



	<u>Effective Date</u>		
	<b>July 2007</b>		
	<u>Number</u> <b>HP 015</b>	<u>Replaces Policy</u>  <b>NEW</b>	
<u>Title</u> <b>Sanctions for Privacy and Information Security Violations</b>	<u>Date Revised</u> <b>July 2007</b>	<u>Date Reviewed</u>	<u>Next Scheduled Review Date</u> <b>July 2010</b>
<u>Signature</u>  _____	<u>Scope of Responsibility</u>  <b>Compliance/HIPAA</b>		
<b>Chief Privacy Officer</b>			

**Purpose:** To facilitate compliance with the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), 45 CFR Parts 160 and 164, Administrative Requirements and HIPAA Standards for the Protection of Electronic Protected Health Information (Security Standards), 45 CFR Parts 160, 162, and 164. To establish guidelines for sanctions for violations of IMH privacy and information security-related Policies

**Policy:** Sanctions for privacy and information security-related violations must be applied consistently. Each of the examples in the Procedure section, as well as any patient privacy-related and/or information security-related violation, must be addressed through privacy and information security sanctions as outlined by the Executive Compliance Committee and recommended by the HIPAA Team.

**Procedure:** This section describes methods for determining the response to a privacy and/or information security violation. The procedure includes an outline of categories of violations with examples and recommended appropriate actions. The IMH Human Resources Director should be involved in all policy and disciplinary action decisions. **Please note:** The examples and recommended actions are not designed to capture every situation involving privacy and information security violations.

The Chief Privacy Officer (CPO) and/or Chief Compliance Officer (CCO) and employee's manager must investigate several factors before assigning a category of violation (see Violation Categories and Examples). Questions to consider are:

- ❖ What is the severity?
  - How many patients were affected?
  - To what degree was a patient harmed?
  - To what degree was the confidentiality, integrity, and/or availability of systems or data impacted?
  - To what degree did the action place the facility's or the enterprise's systems or network at risk?

Policy:  
Policy Number:

- ❖ Was the inappropriate action **negligent** or **purposeful**?
- ❖ Did the inappropriate action cause harm or is it likely to cause harm to a patient or others?
- ❖ To what degree was the facility able to verify the specifics of a situation through audit trails, interviews, or other facts?

In addition to the nature of the violation itself, answers to the following questions may affect the severity of disciplinary action:

- ❖ What is the employee's past work record?
- ❖ Has the employee been disciplined for violations of Policies and Procedures or Information Security Standards in the past?
- ❖ How long has the person been employed?
- ❖ What is the employee's quality of service to the facility?
- ❖ Does the employee have any written warnings for violations in his or her HR file?

As the CPO and/or CCO becomes aware of a potential violation of an IMH policy or standard, the CPO and/or CCO must discuss the situation with the affected employee's department supervisor. Depending upon the severity of the item, the CPO and/or CCO or individual's supervisor may consult with Human Resources Director or IMH's Chief Information Security Officer.

### **Violation Categories and Examples**

For purposes of this policy two violation categories will be used and examples of each provided. The two categories are:

- Negligent
- Purposeful

#### **Negligent Violation Examples:**

- ❖ **Not properly verifying individuals by phone, in person, or in writing. (Negligent)**

Example: A radiology technician receives a call from a physician who is calling for a status report on his patient. The technician does not

Policy:

Policy Number:

recognize the voice of the physician but releases the information on the faith that this person is a physician involved in the patient's care. The physician/person calling is determined, after a patient complaint, to be a friend of the patient and not involved in the care of the patient at all.

Negligent Violation: Failure to verify requestor.

Recommended Action: Oral warning with retraining.

Example: A unit clerk is overheard receiving a call from a patient's family member and, without verifying the person on the phone, proceeds to provide detailed information about the patient's status.

Negligent Violation: Failure to comply with the Patient Information Pass Code Policy.

Recommended Action: Written warning with retraining.

❖ **Improper disposal of protected health information (PHI) (Negligent)**

Example: When performing monitoring on a nursing unit, the CPO discovers a patient label in the regular trashcan. Negligent Violation: Failure to safeguard protected health information.

Recommended Action: The CPO should report this as an accidental disclosure and ensure that the employees on the unit as well as physicians receive appropriate education and are retrained on all policies as appropriate for their job duties and responsibilities.

❖ **Improper protection of medical records or other PHI (Negligent)**

Example: Respiratory therapists are found to be leaving medical records on counters or other areas on the unit without reasonable safeguards in place and in areas where PHI is accessible by unauthorized individuals.

