review the request and determine if an amendment is warranted. The Medical Director is also responsible for communicating the decision to the patient.

Right to Request Restrictions and Alternative Methods of Communication

The HIPAA Privacy Rule gives individuals the right to request restrictions on the uses or disclosures of their PHI. For example, an individual may request that a particular medical procedure be kept confidential and not shared with other providers. Although

we are not required to agree to such a restriction, if we enter into an agreement to restrict, we must abide by the agreement, except in emergency circumstances.

The HIPAA Privacy Rule also gives individuals the right to request that communications of PHI be made by alternative means or at alternative locations. For example, an individual may request that we call them at work instead of at home. We must accommodate all reasonable requests and may not require an explanation from the individual as to why they are making such a request.

Right to Receive an Accounting of Disclosures

Individuals have the right to receive an itemized list of **certain** disclosures of their PHI that we made during the six years prior to the date that the individual requests the accounting, including disclosures to or by business associates. Generally, we must provide the individual with an accounting within 60 days after receiving such a request. We must include:

- the date of each disclosure;
- the name and, if known, the address of the organization or person who received the information;
- a description of the information disclosed; and
- a statement of the purpose of the disclosure.

Because we are required to provide individuals with an accounting of disclosures, we must document certain disclosures we make.

Use and Disclosure of PHI

Permitted Uses and Disclosures

The HIPAA Privacy Rule limits when and how we may use and disclose PHI.

- We "use" PHI when we internally access, share, examine, or analyze PHI**.**
- We "disclose" PHI when we release, transfer, or give access to PHI to another entity.

For treatment, payment, or healthcare operations, (TPO) we may use and disclose PHI without the individual's permission. Healthcare operations include a wide range of activities, including, for example, conducting quality assessment and improvement activities, reviewing the competence of health care professionals, conducting training programs, conducting or arranging for medical review or legal services, business planning and development and business management and administrative activities.

Q & A: Privacy Practices

Q. Is it correct that although we may provide treatment without patients' consent, we must obtain written acknowledgment from patients of their receipt of the Notice of Privacy Practices?

A. Yes. Covered entities are required to give patients the Notice of Privacy Practices and receive a written acknowledgment of receipt of the notice. However, if we render treatment and are unable to obtain written acknowledgment of receipt of our Notice of Privacy Practices, we must document our attempt and the reason why we were unable to get the acknowledgment from the patient.

In addition to uses and disclosures related to treatment, payment or healthcare operations, under certain circumstances [more fully discussed in our HIPAA Policies and Procedures] we are permitted to use or disclose PHI without the patient's written authorization in the following circumstances.

- Uses and disclosures required by law
- Uses and disclosures for public health activities
- Disclosures about victims of abuse, neglect or domestic violence
- Uses and disclosures for health oversight
- Disclosures for judicial and administrative proceedings
- Disclosures for law enforcement purposes
- Uses and disclosures about decedents
- Uses and disclosures for cadaveric organ, eye or tissue donation purposes
- Uses and disclosures for research purposes
- Uses and disclosures to avert a serious threat to health & safety
- Uses and disclosures for specialized government activities
- Disclosures for workers' compensation

In addition, while we are not required to obtain the patient's written authorization first**,** we are required to give the individual the opportunity to object to the following types of disclosures:

- Uses and disclosures for facility directories
- Uses and disclosures to family members and other individuals involved in the patient's care or payment for that care

Before we use or disclose PHI for any other purpose, we must first obtain the patient's written authorization. The HIPAA Privacy Rule requires that certain information be included in the written authorization. To ensure we capture all of the required information, we have developed a standard HIPAA Authorization Form that should be completed prior to any uses or disclosures of PHI outside of those listed above. These Authorization Forms may be obtained through the Ethics & Compliance Department.

Minimum Necessary

When we use or disclose PHI, we must make reasonable efforts to limit the use or disclosure of PHI to the minimum amount necessary to accomplish the purpose of the permitted use or disclosure. This includes uses and disclosures made for purposes of payment and healthcare operations.

