

HIPAA Fact Sheet

February 20, 2003

Southeastern Massachusetts EMS Council

I compiled the following information from multiple sources and withdrew the information regarding HIPAA that was relevant to ambulance providers and services providing emergency medical services. This information is intended to be an overview, and it is recommended that any policies that are implemented at your service be reviewed by legal council. As always if you have any questions in regards to the HIPAA regulations please feel free to contact my office at 508- 946-3960 or email me at dsampson@semaems.com.

Sincerely,

Dana Sampson
Executive Director

HIPPA does.....

NOT override state laws governing reporting of child abuse or neglect, public health and reporting laws.

NOT supercede state laws that govern privacy of health care information that are more stringent than the HIPAA requirements.

Require that each person who maintains health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards to insure the integrity and confidentiality of health information.

Require that you protect against any anticipated threats or hazards to security including unauthorized users accessing the information.

Require that healthcare clearinghouses (including third party billers) has policys and procedures that does not allow for unauthorized access to privileged patient information

Administrative Simplification Standards:

Purpose:

- 1.) To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information
- 2.) To improve the quality of health care in the U.S. by restoring trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care.
- 3.) To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and individual organizations and individuals⁽¹⁾

⁽¹⁾ Federal Register / Vol. 65, No. 250 / Thursday, December 28,2000 / Rules and Regulations

Transactions that are covered by HIPAA include “patient encounter information”, which would include Prehospital Care Reports, and healthcare payment and remittance advice.

Electronic Health Information

If you or a third party biller is using electronic remittance systems, these systems must use a standardized format, these code sets have been set forth by CMS. Vendors of software products used by providers must ensure their products are in compliance with the HIPAA coding requirements, and must include warranties to that effect in their license agreements. However there is no obligation to use electronic media to exchange protected patient information (includes patient billing transmission).

If your service opts to use electronic health information, it is recommended that these policies be developed and put into place:

- 1.) Information system security (i.e. user passwords, authorizing users to only view information that is pertinent to their function in your organization, and physical security of records.)
- 2.) Enforcement guidelines, including disciplinary action when a privacy policy is broken.
- 3.) Training your employees to understand their responsibility in regards to protected health information, as well as making them aware of the policy and procedures in place.
- 4.) Developing confidentiality agreements that outline an employees responsibility towards patient confidentiality, these agreements should be discussed and signed by the employee.

Standards for Privacy

Detailed policy and procedures for meeting the privacy provision of HIPAA is left to the individual covered agencies (Ambulance Service). The complete final regulation is known as 45 CFR 160 and 164, Standards for Privacy of Individually Identifiable Health Information. Below I have highlighted the actions that need to be taken and the responsibilities of the individual ambulance service under these regulations:

Sec. 160.201 Applicability

- State laws that are contrary to the requirements are preempted by the federal requirements with the exception of:
 - o State laws that address controlled substances
 - o State laws on privacy of individually identifiable health information that are more stringent than the federal HIPAA requirements (see 105 CMR 170.345 (D)).

Sec 164.502 Uses and disclosures of protected health information : general rules

a) Standard

- Care providers that have a direct treatment relationship with an individual to obtain general consent from the individual in order to use or disclose protected health information about the individual for treatment, payment, and health care operations.
- Verbal permission must be granted prior to providing protected health information to persons assisting in the care of the individual.

b) Standard : minimum necessary

- Requires the service to make all reasonable efforts not to use or disclose more information than necessary to accomplish the intended purpose of the use or disclosure.

d) Standard: uses and disclosures of de-identified protected health information

- Services may use protected health information to create de-identified information. De-identified information is not subject to the requirements of these privacy rules unless it is re-identified.
 - o Note: All future printing of SARFs will de-identify patients on the pink regional copy by blacking out the patients name and date of birth.

e) Standard: disclosures to business associates

- A business associate (i.e. third party biller) should have a contract regarding privacy when the Service releases protected health information to that business associate.
- The service may not disclose protected health information to a business associate without satisfactory assurance it will properly safeguard the information.

f) Standard: deceased individuals

- Protected health information of the deceased individual remains protected for the length that the service maintains the patient care record.
- The personal representative of the patient is able to act in the interest of the decedent

g) Standard: personal representatives

- Services must treat a person as a personal representative of an individual if it can be substantiated by law (Health care proxy, power of attorney).
- Services must treat a person that meets the requirements of a personal representative as the individual (patient).