Negligent Violation: Failure to safeguard protected health information.

Recommended Action: Staff should be re-trained on the policy and procedures. The work areas should be surveyed to ensure that reasonable safeguards are applied to further protect patient privacy. An oral warning with discussion of the policy, procedure and requirements should take place with the responsible employee(s).

❖ **Failure to verify a patient's Directory Opt out status. (Negligent)**

Example: A unit clerk receives a call on the unit from someone who says he is "a friend of the patient" and just wants to check to see if the patient has been discharged yet. The individual does not ask for a patient information pass code or otherwise verify but says, "No she is still a patient." The individual calling is an abusive spouse. When the spouse called the front desk he was told they had no information about the patient. The spouse then used a secondary calling route by contacting the unit to determine if the patient was indeed at the hospital.

Policy:

Policy Number:

Negligent Violation: Failure to comply with the patient's right to opt out of the Directory and failure to use the Patient Information Pass Code Policy.

Recommended Action: Written warning with retraining on the policies.

❖ **Faxing information to an incorrect fax number in error. (Negligent)**

Example: A case manager is working with an insurance Iverson Memorial Hospital to get a patient's stay certified. Instead of pre-programming fax numbers, the case manager dials the number and transposes a number, inadvertently faxing information to a beauty salon.

Negligent Violation: Failure to safeguard protected health information.

Recommended Action: Oral warning with retraining. In addition, the employee should be instructed to pre-program fax numbers and check fax numbers at least annually.

❖ **Not accounting for disclosures outside of treatment, payment or healthcare operations within the correct system or using a manual process. (Negligent)**

Example: While spot-checking the Accounting of Disclosures (AOD) in the Correspondence module, the CPO discovers that a recent dog bite called to the state as required was not included in the accounting for disclosures.

Negligent Violation: Failure to comply with the Accounting of Disclosures Policy.

Recommended Action: Oral warning with retraining. In addition, the dog bite information should be appropriately entered and the disclosure recorded in the AOD. Training and education should be performed in the area where the disclosure was made and emphasis given to all employees on the importance of entering disclosures into the AOD.

❖ **Failure to provide a private environment to discuss PHI. (Negligent)**

Example: A physician needs to discuss a patient's drug use with the patient but does not ask her if she wants her friends and family to step out of the room prior to the discussion. The physician then proceeds to discuss the drug abuse and effects on the unborn fetus with others present. The patient submits a complaint.

Negligent Violation: Failure to comply with the minimum necessary requirement and the uses and disclosures for care and notification purposes requirement.

Recommended Action: Disciplinary action, pursuant to the hospital's medical staff by-laws and rules and regulations, including a discussion with the physician and privacy retraining should be undertaken.

Policy:

Policy Number:

Example: A nurse performs a nursing assessment for an OB patient with several members of the patient's family present. The nurse did not ask the patient if she would like the visitors to step out of the room.

Negligent Violation: Failure to meet the minimum necessary or uses and disclosures for care and notification purposes requirements.

Recommended Action: Oral warning with retraining.

Example: A patient comes to the nursing unit to ask a question of his physician. The physician then proceeds to explain, "You cannot do that, you are HIV positive" in what the patient terms as a loud voice.

Negligent Violation: Failure to safeguard protected health information and meet the minimum necessary requirement.

Recommended Action: Disciplinary action, pursuant to the hospital's medical staff by-laws and rules and regulations, including a discussion with the physician and privacy retraining should be undertaken.

❖ **Leaving Detailed PHI on answering machine. (Negligent)**

Example: A patient calls to complain about an inappropriate disclosure of her PHI. The patient states that an employee of the Radiology Department called her home and left the results of her mammogram, which were abnormal, on the answering machine. The employee requested that the patient return to the facility for additional testing. The patient's son retrieved the message from the answering machine.

Negligent violation: Failure to comply with reasonable safeguards and minimum necessary requirements.

Recommended Action: Oral warning with retraining.

❖ **Failure to properly safeguard PHI or systems storing PHI. (Negligent)**

Example: During routine security monitoring rounds, an employee is seen leaving his workstation without signing off his opened clinical system.

Negligent Violation: Failure to safeguard protected health information.

Recommended Action: Oral warning with retraining.

Example: The main computer room of a hospital is not locked. A curious member of the custodial staff enters the room to look around and accidentally disconnects a network cable from a server, disabling the hospital's computer network.

Negligent Violation: Failure to control access to locations in which electronic information systems are housed.

