Patient Privacy Violation Policy

ASC Policy

Effective Date: October 2019

Review/Revision Date:

Document Number: HIM 3.20

Responsible Party: Center Administrator

I. Purpose:

a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with Privacy Policies and Procedures of the entity, or the requirements of the Rule (45 CFR SS 164.530(e)(1). Accordingly, it is the intention of Andover Ambulatory Surgery Center to ensure the confidentiality and integrity of consumer and/or employee protected health information (PHI) as required by law, professional ethics, and accreditation and/or licensure requirements. This policy establishes agency policy, guidance, and standards for workforce performance expectations in carrying out the provisions of HIPAA, and the corrective action(s) that may be imposed to address privacy violations. This policy is in effective for all Andover Ambulatory Surgery Center non-physician employees. All physician employee HIPPA violations will be reported to the CEO and he/she will manage.

II. Policy:

a. Consumer and/or employee PHI information will be regarded as confidential, and may not be used or disclosed except to authorized users for approved purposes. Access to PHI is only permitted for direct consumer care, approved administrative and/or supervisory functions, or with approval of the Privacy Officer, Executive Director, or Human Resources Director.

III. Procedure:

Permitted Use and Disclosures

a. Andover Ambulatory Surgery Center is permitted to use or disclose PHI in the following instances:

   I. To the individual who is the subject of the PHI;

   II. In compliance with consent to carry out treatment, payment or health care operations;

   III. Without consent, if consent is not required and has not been sought;

   IV. In compliance with valid authorization;

   V. Pursuant to an Agreement.

Required Disclosures

a. Andover Ambulatory Surgery Center is required to disclose PHI in the following instances:

   I. To an individual, when requested under and as required by SS164.524 (Access of individuals to PHI) or SS164.528 (Accounting of disclosure of PHI) of the HIPAA Regulations;

   II. To specific private entities that provide services under contractual agreements (health benefits, life insurance, Workers Compensation, etc.) in order to provide such services;

   III. When required by the Privacy Officer, Executive Director, or Human Resources Director to investigate or determine compliance with HIPAA requirements.

Minimum Necessary

a. When using or disclosing PHI, or when requesting PHI from another covered entity, Andover Ambulatory Surgery Center will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Sanction Exemptions

a. Sanctions will not apply to disclosures by employees who are whistleblowers or crime victims. Andover Ambulatory Surgery Center is not considered to have violated PHI disclosure requirements if the disclosure is by an employee or business associate as follows:

Disclosure by Whistleblowers:

a. The employee is acting in good faith on the belief that Andover Ambulatory Surgery Center has engaged in conduct that is unlawful or otherwise violates professional or clinical standards.

b. That the care, services and conditions provided by Andover Ambulatory Surgery Center potentially endangers one (or more) Andover Ambulatory Surgery Center consumers, employees or a member of the general public.

c. The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered entity.

d. The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Andover Ambulatory Surgery Center.

e. The disclosure is made to an attorney retained by or on behalf of the employee or business associate for the purpose of determining legal options regarding disclosure conduct.

Disclosure by Crime Victims:

a. A covered entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is the victim of a criminal act discloses PHI to a law enforcement official about the suspected perpetrator of the criminal act, and the disclosed PHI is limited to identification and location purposes.

Mitigation:

a. Mitigating circumstances include conditions that would support reducing the sanction in the interest of fairness and objectivity. Andover Ambulatory Surgery Center will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of PHI in violation of HIPAA regulations.

Retaliation

a. Andover Ambulatory Surgery Center will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

   I. Exercises his rights or participates in the Andover Ambulatory Surgery Center complaint process.

   II. Files a complaint with the Secretary of Health and Human Services.

   III. Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing.

   IV. Opposes any act or practice unlawful under HIPAA, providing that the individual acted in good faith, believing that the practice was unlawful, the manner of opposition is reasonable, and does not involve disclosure of PHI in violation of HIPPA regulations.

IV. Disciplinary Sanctions:

a. Employees found to have violated PHI disclosure provisions will be disciplined in accordance with Andover Ambulatory Surgery Center Policy HIM 3.20, Standards of Conduct, up to and including termination of employment. The type of sanction will depend on the intent of the individual and severity of the violation. The offenses listed below, while not all inclusive, are organized according to the severity of the violation.

b. **Group I: Improper and/or unintentional disclosure of PHI or records.**

   I. This level of breach occurs when an employee unintentionally or carelessly accesses, reviews or reveals consumer or employee PHI to himself or others without a legitimate need-to-know. Examples include, but are not limited to: employees who discuss consumer information in a public area; an employee leaves a copy of consumer medical information in a public area; an employee leaves a computer unattended in an accessible area with consumer information unsecured.

c. **Group II: Unauthorized use and/or misuse of PHI or records.**

I. This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with Andover Ambulatory Surgery Center policies and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee looks up birth dates, address of friends or relatives; an employee accesses and reviews the record of a consumer out of curiosity or concern; an employee reviews a public personality's record.

d. **Group III and IV: Willful and/or intentional disclosure of PHI or records.**

I. This level of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent. Examples include, but are not limited to: an employee reviews a consumer record to use information in a personal relationship; an employee compiles a mailing list for personal use or to be sold.

