

HIPAA BASICS FOR EMS PRACTITIONERS

Am I Covered by HIPAA?

If you work or volunteer for an agency that provides healthcare - including ambulance services and EMS agencies - and that agency bills for healthcare services, you are part of a HIPAA “covered entity.” As an employee or volunteer of a HIPAA covered entity, you must **comply with** and be **trained** on HIPAA and your agency’s HIPAA privacy, security, and breach policies.



What Does HIPAA Apply to?

HIPAA applies to **protected health information (PHI)**. PHI is information you learn about patients in your role as an EMS practitioner. Anything that could reasonably identify a patient and relates to the patient’s physical or mental health is PHI. The information does not have to include the patient’s name in order to be PHI.

Ask: “Would someone who knows the patient be able to identify the individual based on the information provided?” If the answer is yes, and the information relates to the health of the patient, that information is probably PHI protected by HIPAA.

PHI can come in ANY form, including:

- **Hard copy**
- **Digital (including photos and videos)**
- **Verbal**



When Does HIPAA Apply?

If you work or volunteer for a covered entity, HIPAA applies to you both on and off duty. You may only share PHI you learn while providing services for a covered entity when HIPAA says that you can – such as sharing for treatment, payment and operations.

Ask: “Am I sharing this PHI for a legitimate job-related purpose?” If you are not, you could be violating HIPAA.



When Can I Use or Disclose PHI?

Generally, when you are participating in treatment, payment, or operations activities (TPO), you may use or disclose PHI that is necessary to conduct those activities without patient authorization.



Examples:

- **Treatment** – You may share any PHI with first responders, hospitals and facilities, providers, and others involved in the patient’s treatment.
- **Payment** – You may share PHI with individuals that bill for the services you provide, such as billers and reviewers.
- **Operations** – You may review your and other practitioners’ trip reports and other medical records when conducting quality assurance/quality improvement (QA/QI) activities.

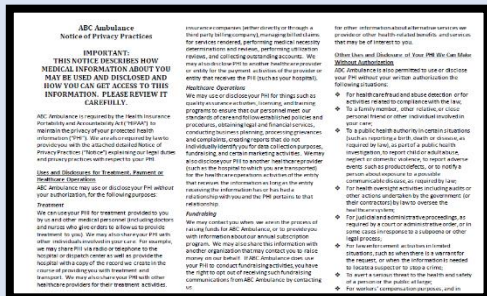
How Do I Handle the Notice of Privacy Practices?

Distribution

The Notice of Privacy Practices (NPP) should be provided to patients at the time of service in non-emergency treatment situations when doing so would not interfere with patient care and when the patient is not experiencing a medical emergency or under duress. **But, ALWAYS follow your agency’s policy on distributing the NPP.**

NPP Documentation

Document if you did/did not provide the NPP to the patient. **ALWAYS follow your agency’s policy on NPP documentation practices.**



Follow the Minimum Necessary Rule: Use or disclose only the minimum amount of PHI necessary to accomplish the required task:

Example: Remove identifying information from patient care reports before using them to conduct QA/QI if identifying information is not necessary for conducting the review.

HIPAA TIPS FOR EMS PRACTITIONERS

Sharing PHI With Law Enforcement



General Rules

- HIPAA generally does not apply to the police, so they cannot violate HIPAA.
- Police may speak directly to your patient.
- Police can serve your agency with a subpoena for your care report after the incident.
- When you are not releasing PHI (e.g., you alert law enforcement about a weapon on the scene), HIPAA does not apply, and you may release non-PHI to the police.

Tips for Releasing PHI

You may generally release limited, **necessary** PHI to law enforcement when:

- The police are trying to locate or identify a suspect, fugitive, missing person, or witness.
- A crime occurs during the response (e.g., the patient assaults a crewmember).
- You are treating the victim of a crime and the police are not going to use the information against your patient.
- You are required by your state law to release the PHI to the police (e.g., to report a gunshot wound or abuse/neglect).
- Releasing PHI would prevent imminent harm to someone.
- You are releasing information about the patient's destination.

NOTE: If you are unsure about whether you may release PHI to law enforcement, check with your supervisor or your agency's privacy officer.

Accessing PHI Securely

You may only access PHI to which you have a legitimate, work-related need to access. Never **snoop** (access a record just because you are curious, know the person, or some other **non**-business-related reason) on records. Electronic access to records is tracked in the system.

Reporting Breaches & HIPAA Issues

Report all known or **suspected** breaches and other HIPAA issues to a supervisor, compliance officer, or privacy officer immediately. This includes, but is not limited to:

- Any suspected or known improper disclosures of PHI;
- Any lost or stolen device or hard copy material containing PHI;
- Malware or other security threat; or
- Any known or suspected unauthorized access to PHI.



Sharing PHI With Patient's Family/Caregivers

You may disclose PHI to relatives, friends, or other individuals involved in patient's **care** if doing so is in the best interests of patient. For example, you may disclose the transport destination, general condition, and other general information about the patient.



Dealing With the News Media

You should not release PHI to the news media without written patient authorization.

Refer media requests to the appropriate spokesperson for your agency.



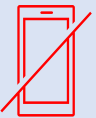
Posting About Work Online

Do not post about **patient** events on social media, even if you believe the information would not identify the patient. **Follow your agency's policy regarding social media postings.**



Personal Devices

Unless authorized, do not use **personal** devices to capture or transmit PHI. This includes texting and capturing photos or recordings during patient calls. **Follow your agency's policy on using devices for recording and sharing PHI.**



Electronic Devices - Best Practices

- Lock all devices when not in use.
- Report all lost or stolen devices **immediately**.
- Use unique passwords, change them periodically, and do not share passwords.
- Do not disable security settings on devices.
- Never leave an unsecured device unattended.

