SOUTH PENINSULA HOSPITAL

POLICY# **HW-**

SUBJECT: **TERMINATION OF ACCESS PROCEDURE**

DEPARTMENT: **HOSPITAL WIDE**

APPROVED BY: **ADMINISTRATION**

APPROVAL DATE:

Introduction: South Peninsula Hospital (SPH) has adopted this Termination Procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations as well as acknowledge our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of SPH must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Assumptions:

This Termination Procedure is based on the following assumptions:

- · In any organization, people are the greatest asset in maintaining an effective level of security.
- · Conversely, people are the greatest threat to data security and confidentiality.
- · A terminated employee may pose a threat to data security and confidentiality, particularly if dissatisfied with his or her employment or termination.

SCOPE: **HOSPITAL WIDE**

POLICY: HIPAA and the DHHS security and privacy regulations require termination procedures for all personnel with access to individually identifiable health information..

- Department managers and the director of human resources are responsible for notifying the manager of Information Systems of employees and others, such as independent contractors, who will be leaving SPH's employ or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to health information.
- Department managers and the director of Human Resources are responsible for notifying the manager of Information Systems of employees and others, such as independent contractors, who through reassignment or otherwise no longer need the level of access that they had had so that their level of access can be adjusted.
- Any other data user who becomes aware that a data user is leaving SPH’s emply either permanently or for an extended or unexplained absence should report the matter to their department manager or the manager of Information Systems for a determination of whether to revoke/suspend that person's access.

- Upon termination of an employee or other person with access, the manager of Information Systems will immediately take the following actions:

    - Revoke access privileges, such as user-IDs and passwords, to system and data resources and secure areas.
    - Retrieve all hardware, software, data, access control items, and documentation issued to or otherwise in the possession of the data user.
    - Arrange for an exit briefing to verify retrieval of all items, to discuss any security/confidentiality concerns with the data user, and to remind the data user of the continuing need to protect data security and patient confidentiality.
    - Notify human resources of completion of the termination procedure so that the data user can receive any final pay due.
    - Keep records of the termination procedure for each such person, including the retrieval of security-related items, such as passwords, and information system assets, for not less than six years from the termination date.

- When necessary, the manager of Information Systems, the manager of Health Information Management, a facility administrator or director of Human Resources will arrange for security escort of terminated personnel from the facility and for an immediate audit of their accounts to detect any security or confidentiality threats or breaches.

Enforcement

All officers, agents, and employees of SPH **must** adhere to this policy. SPH will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with SPH's Employee Corrective Action Plan.

SPECIAL CONSIDERATIONS: **NONE**

REFERENCES:

SOUTH PENINSULA HOSPITAL

POLICY# **HW-**

SUBJECT: **RESPONSE PROCEDURE**

DEPARTMENT: **HOSPITLAL WIDE**

APPROVED BY: **ADMINISTRATION**

APPROVAL DATE:

Introduction

South Peninsula Hospital has adopted this Response Procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department of Health and Human Services ("DHHS") security and privacy regulations, as well as to acknowledge our duty to protect the confidentiality and integrity of confidential medical information as required by law and professional ethics. In addition, this Response Procedure will assist SPH in fulfilling its obligation under SPH must comply with this policy. Familiarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Assumptions

This Response Procedure is based on the following assumptions:

- Breaches of security, confidentiality, or SPH's policies and procedures may occur despite security and confidentiality protections.
- Early detection and response to such breaches is critical to stop any such breach, correct the problem, and mitigate any harm.
- In appropriate cases, a thorough investigation is necessary to assess the breach, mitigate any harm, determine how to prevent recurrence, and provide a basis for any necessary disciplinary action.

Policy

Individuals detecting or suspecting a breach of health information security or confidentiality must report the breach or suspected breach as specified therein, including a written report to the Privacy Officer as soon as possible as specified in SPH's Report Procedure.

The purpose of responding to and investigating health information breaches and suspected breaches is to as follows:

- Minimize the frequency and severity of incidents.
- Provide for early assessment and investigation before crucial evidence is gone.
- Quickly take remedial actions to stop the breaches, correct the problems, and mitigate damages. Implement measures to prevent recurrence of incidents.
- Facilitate effective disciplinary actions against offenders.

SPH will not take any adverse personnel or other action against a person who reports an actual or suspected breach of security, confidentiality, or SPH's policies and procedures protecting the security and confidentiality of health information so long as the report is made in good faith. Making a knowing false report, however, may result in disciplinary action under SPH’s Employee Corrective Action Plan.

