GENERAL ORDER 323.02

HIPAA Risk Analysis

EMERGENCY SERVICE BUREAU

Issue Date: **February 26, 2021**
Revision Date: **N/A**

APPLICABILITY

All Personnel

POLICY

The Howard County Department of Fire and Rescue Services (Department) is responsible, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), to ensure the privacy and security of all Protected Health Information (PHI) that we use or disclose. The foundation of compliance with HIPAA is the completion of a Risk Analysis to identify existing Risks and Vulnerabilities in the way we create, receive, maintain or transmit our PHI. This policy describes our general approach to our HIPAA Risk Analysis.

DEFINITIONS

- **Electronic Protected Health Information (ePHI) & Protected Health Information (PHI)** – any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media or paper form.

- **Risk** – the likelihood that a Threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability and integrity of ePHI, and other confidential or proprietary electronic information, or other systems assets.

- **Risk Assessment** – This is referred to as a Risk Analysis in the HIPAA Security Rule. A Risk Assessment is the process which:
  - Identifies the Risks to information system security and determines the probability of occurrence and the resulting impact for each Threat/Vulnerability pair identified given the security controls in place,
  - Prioritizes Risks, and;
  - Results in recommended possible actions/controls that could reduce or offset the determined Risk.

- **Risk Management** – means the major process components: Risk Assessment and Risk Mitigation.

- **Risk Management Team** –individuals who are knowledgeable about the covered entity's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up and technical security controls and who are responsible for the Risk Management process and procedures outlined in this Policy. The Department Risk Management team includes, but is not limited to:
  - HIPAA Compliance Officer
  - Privacy Officer(s)
  - Information Security Officer or designee
  - Other designated subject matter experts

- **Risk Mitigation** – This is referred to Risk Management per the HIPAA Security Rule. Risk Mitigation is the process that prioritizes, evaluates, and implements security controls that will reduce or offset the Risk determined in the Risk Assessment process to satisfactory levels within the Department given its mission and available resources.

- **Threat** – the potential for a particular Threat source to successfully exercise a particular Vulnerability. Threats are commonly categorized as:
  - *Environmental Threat* – External fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
  - *Human Threat* – Hackers, data entry, workforce/ex-workforce members, impersonations insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
  - *Natural Threat* – Fires, floods, electrical storms, tornados, etc.
  - *Technological Threat* – Server failure, software failure, ancillary equipment failure, etc.
  - *Other Threat* – Explosions, medical emergencies, misuse of resources, etc.

- **Threat Source** – means any person, circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system, which may be categorized as Environmental, Human or Natural and can impact the covered entity's ability to protect ePHI.

- **Vulnerability** – a weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of the system (e.g. security breach).

- **Workforce** – means employees, volunteers, trainees and other persons whose conduct, in the performance of work for a covered entity, is under the direct controls of such entity, whether or not they are paid by the covered entity.

PROCEDURES

The Department's HIPAA Risk Analysis will include an assessment of potential Risks and Vulnerabilities to the confidentiality, availability and integrity of all PHI that the Department creates, receives, maintains or transmits. This includes assessing any Risks and Vulnerabilities

to the confidentiality, integrity and availability of non-electronic PHI (such as papers and documents) and Electronic Protected Health Information (ePHI). At a minimum, the Risk Analysis will include a review of the Department's:

- General security hardware and procedures to protect our organization, vehicles and electronic assets.
- Computer servers (on or off-site) that store PHI.
- Computer network (including any local and wide area networks, communications servers and bandwidth connections, and storage devices and hardware).
- Databases where patient information is created, stored and accessed by the Department, whether on or off-site.
- Electronic media that stores ePHI such as hard drives, disks, CDs, DVDs, USB drives, thumb drives or other storage devices, transmission media, or portable electronic media.
- Electronic devices used for processing patient information (such as laptops and field data collection devices).
- Workstations and access points where PHI is created, accessed and used.
- Policies and procedures (written and unwritten) that involve the creation, use or access to ePHI.

Risk Assessments will be conducted throughout Information Technology (IT) system life cycles:

- Before the purchase or integration of new technologies, and changes are made to physical safeguards;
- While integrating technology and making physical security changes; and
- While sustaining and monitoring appropriate security controls.

Risk Assessment on an annual basis will include the following:

- Identifying and documenting all places where the physical (paper) PHI and e-PHI is stored, received, maintained, or transmitted by the Department (i.e., all sources of PHI whether on or off-site).
- Identifying and documenting all current and potential risks to the confidentiality, security, integrity, and availability of all PHI sources.
- Assessing the likelihood of each identified risk and assigning the risk to a "risk level" and "potential impact" category.
- Identifying and documenting any measures currently in place to address identified Risks, including policies, procedures, hardware, software, security devices, etc., and then identifying any methods that are not currently in place that may eliminate or mitigate the risk.
- Providing recommendations that may remedy identified Risks and Vulnerabilities, and improve the security, integrity, and availability of all ePHI sources.
- Implementing methods that might remedy identified risks and vulnerabilities, and improve the confidentiality, integrity, and availability of all ePHI sources.

IMPLEMENTATION SPECIFICATIONS:

Implementation specifications under HIPAA that are required must be implemented and documented as to how they were implemented. Implementation specifications under HIPAA that are "addressable" will be implemented as follows:

- If the implementation specification is reasonable and appropriate, the Department will implement it.
- If the implementation specification is determined to be inappropriate and/or unreasonable, but the security standard cannot be met without the implementation of an additional security safeguard, the Department may implement an alternative measure that achieves the addressable specification.
- If the Department meets the standards through alternative measures, the decision not to implement the specification will be documented, including the rationale for the decision, and a description of the alternative safeguard that was implemented.

REFERENCES

- None

SUMMARY OF DOCUMENT CHANGES

New General Order

FORMS/ATTACHMENTS

- None

APPROVED

William Anuszewski, Fire EMS Chief
Office of the Fire Chief

Author:

Sean Alliger, Assistant Chief
Emergency Services Bureau