



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy and Security</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>Sanctions Policy</b>	<b>Revision Date:</b>	<b>9/30/09</b>
<b>Policy #:</b>	<b>ISP-010</b>	<b>Review Date:</b>	<b>9/30/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>3</b>

---

**Scope:**

This policy applies to all workforce members of Essent Healthcare, Inc., (“Essent”).

**Purpose:**

This policy outlines the sanctions that will be imposed on any workforce member who accesses, uses, or discloses sensitive information without proper authorization.

**Policy:**

It is the policy of Essent that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. Essent will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. *Note: Employees are not allowed to use their system access rights to access the system for personal reasons – access to all Essent information systems is for legitimate business purposes only.*

---

**Definitions**

**Sensitive information** includes, but is not necessarily limited to, the following:

1. **Protected Health Information (PHI)** – Any individually identifiable health information that is created, maintained, stored, or transmitted by the facility.
2. **Electronic Protected Health Information (ePHI)** – PHI that is in electronic format.
3. **Personnel files** – Any information related to the hiring and/or employment of any individual who is or was employed by Essent.
4. **Payroll data** – Any information related to the compensation of an individual during that individual’s employment with Essent.
5. **Financial/accounting records** – Any records related to the accounting practices or financial statements of Essent.
6. **Other information that is confidential** – Any other information that is sensitive in nature or considered to be confidential.

**Workforce:** (As defined in the HIPAA Regulations), employees, volunteers (board members, community representatives), trainees, students, contractors, and other persons under the direct control of a covered entity (hospital).



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy and Security</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>Sanctions Policy</b>	<b>Revision Date:</b>	<b>9/30/09</b>
<b>Policy #:</b>	<b>ISP-010</b>	<b>Review Date:</b>	<b>9/30/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>3</b>

---

### Procedures:

- 1) When using or disclosing sensitive information, Essent honors the “*minimum necessary standard*”. This means that only the minimum amount of information needed to complete the task at hand should be used or disclosed. For example, when responding to a documentation request by an insurance company, it would be appropriate to release documentation related to the visit or claim in question. It would not be appropriate to release the entire medical record.
- 2) All workforce members will receive education and sign an acknowledgement of their responsibility to protect sensitive information from unauthorized use or disclosure. The Human Resources Department shall maintain copies of signed confidentiality agreements in each employees personnel file.
- 3) All workforce members are responsible for protecting sensitive information from unauthorized use or disclosure at all times.
- 4) Unauthorized use or disclosure of protected health information will result in disciplinary action up to and including termination, professional discipline, and potentially civil penalties and/or criminal prosecution.
- 5) **Unintentional** unauthorized use or of disclosure sensitive information will result in a verbal or written reprimand depending on the severity of the offense. Repeat offenses will result in additional disciplinary action up to and including termination of employment. In addition, the HHS Office for Civil Rights (OCR) has the authority to impose civil penalties, including significant fines for violators who unintentionally disclose information. OCR may also recommend that violators be subject to criminal prosecution by the Department of Justice. Examples of unintentional disclosure subject to verbal or written reprimand include:
  - a) Leaving computer systems that access PHI unattended and/or failure to log-off system
  - b) Accessing ones own medical record (or the record of a minor child) without proper authorization
  - c) Negligence leading to improper disclosure



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy and Security</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>Sanctions Policy</b>	<b>Revision Date:</b>	<b>9/30/09</b>
<b>Policy #:</b>	<b>ISP-010</b>	<b>Review Date:</b>	<b>9/30/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>3</b>

---

- 6) A follow-up audit shall be conducted on all individuals who receive reprimands under this policy within 6 months of resuming work to ensure that there are no repeat offenses. These follow-up audits shall be conducted as an addition to the hospital's normal monthly privacy audits.
- 7) ***Intentional*** unauthorized use or disclosure of sensitive information for commercial gain, personal reasons, and/or to cause malicious harm will result in immediate suspension or termination of employment. In addition, the Office for Civil Rights (OCR) has the authority to impose significant civil penalties against individuals who improperly disclose PHI.

For disciplinary purposes, intentional unauthorized disclosures are divided into two categories:  
Level I and Level II:

- a) Examples of ***Level I offenses*** include discussing patient information with others for non-work related purposes (gossiping), accessing medical records of friends or family members without proper authorization, accessing medical records of co-workers or other patients for non-work related purposes, and repeat of unintentional offenses described above. Level I offenses are punishable by a written reprimand or three day suspension of employment depending on the severity of the offense.
- b) Examples of ***Level II offenses*** include leaking patient information to members of the press, selling or releasing sensitive information for personal gain, and/or using or disclosing sensitive information in a malicious manner. Level II offenses will result in immediate termination of employment.
- 8) All sanctions applied to employees as a result of a violation (or pattern of violations) of the HIPAA policies and procedures will be documented in the Employee's personnel file.
- 9) Disclosure of violations by whistleblowers and workforce member crime victims will not result in disciplinary action.
- 10) If a workforce member believes in good faith that Essent has acted unlawfully or violated professional or clinical standards, or that its care or services potentially endanger a patient, employee, or the public, and in that connection discloses PHI to a health oversight agency, health care accreditation organization, appropriate public health authority, or to an attorney retained by



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy and Security</b>	<b>Effective Date:</b>	<b>4/20/05</b>
<b>Subject:</b>	<b>Sanctions Policy</b>	<b>Revision Date:</b>	<b>9/30/09</b>
<b>Policy #:</b>	<b>ISP-010</b>	<b>Review Date:</b>	<b>9/30/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>3</b>

---

the disclosing person, the disclosure is not considered a violation of the HIPAA Regulations or Essent Policies and Procedures.

- 11) Essent employees who are the victim of a work-related crime may release information to law enforcement representatives without disciplinary action. The information may be released provided that:
- a) The protected health information disclosed is about the suspected person responsible for the crime; and
  - b) The protected health information disclosed is limited to facility directory information (patient name, location in the hospital, general condition such as critical, stable...).
- 12) Essent will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual or other person for:
- a) Filing a complaint with the Secretary of DHHS under subpart C of part 160 of the HIPAA regulation;
  - b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
  - c) Opposing any act or practice made unlawful in the HIPAA regulation, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA regulation.

### **References:**

HIPAA Section 164.308(a)  
OIG Compliance Guidance for Hospitals  
NIST Publication 800-12  
NIST Publication 800-18  
NIST Publication 800-53  
ARRA 2009