Policy:

Policy Number:

Recommended Action: Oral warning with retraining of the employee with responsibility for physical security of the main computer room.

❖ **Not forwarding appropriate information or requests to CPO or designee for processing. (Negligent)**

Example: A nurse has agreed to a patient's request for a copy of his medical record. The nurse then proceeds to forget to tell HIM or the CPO of the request.

Negligent violation: Failure to comply with the patients' right to access.

Recommended Action: Oral warning with retraining. The CPO is notified of the request and asked to follow-up.

❖ **Careless handling of usernames and passwords. (Negligent)**

Example: An employee notices a user looking under her keyboard before logging into the workstation. The employee examines the keyboard later and discovers the user had written her login name and password on a sticky-note and attached it to the bottom of the keyboard.

Negligent Violation: Failure to maintain the confidentiality of system credentials.

Recommended Action: Oral warning with retraining.

❖ **Inadequate information security training procedures. (Negligent)**

Example: New employees in some departments do not receive information security training in accordance with the facility's information security training and awareness program and with Ivinson Memorial Hospital policies and standards. The CPO assumes that supervisors and co-workers explain the need for information security to new employees.

Negligent Violation: Failure to train staff in accordance with the facility's information security training and awareness program.

Recommended Action: At a minimum, oral warning to the CPO with retraining about key CPO job responsibilities.

❖ **Connecting the Ivinson Memorial Hospital network to another external network without boundary protection. (Negligent)**

Example: A therapist uses a dial-up connection (modem) to connect to the Ivinson Memorial Hospital network and review patient information. Simultaneously using the same computer device, the therapist establishes a broadband connection to a cable Internet provider with no boundary protection or firewall in place between the two networks (the Ivinson Memorial Hospital network and the Internet provider's network or Internet).

Policy:

Policy Number:

Negligent violation: Connecting a computer to the Ivinson Memorial Hospital network that is simultaneously connected to another external network without adequate boundary protection.

Recommended Action: Oral warning to the therapist with retraining.

❖ **Exposure of Ivinson Memorial Hospital information systems to malicious code. (Negligent)**

Example: An employee has a Ivinson Memorial Hospital-owned laptop computer that he takes home and connects to the Internet. While online at home, the computer is not protected by a firewall and becomes infected with a virus. When the employee brings the computer back to work and connects it to the Ivinson Memorial Hospital network, the virus spreads to the Ivinson Memorial Hospital network.

Negligent violation: Failure to use sufficient protection against malicious code when connecting to the Internet.

Recommended Action: Oral warning to the employee with retraining.

Purposeful Violation Examples:

❖ **Accessing or using PHI without having a legitimate need to do so. (Purposeful)**

Example: An employee who is “curious” about the status of a friend who is having surgery accesses the record.

Purposeful Violation: Failure to meet the minimum necessary requirement.

Recommended Action: Written warning with retraining.

Example: An HIM employee observes a physician pulling patients’ medical records from another physician’s stack of charts. The employee questions the physician about his actions. The physician states that he knows the stack will have interesting cases in it. The CPO investigates and discovers no patient/ physician relationship or colleague requests.

Purposeful Violation: Failure to meet the minimum necessary requirement.

Recommended Action: Disciplinary action, pursuant to the hospital’s medical staff by-laws and rules and regulations, including a discussion with the physician and privacy retraining should be undertaken.

❖ **Allowing another employee to utilize any systems via your password. (Purposeful)**

Policy:  
Policy Number:

Example: A nurse in the ER has determined that it is much easier to sign on a specific computer in the morning for the entire department to use rather than signing on and off all day. During routine audit trails it is found that the nurse's log on is matching with a patient for whom she did not care for and therefore did not have a legitimate "need to know" the PHI that was accessed.

Purposeful violation: Failure to comply with reasonable safeguards requirement.

Recommended Action: Oral warning with retraining.

❖ **Disclosure of PHI to unauthorized individual or Ivinson Memorial Hospital. (Purposeful)**

Example: An employee whose friend has ownership in a local rehab clinic uses his access to gather information about prospective patients for the clinic. The clinic calls the patients and solicits their business.

Purposeful violation: Failure to comply with the reasonable safeguards and minimum necessary requirements.

Recommended Action: The employee should be terminated.

❖ **Disclosing PHI without a business "need to know." (Purposeful)**

Example: During the course of his job duties, a lab technician accessed a co-worker's test results. In turn, the lab technician shared the results with other co-workers who did not need to know the information to perform their job responsibilities.

Purposeful Violation: Disclosed PHI to individuals with no business "need to know."