When we disclose PHI to another healthcare provider for treatment purposes, including oral disclosures, we are not subject to the minimum necessary standard. For example, an EMT is not required to apply the minimum necessary standard when discussing a patient's medical condition with an emergency department physician at a hospital.

Q & A: Incidental Uses and Disclosures

Q. Can healthcare providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

A. Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. The regulation recognizes that oral communications often must occur freely and quickly in treatment settings. These types of disclosures are considered "incidental disclosures." Thus, healthcare providers may engage in communications as required for quick, effective, and high quality healthcare.

Incidental Uses and Disclosures

The HIPAA Privacy Rule is not designed to keep healthcare providers from talking to each other or to their patients. Incidental uses or disclosures of PHI that occur as a result of an otherwise permitted use or disclosure are not considered violations of the HIPAA Privacy Rule provided that we have taken reasonable precautions to safeguard the information. Reasonable precautions may include:

- speaking quietly when discussing a patient's condition with family members in a waiting room;
- avoiding use of a patient's name in public hallways and elevators;
- avoiding discussion of the patient's condition with bystanders.

Safeguarding the PHI of current and former employees

Under the HIPAA Privacy Rule, our colleagues and former employees have a right to expect privacy and confidentiality when it comes to their own healthcare. Co-workers and former co-workers of covered entities have the same privacy rights that any other individual has under the HIPAA regulations. In the event a colleague, co-worker or former employee is a patient at a facility for medical or psychological treatment**,** we must continue to follow the HIPAA Privacy Rule. We must use the same measures to protect his or her confidentiality as we would any other patient. This means that we must not use or disclosure the PHI in any way that we would not otherwise be permitted to do without the patient's authorization. In addition, we must follow the minimum necessary requirements to limit disclosures of PHI to anyone not directly involved with the patient's care. We must also refrain from mentioning the presence or condition of this person to any other co-worker or colleague.

Videotape and/or Photographs of PHI

All employees must not, and may not allow anyone else**,** including members of the media, a third party vendor or any other employee, to videotape or photograph any aspect of our operations without prior written notice to the Chief Compliance Officer and prior written authorization of the individual who may be the subject of the PHI. Such conduct could be considered an impermissible use or disclosure of PHI and a violation of the HIPAA Privacy Rule. This applies to clinical training and for all purposes other than treatment, payment and healthcare operations.

Business Associates

We routinely hire other companies and consultants to provide services for us that may involve the use or disclosure of PHI. These entities are called "business associates." We must obtain satisfactory assurance that the business associate will appropriately safeguard the information. This will normally take the form of a written agreement called a "Business Associate Agreement" that prohibits the business associate from using or disclosing the information other than as permitted or required by the agreement.—

Q & A: Business Associates

Q. Would healthcare provider need a Business Associate Agreement with every insurance company to which it sends bills?

A. No. A Business Associate Agreement is required only when a third party is providing certain services or performing functions on our behalf that involve the use or disclosure of PHI. Insurance companies that are paying healthcare claims for services that we render are not considered to be doing so on our behalf (rather, it is on behalf of the patient) and, therefore, business associate contracts are not required with such entities.

Law Enforcement

The HIPAA Privacy Rule does not expand current law enforcement access to PHI. Your state privacy laws may be more protective than the federal HIPAA regulations. If that is the case, continue to follow your state privacy laws.

Even in cases when the Privacy Rule permits disclosure to law enforcement, we must follow the Minimum Necessary Standard.

The HIPAA Privacy Rule permits disclosure of certain PHI (e.g. name, address, birth date, social security number, blood type, type of injury, date and time of treatment and a description of distinguishing features) to law enforcement officials without the patient's authorization for identification or investigative purposes.

Q & A: Physical Privacy and Security

Q. Does HIPAA require emergency departments to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?

A. No. The HIPAA Privacy Rule and Security Rule do not require these types of structural changes be made to facilities. The Rules require only that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule.

We may also disclose PHI about a crime victim to law enforcement officials if the victim agrees to the disclosure, or, if the individual is unable to agree we receive certain representations from the law enforcement official.

In addition**,** when possible, we must obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement unless the disclosure is otherwise required by law.

