

HIPAA Privacy and Security Compliance

HIPAA Privacy and Security Compliance

Policy #3000

Policy

Inova is committed to protecting the privacy of all individually identifiable health information that may include medical records, patient bills, and any paper or electronic records that identify patients. All employees, vendors, contracted workers or any person or entity with authorized access to Protected Health Information (PHI) are required to adhere to Inova's policies and procedures for HIPAA Privacy and Security as well as comply with all Federal, State, or Local privacy laws and regulations.

General Guidelines

Employee access to and disclosure of PHI should be limited to those tasks or duties necessary for fulfilling the responsibilities of their job or role at Inova. Expectations for access and disclosure can be found by referring to the Inova Patient Privacy and Security Policies provided by the Compliance and Information Technologies departments. Employees should seek advice and approval from their supervisor or the Chief Privacy Officer prior to accessing a patient or employee's medical record if there are questions or concerns related to their authorized access or use.

Should a HIPAA violation occur, managers are required to adhere to all processes associated with Progressive Discipline, to include the incorporation and usage of the Performance Decision Tree, prior to finalizing and administering any disciplinary action for an employee. (See Progressive Discipline Policy #3024, Appendix C: Inova Performance Decision Tree & Leader Tip Sheet). Results of decision-making and actions taken must be communicated to the Chief Privacy Officer or designee.

HIPAA Violations

Inova reserves the right to assess disciplinary actions in the event of HIPAA violations on a case-by-case basis. We also reserve the right and absolute discretion to vary the disciplinary steps outlined in this policy and associative policies (e.g. Policy #3024 Progressive Discipline) based on the facts in any particular case. If warranted and depending upon the offense, discipline may be more severe and may lead to immediate termination. In all but immediate termination, additional HIPAA training should be provided.

Examples of violations are as follows (this list is not all inclusive):

- Faxing or mailing patient information to the wrong recipient.
- Including portions of one patient's record in information provided to another patient.
- Forwarding an e-mail containing patient information to an individual who does not need that information to perform their job.
- Viewing patient information in a record that is not required to perform job duties; including co-workers, subordinates, family members or high profile patients.
- Using/disclosing patient information other than in the normal course of Inova's legitimate business. This includes sharing information inside or outside of Inova.
- Using patient information for personal gain.
- Posting identifiable patient information on social media sites.