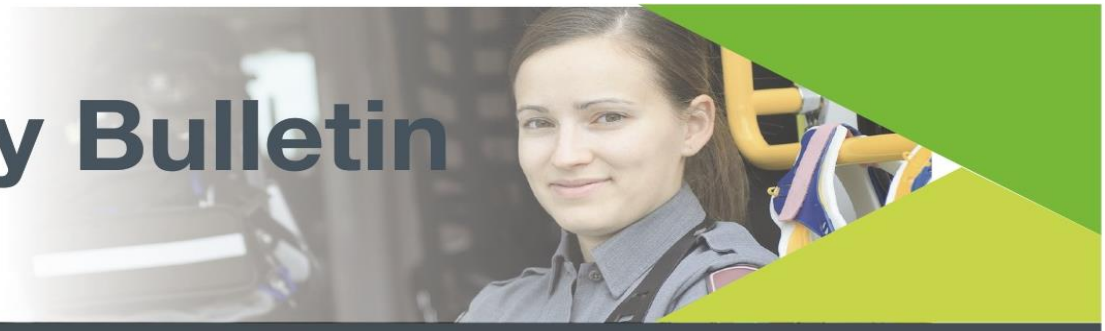

PHI (Protected Health Information) Security Breaches and Their Impact on EMS Agencies

With health data breaches being announced almost daily, EMS Agencies providing ambulance transport services need to understand exactly what is required for PHI security. However, there are distinctions in types of data that healthcare organizations keep on hand.

Patients need to be notified if their personal information is potentially accessed by unauthorized users, but not all data security incidents involve PHI. We'll dissect what makes PHI security different, and why it is treated differently than other data security breaches.

What is protected health information?
Protected Health Information (PHI) is any information about health status (medical records), or any financial information for payment (payment history) for health care that can be linked to a specific patient or individual. Health information means any information in any form (oral, written or recorded). Moreover, information, including demographic data that relates to the following is part of PHI:

- Created or received by a healthcare provider (EMS Agency), health plan, public health authority, employer, life insurer, school or healthcare clearinghouse.
- Relates to the past, present, or future physical or mental health or condition of any individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual.

"***Individual identifiable health information"*** is any information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

- Relates to the past, present, or future physical or mental health or condition of any individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual:
    - That identifies the individual; or
    - With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
    - Common identifiers, including but not limited to name, address, date of birth, social security number.

What are key data breach prevention measures?
According to HHS, there are four general rules that covered entities (CE's) must follow to ensure the protection of PHI:

- Ensure the confidentiality, integrity, and availability of all paper PHI & e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

As EMS Agencies determine the best security measures for their facility, it is essential for them to consider their size, complexity, and capabilities. The CE's technical, hardware, and software infrastructure must also be

reviewed, as well as the costs of security measures. Finally, every facility must consider the likelihood and possible impact of potential risks to paper PHI & e-PHI.

From there, EMS Agencies need to ensure they have the necessary administrative, technical, and physical safeguards in place. Again, a type of safeguard that works for one EMS Agency might not be necessary for another.

"A covered entity must identify and analyze potential risks to paper PHI & e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level**. Health and Human Services states on its website: "A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures."**
Risk assessments will also play a critical role in PHI security. Covered entities could prove through one of two ways that notification was not necessary if they have documentation proving that:

- its risk assessment demonstrates a low probability that the protected health information has been compromised by the impermissible use or disclosure;
- the application of any other exceptions to the definition of "breach."

What happens when a PHI data breach does occur?
If PHI security is compromised in an EMS Agency data breach, the notification process is essential. However, the **HIPAA breach notification rule** states that when unsecured PHI is compromised, then EMS Agencies and their business associates need to notify potentially affected parties. This is PHI **"that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance."** In other words, if

the information was encrypted, water or fire damaged and unreadable, or unable to be accessed then potentially affected parties do not need to be notified.

If more than 500 individuals are possibly at risk, then EMS Agencies must notify prominent media outlets serving the state or jurisdiction. Moreover, this notice must be given "without unreasonable delay" and in no case later than 60 days following the discovery of a breach. When more than 500 individuals are involved, the Secretary must also be notified.

If fewer than 500 people are affected, then covered entities need to make an annual report. However, these notices are due to the Secretary "no later than 60 days after the end of the calendar year in which the breaches are discovered."
It is also essential for EMS Agencies to have written policies and procedures in place that cover the breach notification process. EMS Agency staff at all levels need to be trained on those policies and procedures.

Working toward strong PHI security
Not all healthcare data breaches will involve PHI, but EMS Agencies need to remain vigilant in their approach to data security. Federal, state, and local regulations could all potentially have guidelines on how a data security breach should be handled. Some of those laws may not require that breach notification be given if medical data is compromised, but should addresses or social security numbers be exposed, then it is necessary.

Even so, EMS Agencies need to keep all safeguards up to date and ensure that they are compliant with state and local laws, as well as HIPAA compliant. PHI security can be compromised in numerous ways, which is why facilities have to be vigilant and able to adjust safeguards as necessary.