164.506 Consent for uses or disclosures to carry out treatment, payment, or health care operations

A consent needs to be written in general terms, and refers the patient to the notice of privacy practices. It allows the service to use protected health information for the purposes of treatment, payment, and health care operations.

a) Standard: consent requirement

- Covered health care providers are required to obtain the individual's consent prior to disclosing protected health information to carry out treatment, payment or health care operations.
- Consents must:
- Services must produce a notice of privacy practices.
- **The exceptions to this rule:**
 - o **Services that provide care to inmates or correctional institutions are not required to gather consent for access to the inmate's records.**
 - o **Information created or received in emergency treatment situations.**

b) Implementation specifications: general requirements

- Services must produce a notice of privacy practices.
- Consents for uses of disclosures of protected health information to carry out treatment, payment, and health care operations may be combined in a single document covering all three types of activities and may be combined with other types of legal permission.
- Within a single document, consent for use and disclosure of protected health information must be visually and organizationally separate from the other consents, and must be separately signed and dated.
 - o While the consent for release of protected health information can appear on the same form as other types of consent (for instance consent for treatment), it needs to be separately laid out and signed.

c) Implementation specifications: consent content requirements

- Consents must:
 - o Be written in plain understandable language
 - o Inform the patient that protected health information may be used to carry out treatment, payment, or health care operations.
 - o Refer and indicate to the patient the right to review the notice of privacy practices prior to signing.
 - o Indicate the terms of the notice of privacy practices may change, and how the patient would get a copy of the revised notice.
 - o Inform the patient that they have the right to request restrictions on uses and disclosures of protected information, although the service is not required to agree to those restrictions
 - o Indicate that the patient has the right to revoke the consent in writing , except to the extent that the service has already used the information based on the original consent.
 - o Signature and date of the signature

164.508 Uses and Disclosures for which an authorization is required

An authorization allows the use and disclosure of protected health information for purposes other than treatment, payment, and healthcare operations. It is suggested that you refer to MA 105 CMR 170.345 (D) for specific guidelines in release of protected healthcare information.

c) Implementation specifications: core elements and requirements

- A minimum set of elements for an authorization to disclose protected patient information should include :
 - o Specific description of the information to be used or disclosed

- Include the name of people or groups of people that are authorized to use or disclose the protected health information
- State an expiration date
- State that the individual signing the authorization has the right to revoke an authorization in writing, excepting information release that has already taken place under the authorization
- Include instructions in how to revoke the authorization
- Inform the individual that once the information is disclosed the party receiving the information can re-disclose it and it may not be protected by this rule.
- Signature and date
- Should be written in plain language
- If the authorization is signed by a personal representative of the patient they must indicate their relationship to the patient.

164.152 Uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required

b) Standard: uses and disclosures for public health activities

- Services are allowed to disclose protected health information without individual authorization to:
 - Public health authorities authorized by law to collect or receive information for the purpose of preventing disease, injury, or disability, certain events such as birth or death, and to conduct public health surveillance, investigations, and interventions.
 - A public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect.
 - Public health authorities (FDA, OSHA, CDC), and state and local public health departments

c) Standard: disclosures about victims of abuse, neglect, or domestic violence

- Services are allowed to disclose protected health information without individual authorization to:
 - Specified authorities in abuse situations other than those involving children
 - Law enforcement and authorized public officials in cases involving domestic violence , as well as those involving abuse and neglect
 - Any government authority authorized by law to receive reports of abuse, neglect, or domestic violence
 - The Service, in the exercise of professional judgment, believes that the disclosure will prevent serious harm to the patient or to other potential victims
- Services that make disclosures due to mandated reporting laws must inform the patient of the report, this can be done orally. There are two exceptions:
 - The provider does not need to inform the patient if in the exercise of professional judgment, believes that informing the patient would place that person at risk of serious harm.
 - If the provider would need to inform the patient representative due to patient condition, and they believe that that this representative is responsible for the abuse, neglect or injury caused to the patient.

e) Standard: disclosures for judicial and administrative proceedings

- Protected health information can be revealed for a judicial or administrative proceeding, if the request is made through an order of a court or administrative tribunal, subpoena, or discovery request.
- Services can only disclose the protected health information expressly authorized by the above listed orders

f) Standard: disclosures for law enforcement purposes

- Services are allowed to disclose limited identifying information (name, address, social security number, date and place of birth, type of injury, blood type, date and time of treatment, date and time of death) for purposes of identifying a suspect, fugitive, material witness, or missing person in response to a law enforcement request.
- Services may disclose protected health information about an individual that has died, if there is a suspicion that the death may have occurred as a result of criminal conduct.
- A provider providing emergency health care in response to a medical emergency can disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:
 - The commission and nature of a crime
 - The location of such crime or of the victims of such a crime
 - The identity, description, and location of the perpetrator of such a crime

