| | Ethics & Compliance Department | | |
|---|---|---|---|
| | Policy No.: 51 | **Created:** | 01/2018 |
| | | **Reviewed:** | 06/2025 |
| | | **Revised:** | 06/2025 |

# HIPAA: SAFEGUARDS

## SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

## PURPOSE:

Envision Healthcare Operating, Inc. and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Safeguards policy to communicate that the Company will implement organizational safeguards to protected health information ("PHI") from any intentional or unintentional use or disclosure that violates a patient's right to privacy, and from any threat to the integrity and availability of that information.

## POLICY:

The Company will ensure that technical security services and mechanisms are in place to guard the integrity, confidentiality, and availability of PHI. Services include processes and tools to control and monitor information access. Security mechanisms will prevent unauthorized access to data that is resident on information systems, and that is transmitted over a communications network. The Security Official retains authority for compliance with this standard.

The Company will ensure that physical safeguards are in place to guard the integrity, confidentiality and availability of PHI. These safeguards relate to the protection of physical computer systems and devices from intrusion, from environmental hazards, and natural disasters. The Security Official retains authority for compliance with this standard.

### Physical Access to Medical Records

The records of all patients will be compiled in paper-based and/or computerized patient charts. In order to make patient information freely available to teammates yet simultaneously prevent access of unauthorized users, patient charts will be stored in, and not be allowed to circulate outside of, restricted areas.

Each Department Director is responsible for defining and maintaining appropriate access to the restricted areas within their department.

Paper charts should not be left open when not in use and should not be left unattended in public areas.

Computer screens should not be positioned for public viewing; when no alternative is available, privacy screens designed specifically for the monitors should be ordered. Electronic records should be closed when not in use.

**Handling Confidential Information in Meetings**

Using PHI during meetings or similar settings should be done in such a way that disclosure of information is not provided unnecessarily to unauthorized individuals.

Meetings where PHI is discussed should be attended by individuals who have been specifically invited or by individuals with a specific business purpose for attending. These meetings should be conducted in a secure area such that PHI is not overheard or viewed by unauthorized individuals.

All meetings with third party visitors (vendors, customers, regulators, etc.) who are not authorized to have access to PHI must take place in a fully enclosed conference room or office if PHI is being handled by teammates in the immediate vicinity of the meeting room.

When PHI has been recorded on black boards or white boards, it must be definitively erased before the authorized recipients of this information leave the area.

If documents containing PHI are distributed during the course of the meeting, and those documents are not required by the recipient for health care operations, the documents must be collected and destroyed at the completion of the meeting.

**Confidential Information and Equipment in Public Areas**

Teammates should be vigilant in ensuring that PHI is not inappropriately used or disclosed through the inappropriate use or location of equipment or other confidential materials.

Departments must not position any equipment, including telephones, workstations, fax machines, copiers, and printers in public areas such that PHI may be overheard or viewed by unauthorized individuals.

The display screens for all PCs, workstations, and dumb terminals used to handle sensitive data must be positioned such that they cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related public areas.

Fax machines and computer printers used to print sensitive data must be located in such a manner that the printouts cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related public areas.

Teammates who work on transportable computers (portables, notebooks, laptops, palmtops, etc.) and paper records should also be cognizant of their position with regard to unauthorized viewing of PHI.

Teammates should make every effort to conceal or screen paper charts, medical records, faxes, and other documentation containing PHI. Electronic records should be closed or screened when not needed for access. Verbal communication should be conducted in the most discreet manner possible.

Computer printouts, faxes, medical records, and other paper records should not be left in open work areas so as to expose the contents of the records. Files and papers should be put away when not in use.
Medical Records and charts should be kept and updated in appropriately designated areas. File cabinets should be locked when not appropriately supervised.

Faxes, computer printouts, and copies/originals should be collected as soon as possible and appropriately filed.

All activities pertaining to sensitive information must take place in areas that are physically secured and protected against unauthorized access, interference, and damage.

## POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.