V. Documentation:

a. **Initial Reporting:**

I. Employees who observe or are aware of a breach must immediately report it to his/her Supervisor. The Supervisor will report the breach to the Privacy Officer, who will notify the Executive Director and Human Resources Director.

II. Failure to report a breach of which one has knowledge will result in appropriate disciplinary action. Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

b. **Clear-cut Level I Breaches:**

I. For a breach involving any staff that is clearly a Level I breach, the Privacy Officer, in conjunction with the employee Supervisor, Executive Director and Human Resources Director, will develop and implement an appropriate Plan of Correction, and in a timely manner. (See guidance chart below)

c. **Breaches Other Than Clear-cut Level I Breaches (Level II-Level IV):**

I. For all levels other than a clear-cut Level I breach, the Privacy Officer will establish an Investigation Team that will include senior Management and Human Resources representation, and legal counsel participation or consultation.

II. The Investigation Team will conduct an appropriate investigation, commensurate with the level of breach and specific facts. This may include, but is not limited to, interviewing the employee accused of the breach, interviewing other employees or consumers, and reviewing documentation.

III. Upon conclusion of the investigation, the Investigation Team will prepare a written report including all findings and conclusions regarding the alleged breach, and forward it to the Privacy Officer. The Executive Director will make final determination of the appropriate disciplinary action, based on the report of the Investigation Team. (See guidance chart below)

IV. All HIPPA Violations will be assigned a "Level" based on severity that is decided by Administrative Team.

d. **Reporting and Filing Requirements:**

I. For all levels of breach, after final resolution the initial report and all supporting documentation will be filed in a confidential file with the Privacy Officer. A copy of the report and supporting documentation will also be placed in the Personnel File of the employee.

e. **Principles:**

I. Protected health information (PHI) is confidential and protected from access, use, or disclosure except to authorize individuals requiring access to such information. Attempting to obtain or use, actually obtaining or using, or assisting others to obtain or use PHI, when unauthorized or improper, will result in counseling and/or disciplinary action up to and including termination.

f. **Definitions and Caveats:**

I. PHI = Protected health information; this includes all forms of patient-related data including demographic information

II. Depending on the nature of the breach, violations at any level may result in more severe action or termination

III. Levels I-III are considered to be without malicious intent; Level IV connotes malicious intent

IV. At Level IV, individuals may be subject to civil and/or criminal liability

V. For any offense, a preliminary investigation will precede assignment of level of violation.

VI. All Andover Ambulatory Surgery Center HIPPA violations will be reported to the Health and Human Services via their website within 30 days of notification of the violation as required.

Level of Violation	Examples	Minimum Disciplinary Corrective Action
Level I	• Misdirected faxes, e-mails & mail. • Failing to log-off or close or secure a computer with PHI displayed. • Leaving a copy of PHI in a non-secure area. • Dictating or discussing PHI in a non-secure area (lobby, hallway, cafeteria) • Failing to redact or de-identify patient information for operational/business uses. • Leaving detailed PHI on an answering machine. • Improper disposal of PHI. • Transmission of PHI using an unsecured method.	• First offense: written counseling • Second offense within one year: written warning. • Third offense within one year: suspension or termination • Notify Privacy Officer of all incidents. • Retake Compliance **HIPPA Health streams** Training.
Level II	• Requesting another individual to inappropriately access patient information. • Inappropriate sharing of ID/password with another coworker or encouraging coworker to share ID/password. • Failure to secure data on mobile devices through encryption/password.	• First offense: written warning • Second offense within one year: suspension or termination. • Notify Privacy Officer of all incidents. • Retake Compliance **HIPPA Healthstreams** Training.

Level III	•Releasing or using aggregate patient data without facility approval for research, studies, publications, etc. •Accessing or allowing access to PHI without having a legitimate reason relating to your specific job duties. •Giving an individual access to your electronic signature. •Accessing patient information due to curiosity or concern, such as a family member, friend, neighbor, coworker, famous or "public" person, etc. •Posting PHI to social media.	• First offense: written warning, suspension and/or termination based on level of severity. • Second offense: suspension or termination based on level of severity. • Notify Privacy Officer of all incidents. • Retake Compliance **HIPPA Healthstreams** Training.
Level IV	• Releasing or using data for personal gain. • Compiling a mailing list to be sold for personal gain or for some personal use. • Disclosure or abusive use of PHI Tampering with or unauthorized destruction of information.	• Termination • Violation will be reported to appropriate licensing boards and third party agencies when required. Notify Privacy Officer of all incidents.