164.514 Other requirements relating to uses and disclosures or protected health information

h) Standard: verification requirements

- The service must establish and use written policy and procedures, that are designed to verify the identity and authority of the requestor where the service does not know the person requesting the protected health information.
- Services are required to take reasonable steps to verify the identity of individuals requesting access to their own protected health information.

164.520 Notice of privacy practices for protected health information

b) Implementation specifications: content of notice

- Required elements of a “notice of privacy practice”
 - o Written in plain English
 - o The header must read: “*THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.*”
 - o Services must describe each purpose for which they are permitted to use or disclose protected health information under this rule without authorization.
 - o The description for uses and disclosures to carry out treatment, payment, and health care operations must include at least one example of the types of uses and disclosures the covered entity is permitted to make.
 - o State that all other uses and disclosures will be made only with the patients authorization and that the patient had the right to revoke such authorization.
 - o The following rights must be described:
 - The right to request restrictions on certain uses and disclosures including a statement that the Service is not required to agree to a requested restriction
 - The right to inspect and copy protected health information
 - The right to amend protected health information
 - The right to an accounting of the disclosures of protected health information
 - The right of an patient (including a patient who has agreed to receive the notice electronically) to obtain a paper copy of the notice upon request.
 - o Services must state in the notice that they are required by law to maintain the privacy of protected health information, to provide a notice of their legal duties and privacy practices, and to abide by the terms of the notice currently in effect.
 - o Must inform the patient about how they can lodge complaints with the service if they believe that their privacy rights have been violated
 - o State that individuals can file complaint with the Secretary
 - o A statement that an individual will not suffer retaliation for filing a complaint
 - o Point of contact information for patients to request additional information
 - o Date the notice went into effect

164.522 Rights to request privacy protection for protected health information

a) Standard: Right of an individual to request restriction of uses and disclosures

- In emergency treatment situations, a covered entity (Nursing home etc.) that has agreed to a restriction of health information, can disclosed that information if it necessary for emergency treatment.
- If information is granted in emergency situations, the covered provider that released the information must request that the provider not further use the information or disclose the information.

164.524 Access of individuals to protected health information

a) Standard: access to protected health information

- Patients have the right to access any protected health information that is used in whole or in part to make decisions about that patient.
- Patients do not have the right to access their protected information that is compiled in reasonable anticipation of a civil, criminal, or administrative action proceeding

b) Implementation specifications: requests for access and timely action

- Services are required to permit a patient to request access to inspect or obtain a copy of protected health information that has been collected. (Written request)
- Services must act on a request within 30 days of receiving the request for information that is stored on the premises, 60 days if not stored on the premises.

d) Implementation specifications: denial of access

- If a service has grounds to deny access to health information, you must provide the individual with a written denial in plain language that explains the grounds for denial.
- If the service denies a request because it does not maintain the requested information, but knows where that information is maintained – the service must inform the patient where to request the access.

164.530 Administrative requirements

a) Standard: personnel designations

- Services are required to designate a privacy official and contact person.

b) Standard: training

- Services are required to train all members of the workforce on the policies and procedures with respect to covered healthcare information, that effect their workplace performance in regards to information.
- Services must document the completion of this training with their employees

e) Standard: sanctions

- Services must develop and apply sanctions against members of its workforce who failed to comply with privacy policies or procedures.

i) Standard: policies and procedures

- Policy and procedures should be reasonably designed to comply with the standards, taking into consideration the size and the nature of the activities that the service carries out.

164.534 Compliance dates for initial implementation of the privacy standards

- A service must be in compliance not later than 24 months following the effective date of this rule.

References:

Code of Federal Regulations, Title 45, Volume 1, Part 160 and 164

Standards for Privacy of Individually Identifiable Health Information: Final Rule, Federal Register, December 28, 2000

Administrative requirements in implementing HIPAA, Center for Medicare and Medicaid Services

An Overview of Medical Records Privacy and HIPAA, Sharon Lee, RN, C, CPHQ, Quality Credit Providers.

<http://www.hhs.gov/ocr/hipaa/>, Department of Health and Human Services