AMERIMED SOP
1.8.1 HIPAA
Rev 10/2020

OVERVIEW

When patients trust you enough to share their health information, you will have a more complete picture of their overall health. Breaches of privacy and security can have serious consequences for our patients, the facilities we service, us as an organization, and the individual responsible for the breach.

The federal government created the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to provide federal protections for patients through regulation. The integrity of Amerimed EMS, our patients and our customers is fully protected as long as every Amerimed EMS associate adheres to privacy guidelines.

SECTION A

Patient information may be received via phone, fax, facility, provider, family, and the patient themselves. It may be transmitted and/or stored on a computer, in an Electronic Health Record (EHR), on paper, or mobile devices such as tablets and cell phones. Patients have an array of rights with respect to that information and we have responsibilities for safeguarding it under The Health Insurance Portability and Accountability Act (HIPAA) Rules.

SECTION B

The HIPAA Privacy Rule requires health care providers to develop and distribute a notice that provides a clear, user friendly explanation of individual's rights with respect to their personal health information and the privacy practices of the provider. All patients should be provided with a copy of the Amerimed Notice of Privacy Practice on completion of each patient encounter, whether transport or refusal.

The Privacy Rule establishes national standards for individuals' privacy rights to understand and control how their health information is used and shared. In general, associates involved in the care of or financial processes of a patient may use and disclose PHI for treatment, health care operation activities, insurance carriers, other facility administrative departments, other providers involved with patient care — and other permissible or required purposes consistent with the HIPAA Privacy Rule — without obtaining a patient's written permission (e.g., consent or authorization).

Associates must limit the PHI disclosed to what is directly relevant to that person's involvement in the individual's care or payment for care. Use of or disclosure of PHI outside of what is legally required or approved should be done only with written approval from management. Appropriate verification of legal right to access or permission to share must be obtained prior to any other disclosures and should be handled by supervision, management or patient accounting associates following receipt of approved documentation.

Associates are expected to maintain compliance with all HIPAA requirements during verbal encounters with any non-approved individuals and refrain from discussions about patients in public areas.

SECTION C

.

The Privacy Rule protects individually identifiable health information held or transmitted in any form or media, whether electronic, paper, or oral. This includes specifics that identifies or generalities that create a reasonable basis to believe it can be used to identify the individual, particularly as it relates to:

- The individual's past, present, or future physical or mental health or condition
- The provision of health care to the individual
- The past, present, or future payment for the provision of health care to the individual

For example, any medical record which includes patient personally identifiable information:

- Certificate of Medical Necessity (CMN)
- Physician Certification Statement (PCS)
- 10-13 / 20-14 and other legal commitment forms
- Lab reports
- Hospital face sheet
- Photographs or photocopies of patient's driver license, insurance card, military service I.D., etc

Any documents containing PHI must be disposed of in approved, secured receptacles or shredded immediately using a mechanical shredding device. Each station has either a secured receptacle or electric shredding receptacle. Patient care records and other documentation should not be left exposed where accidental access or disclosures can occur. All paper documentation being retained for patient records should be secured in a non-opaque location as specified by AEMS guidelines. Crews are provided envelopes to secure documents that are to be provided to the receiving facility/care giver and internally to patient accounting.

No Amerimed associate will take pictures or videos (to include any device; camcorder, camera, cell phone, etc.) of patients or a patient's injuries regardless of the inability to see the patients face.

SECTION D

PHI may be disclosed by Amerimed associates, supervision/management, communications and administrative personnel as it relates to:

- Treatment provided before, during and/or after transport
- Treatment activities of another health care provider
- Review or assessment of the quality or competence of health professionals, or

- Fraud and abuse detection or compliance

- Payment activities of another involved facility or health care provider

Exposure related events

Health information is authorized by law to be disclosed to a public health authority for specific purposes:

- The purpose of preventing or controlling disease,

- Reporting vital events, such as disease exposure, births or deaths,

- Conducting public health surveillance, investigations, or interventions

PHI is authorized to be released to law enforcement in the event:

- A patient under a mandated custody order such as 10-13 or 20-13 escapes from custody or transport vehicle

- Information is needed to identify or apprehend an escapee or violent criminal.

- Such information will prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone you believe can prevent or lessen the threat (including the target of the threat).

SECTION E

ELECTRONIC SECURITY

Cybersecurity refers to ways to prevent, detect, and respond to attacks against or unauthorized access against a computer system and its information. Cybersecurity protects information or any form of digital asset stored on a computer or in any digital memory device

To support patient care, providers store electronic Protected Health Information (ePHI) in a variety of electronic systems, not just Electronic Health Records (EHRs). Knowing this, providers must remember that all electronic systems are vulnerable to cyber-attacks and must consider in their security efforts all of their systems and technologies that maintain ePHI. Only company provided electronic equipment may be utilized by associates in the service of their jobs.

Associates violating HIPAA Laws can be fined up to $250,000 and/or incarcerated.