Under the HIPAA Privacy Rule, we may disclose PHI to law enforcement officials as required by law or in response to:

- a court order, a court-ordered warrant, or a subpoena or summons issued by a judicial officer;
- a grand jury subpoena; or
- an administrative request, such as an administrative summons or a civil investigative demand that meets specific standards.

We must also confirm the subpoena contains a "Certificate of Satisfactory Assurances" from the attorney requesting the PHI that the requesting attorney has made a good faith attempt to provide written notice to the patient or patient's personal representative of the intent to request the PHI, and that the patient is aware of the request for PHI. The Certificate must also state that either the patient had no objections, or any objections have been resolved prior to the subpoena being submitted.

HIPAA Security

Just as the HIPAA Privacy Rule protects the privacy of PHI in oral, written and electronic form, the HIPAA Security Rule focuses only on safeguarding the security of electronic PHI, or EPHI. Safeguarding EPHI is everyone's responsibility.

Pursuant to the HIPAA Security Rule, we will:

- implement reasonable and appropriate administrative, technical, and physical safeguards that ensure the confidentiality, integrity and availability of the electronic PHI the entity collects, maintains, creates or transmits;
- protect against reasonably foreseeable threats to the security or integrity of the information such as unauthorized access, alteration, deletion or transmission of the EPHI; and
- protect against any reasonably anticipated uses or disclosures of the information that are not permitted or required by the Privacy Standards.

The following is a list of practices that we employ to comply with the HIPAA Security Rule.

Access to Secured Areas

You should report any observed or suspected incidents to your Medical Director or designated Information Systems personnel immediately.

Virus Protection

You should take precautions to prevent and detect the introduction of any type of viruses or other malicious software.

NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash (Deleted Items Folder, Recycle Bin, and so on.) Keep in mind that viruses are often sent by someone pretending to be someone you know or trust.

Passwords & Password Protection Standards

- A poorly chosen password may result in the compromise of our entire corporate network. As such, you are responsible for taking the appropriate steps to select and secure your passwords.
- Do not use the same password for EmCare accounts as for other non-work access, for example, personal ISP account and benefits.
- Where possible, do not use the same password for various work access needs.
- Do not share EmCare passwords with anyone who should not have access to your network logon information.
- All passwords are to be treated as sensitive and confidential information.
- Keep passwords confidential and secure and do not share accounts.
- Authorized users are responsible for the security of their passwords and accounts.
- User-level passwords should be changed every 45 days.

Q & A: Communication Devices

Q. Does the HIPAA Security Rule require encryption of wireless or other emergency medical radio communications that can be intercepted by scanners?

A. No. The HIPAA Security Rule does not require that we make these types of electronic communication changes. We must implement reasonable safeguards to limit incidental, and avoid prohibited uses and disclosures.

PDA's and other hand held electronic devices

Any type of hand held electronic device that is used to store, transmit or create EPHI must be properly safeguarded to ensure the integrity of the data. Take steps to protect the device from theft or loss.

- Remember that your conversations and written communications about patients are private.
- Be aware of who is around you in elevators, airports and restaurants.
- Sensitive information such as PHI should be encrypted and/or password protected.

EmCare personnel who work at hospitals and other facilities should be familiar with the facilities' HIPAA policies and procedures regarding physical and technical security.

ACKNOWLEDGMENT OF HIPAA TRAINING AND COMPLIANCE FORM

I certify that I have received HIPAA training and the HIPAA Training Manual. I have read it and I understand that it represents some of my responsibilities as an employee, officer or director (as applicable) of the Company.

I understand that I have access to a toll-free HIPAA Helpline number, (877) 835-5267, to answer any questions about HIPAA requirements or HIPAA compliance issues. I also understand that I have an affirmative obligation to report any suspected violation to the Privacy Officer or a member of the Ethics & Compliance Department.

Please sign and return this form to your supervisor or manager. It will be sent to the Ethics & Compliance Department and a copy will be placed in your personnel file.

Name (Print): _____

Company: _____

Position Title: _____

Last four digits of SS#: _____

Employee ID #: _____

Location: _____

Hire Date: _____

Signature: _____

Today's Date: _____