Recommended Action: Written warning with retraining on the policies.

❖ **Sale of PHI to any source. (Purposeful)**

Example: An HIM Director's friend stops by work on weekends to visit. He often sits in her office and visits while the HIM Director is working on various tasks. The HIM Director has witnessed the friend compiling patient names and addresses and selling them to a local telemarketing Ivinson Memorial Hospital for money.

Purposeful violation: Failure to meet reasonable safeguards requirements.

Recommended Action: The HIM Director should be terminated per hospital policy for the potential harm this could cause patients.

Policy:

Policy Number:

Employees should be re-educated on having friends, and/or family members at work where PHI may be accessible.

❖ **Any uses or disclosures that could invoke harm to a patient. (Purposeful)**

Example: An Emergency Room registrar calls the spouse of a patient to let him know that his wife is in the Emergency Room and claiming to have been abused by him. The registrar is a friend of the husband and wants to let him know where his wife is. The wife was abused and her records are marked as “confidential” in the system.

Purposeful violation: Failure to meet reasonable safeguards and minimum necessary requirements.

Recommended Action: The registrar should be terminated.

❖ **Connecting unapproved devices to the Ivinson Memorial Hospital network. (Purposeful)**

Example: A doctor has a personal digital assistant (PDA) that he brings to work and connects to his workstation, downloading patient information so he will have access to it at home. The PDA has wireless connectivity capabilities and minimal security. The doctor did not consult with the facility’s Information Security Officer about Ivinson Memorial Hospital-required safeguards for PDAs prior to connecting the device to the Ivinson Memorial Hospital network.

Purposeful violation: Unauthorized connection of a non-Ivinson Memorial Hospital-owned device to the Ivinson Memorial Hospital network.

Recommended Action: Oral warning to the doctor with retraining about the rationale for standards.

❖ **Failure to secure confidential information. (Purposeful)**

Example: An insurance provider contacts a hospital office to get information about the treatment of one of its customers. A clerk at the hospital transmits the requested information via Internet email without securing the contents.

Purposeful violation: Transmission of confidential information using an insecure, unapproved method.

Recommended Action: Written warning to the clerk with retraining.

Policy:

Policy Number:

❖ **Exposure of Ivinson Memorial Hospital information systems to malicious code. (Purposeful)**

Example: An administrative assistant in a hospital receives an unexpected email from an unknown third party with an attachment. They open the attachment, since the email subject line appears interesting. The attachment contains a virus that infects the assistant's computer and starts emailing itself to other addresses in the assistant's address book.

Purposeful violation: Failure to use sufficient protection against malicious code.

Recommended Action: Oral warning with retraining.

❖ **Compromising physical security measures. (Purposeful)**

Example: A vendor enters a facility to service computer systems in public areas, receiving a visitor badge that does not open electronic locks in the building. When the vendor needs to retrieve something from his car, an employee lets him borrow an employee badge so he can use a side door instead of going through the front entrance. The employee badge will open some restricted areas within the facility.

Purposeful violation: Improper control of security credentials.

Recommended Action: Written warning with retraining.

❖ **Misuse of Ivinson Memorial Hospital information systems. (Purposeful)**

Example: A biller at a billing center uses the network access to the Internet on a Ivinson Memorial Hospital computer to view adult or other inappropriate web sites.

Purposeful violation: Misusing the Ivinson Memorial Hospital network to view inappropriate material.

Recommended Action: A *minimum* of a written warning and retraining. Termination, and referral to law enforcement agencies for investigation may be warranted, depending on the nature of the material accessed.

❖ **Misuse of confidential Ivinson Memorial Hospital information. (Purposeful)**

Example: A collector at a billing office writes down names, social security numbers, and credit card numbers from patient records and attempts to use them to purchase items over the Internet and apply for credit cards.

Policy:

Policy Number:

Purposeful violation: Stealing information from Iverson Memorial Hospital information systems to commit identity theft.

Recommended Action: Termination and referral to law enforcement agencies for investigation and criminal prosecution.

❖ **Deliberately compromising electronic information security measures. (Purposeful)**

Example: A Hospital Chief Information Officer (CIO) decides to create a private access point into the facility's network. In an attempt to cover his actions, he uses a known vulnerability in one of the routers to reset its password; changing the password to one of his own choosing and disabling event reporting. He then creates an access point through a switch attached to the router.

Purposeful violation: Disabling information security tools, bypassing security measures, and misusing tools that can compromise information security systems.

Recommended Action: Termination and audit of CIO activities within facility information systems.