Upon receiving the report, the Privacy Officer will take the following steps:

- Take any necessary immediate corrective action.
- If the breach appears to involve gross negligence, willful misconduct, or criminal activity of a person or persons holding access privileges, immediately, in conjunction with the manager of Information Systems, suspend that person(s) access pending investigation, including taking all necessary steps to prevent access (removal of user accounts, recovery of keys, and so forth).
- Provide copies of the report with an endorsement as to any corrective action taken, including suspensions of access, and recommendations for future action to all the following people and departments:
    - Administration.
    - Manager of Information Systems.
    - Risk Management.
    - Quality Assurance.
    - Human Resources.
    - Concerned department directors.

- The facility administrator may appoint an investigating officer, which may be the Security or Privacy Officer, to conduct an investigation in appropriate cases. Factors to be considered in determining whether an investigation is necessary include the following:

    - Seriousness of the breach.
    - Whether the breach resulted in actual harm.
    - Extent of any harm.
    - Whether the breach has the potential for legal liability.
    - Whether the breach involved gross negligence, willful misconduct, or criminal activity.
    - Whether the breach put patient or other individuals' welfare at risk.
    - Whether there has been a series of similar or related breaches.
    - Whether the suspected offender has committed other breaches.

    - The investigating officer will conduct a thorough investigation into all the facts and circumstances of the breach or suspected breach and will provide the facility administrator a detailed report of the facts and circumstances of the breach including recommendations for corrective and/or disciplinary action.

    - All SPH personnel will cooperate with any such investigation. Failure to cooperate, failure to furnish required information, or furnishing false information may result in employee discipline up to and including termination under SPH's Employee Corrective Action Plan. Department managers/supervisors will ensure that the investigating officer has access to necessary persons and information to conduct a through investigation.

    - The Risk Management manager will review the report and its recommendations for legal sufficiency.

    - The facility administrator, the Security Officer, the Privacy Officer, the Investigating Officer, the manager of Risk Management, and other appropriate personnel will discuss the report and recommendations and decide on appropriate action to prevent recurrence of the breach, mitigate any harm caused by the breach, and take necessary disciplinary action in accordance with SPH's Employee Corrective Action Plan.
    - The Privacy Officer will keep all such reports for not less than six years from the date of the report.

    - No such report will be made a part of a patient's medical record. The report is a risk management tool, not a patient care document.

Enforcement

All officers, agents, and employees of SPH **must** adhere to this policy. SPH will not tolerate violations of this policy. Violations of this policy are grounds for disciplinary action up to and including termination of employment and criminal or professional sanctions in accordance with SPH's medical information sanction policy and Employee Corrective Action Plan.

SOUTH PENINSULA HOSPITAL

POLICY# **HW-**

SUBJECT: **REPORT PROCEDURE**

DEPARTMENT: **HOSPITAL WIDE**

APPROVED BY:

APPROVAL DATE:

South Peninsula Hospital (SPH) has adopted this Report Procedure to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health and Human Services ("DHHS") security and privacy regulations as well acknowledge our duty to protect the confidentiality and integrity of confidential medical information as required by law, and professional ethics. All personnel of SPH must comply with this policy. Familarity with the policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

Assumptions

This Report Procedure is based on the following assumptions:

- Breaches of security, confidentiality, or SPH's policies and procedures may occur despite security and confidentiality protections.
- Early detection and response to such breaches is critical to stop any such breach, correct the problem, and mitigate any harm.
- All personnel must know how to report breaches and suspected breaches.

Policy: All employees and others with access to health information **must** report breaches of security/confidentiality or of SPH's policies and procedures protecting the security and confidentiality of health information as specified below.

The purpose of reporting health information breaches and suspected breaches are as follows:

- Minimize the frequency and severity of incidents.
- Provide for early assessment and investigation before crucial evidence is gone.
- Quickly take remedial actions to stop breaches, correct problems, and mitigate damages.
- Implement measures to prevent recurrence of incidents.
- Facilitate effective disciplinary actions against offenders.

SPH will not take any adverse personnel or other action against a person who reports an actual or suspected breach of security, confidentiality, or SPH's policies and procedures protecting the security and confidentiality of health information so long as the report is made in good faith. Making a knowing false report, however, may result in disciplinary action under SPH's Employee Corrective Action Plan. It is the policy of SPH that all personnel should not only feel free to report breaches, without fear of reprisal, but also understand they have a duty to do so.

Employees and others must report the following:

- Breach of security, defined as any event that inappropriately places health information at risk for unavailability, improper alteration, breach of confidentiality, or other potential harm to patients, staff, SPH itself, or others that may result in adverse legal action.

- Breach of confidentiality, defined as the improper disclosure of individually identifiable health information to a person or entity not authorized to receive the information.

- Any violation of SPH's policies and procedures relating to the security or confidentiality of patient information.

- Any violation of SPH's policies and procedures relating to the proper use of computer and other information systems equipment.

PROCEDURE:

The person discovering the breach or suspected breach must institute the reporting procedure as soon as possible after the occurrence of the breach or its discovery. The person discovering the breach must take the following actions:

- Initiate any necessary corrective action. If, for example, a data user detects an unauthorized person observing confidential patient data on a computer screen, he or she should cover the screen, turn off the screen, or otherwise prevent the unauthorized person from continuing to view it.

- Report the matter to Security if necessary, such as in the case of an unauthorized person in the medical records department who refuses to leave immediately.

- Report the incident to his or her immediate supervisor if the supervisor is available.

- Report the incident to the manager of Information Systems/Security Officer at extension 1356 and the manager of Health Information Management/Privacy Officer at extension 1236.

- As soon as possible, make a written report of the following information:
    - Person submitting the report.
    - Date and time of the report.
    - Date and time of the incident.
    - Location of the incident.

- Health information resources involved (hardware, software, data).
- Persons involved (suspects, witnesses).
- Nature of the breach.
- Harm, if any, observed.
- Any statements made by suspects and witnesses.
- Who was notified.
- Remedial action, if any, taken.
- Recommendations for corrective action.

- Such reports are a risk management tool and not a patient care document. No such report may be made a part of a patient's medical record.

- The Privacy Officer must maintain copies of all reports for at least six years from the date of the report.

ENFORCEMENT:

All officers, agents, and employees of SPH **must** adhere to this policy. SPH will not tolerate violations of this policy. Violations of this policy are grounds for disciplinary action up to and including termination of employment and criminal or professional sanctions in accordance with SPH's Employee Corrective Action Plan.

SOUTH PENINSULA HOSPITAL
4300 Bartlett Street
Homer, Alaska 99603

HOW TO FILE A HIPAA PRIVACY COMPLAINT WITH THE HSS OFFICE FOR CIVIL RIGHTS (OCR)

If you wish to file a privacy complaint, the HIPAA privacy regulations require your complaint to:

1. Be in writing, either paper or electronically;
2. Name the person or organization that is the subject of the complaint, and describe the acts or omissions that you believe violate the HIPAA privacy regulations; and
3. Be filed within 180 days of when you knew or should have known that the act or omission you are complaining of occurred (unless you show good cause why the Secretary of HHS should waive the time limit and the Secretary does wave it).

WHERE TO FILE

Send your complaint to either the OCR regional office for the state or territory in which the person or organization you are complaining of is located, or to the OCR headquarters. The address is listed below.

Send inquiries about the HIPAA privacy complaint process to the OCR regional manager. All regional managers in the notice are with the Department of Health and Human Services' Office for Civil Rights.

If you need further information, contact the OCR regional office for the state r territory in which the person or organization you are complaining about is located, or the headquarters office.

OCR HEADQUARTERS

Robinsue Frohboese, Acting Director
Office for Civil Rights
U.S. Dept. of Health and Human Services
200 Independence Avenue SW
Room 509F HHH Building
Washington, D.C. 20201

REGION X: SEATTLE

(Alaska, Idaho, Oregon, Washington)
Linda Yuu Connor, Regional Manager
2201 Sixth Avenue, Suite 900
Seattle, WA 98121-1831
Phone (206) 615-2287
Fax (206) 615-2297
TDD (206) 15-2296

4300 Bartlett Street
Homer, Alaska 99603

REQUEST FOR AN ACCOUNTING OF DISCLOSURES

1. PATIENT INFORMATION

   Date of request: _____ MR# _____

   Patient Name: _____DOB _____

   Address: _____

   _____

   Address to send accounting to: _____

   _____

---

2. DATES REQUESTED
   I am requesting an accounting of all disclosures for the following time frame. Please note: the maximum time frame that can be requested is six years prior to the date of your request, and we are not required to account for disclosures that occurred before April 14, 2003.

   From: _____ To: _____

3. FEES
   There is no charge for the first accounting in a 12 month period. For subsequent requests in the same 12 month period, the charge is $_____. I understand that there is (check one):
   ____ No fee for this request
   ____ A fee for this request in the amount of $_____, and I wish to proceed.

4. RESPOSE TIME
   I understand that the accounting I have requested will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

_____ _____
Signature of patient or legal representative Date

5. ORGANIZATIONAL USE ONLY

Date request was received: _____

Date accounting sent: _____

Extension requested: ___ No ___ Yes

If yes, give reason: _____

Patient notified in writing on this date: _____

Staff member processing request: _____