Title:	**DPH Privacy and Security Manual**
Chapter:	**II. Administrative Policies, Privacy Incident Reporting**
Current Effective Date:	**November 16, 2033**
Original Effective Date:	**November 16, 2003**
Revision History:	**May 12, 2004**

Purpose

The purpose of the Division of Public Health (DPH) privacy incident policy is to address the DPH privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information. This policy is in compliance with the DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, that establishes the NC Department of Health and Human Services (DHHS) privacy incident reporting requirements.

Policy Scope: ***The policy applies across the Division to all DPH workgroups who maintain, use, have access to, or come into contact with IIHI.***

Background

A 'privacy incident' is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of this department. A privacy incident is not to be confused with a 'privacy complaint', which is either an allegation, filed by an individual that IIHI maintained by a division or office in DHHS has been used or disclosed inappropriately; or a complaint filed by an individual concerning DHHS privacy practices, policies, or procedures. Likewise, a privacy incident is not to be confused with an "accident" or other event' that has the potential to cause physical injury to an individual and is reported as an "incident." A privacy incident must pertain to the unauthorized use or disclosure of individually identifying health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

Policy

The Division shall immediately investigate and attempt to resolve all reported suspected privacy incidents wherein the IIHI of a client has not been used or disclosed in accordance with DHHS and Division privacy policies **and** there is potential harm to the client.

Suspected Privacy Incident

DPH staff shall verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a client's IIHI. If the supervisor determines that further review is required, the supervisor and staff member will consult with the DPH Privacy Official or designee to determine whether the suspected incident warrants further investigation.

Documentation

The DPH Privacy Official, or designee within the DPH Privacy Office, shall document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy incident shall be filed in the office of the agency's Privacy Official and in the office of the DHHS Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is not considered part of the client's health record.

Client Contact

If the client is not aware of a privacy incident, the DPH Privacy Official shall investigate the incident thoroughly before determining whether the client should be informed. If the client is aware of a privacy incident, the Privacy Official shall contact the client within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the DPH Privacy Official, but resulting communications with the client must be documented in the Communications Log section of the Privacy Incident Report form, as described in "Implementation" section. In addition, any privacy incident that includes a disclosure for which an accounting is required must be documented and entered into accounting of disclosures logs. Disclosures that must be accounted for apply to covered healthcare components and are described in the DHHS and DPH Privacy policies, Accounting of Disclosures.

Non-Retaliation

The Division shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.

Implementation

Division of Public Health Procedure for Reviewing Privacy Incidents

When a DPH supervisor has received an initial oral report of a suspected privacy incident, the supervisor will review the situation with the staff member who reported the suspected incident. If the supervisor determines that the suspected incident may be a reportable incident or warrants further consultation and review, the supervisor will contact the DPH Privacy Official. The DPH Privacy

Official will review the situation with the staff member and supervisor and determine whether the suspected incident requires further investigation. If further investigation is required or if the situation involves a privacy incident, the DPH Privacy Official, or designee, will prepare Privacy Incident Report form to document the privacy incident and the steps taken to investigate, resolve, and remediate the incident. The Divisions will strive to remediate the report incident within 30 days of it being reported.

Documentation

The Division has developed a Privacy Incident Report form, which is based on the DHHS template. This form is used to document confirmed reports of privacy incidents that have been referred to the DPH Privacy Official from the staff member and supervisor who have reviewed the suspected incident.

The DPH Privacy Official, or designee, assigns the DPH incident report tracking code and number (DPH-PR-xx), classifies the incident and its severity, analyzes the situation, and documents the information on the Privacy Incident Report form. Documentation shall be retained by the DPH Privacy Official for a minimum of six years from the date of the reported incident.

If the Privacy Official/designee is able to resolve the incident, the Privacy Official shall also document the actions taken to resolve the issue in Section III of the Privacy Incident Report form. A copy of the completed report shall be forwarded to the DHHS Privacy Officer for review and permanent filing.

The Privacy Incident Report form can also be accessed on the DPH HIPAA web site at http://www.schs.state.nc.us/hipaa/.

Division of Public Health Privacy Incident Review

The DPH Privacy Incident Review Team is comprised of staff within the DPH Privacy Office. The DPH HIPAA Coordinators are designated to assist the DPH Privacy Official investigate and resolve those incidents that cannot be readily resolved by the Privacy Official. As necessary, members of the DPH management team also may assist in the review and resolution of privacy incidents. In addition, DPH Human Resources and Legal Affairs staff are consulted as part of the DPH review team to assist in the review and investigation of privacy incidents when required.

If the DPH review team is able to resolve the incident, the DPH Privacy Official shall complete Section III of the Privacy Incident Report form and shall forward a copy of the completed report to the DHHS Privacy Officer.

If the DPH review team and the DPH Privacy Official/designee are unable to resolve the violation, the Privacy Official/designee shall send copies of the information generated by the group, including the Privacy Incident Report form, to the DHHS Privacy Officer for resolution.

DHHS Privacy Officer Review

The DHHS Privacy Officer shall review the privacy incident and DPH resolution, if any. If the DPH has not resolved the incident, the DHHS Privacy Officer shall involve anyone determined to be necessary to assist in resolution of the incident, including the Office of the Attorney General. The DHHS Privacy Official shall document the review comments and/or resolution in Section IV of the Privacy Incident Report form, and a copy of such documentation shall be returned to the DPH Privacy Official. The DHHS Privacy Officer shall maintain the incident file.

Communications Log

Section V of the Privacy Incident Report form provides a record of communications relating to the resolution of the privacy incident. The DPH Privacy Official or designee shall be maintained from the beginning of the investigation through the resolution phase, providing the Division and the Department with a comprehensive accounting of the measures taken while seeking resolution.

Training

Whenever a privacy incident has occurred, DPH will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the DPH Privacy Official may determine that the entire Division workforce should receive training that is specific to the privacy incident. The DPH Privacy Official/designee will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the DPH privacy policies and procedures."

Client Notification

The Division will investigate all suspected privacy incidents and shall assess the potential for harm to a client to determine if the client or personal representative should be informed of the privacy incident. If it is determined that there is no reason to inform the client of the privacy incident, the Division Privacy Official or designee will document the reasons for the decision not to inform the client.

If it is determined that the client should be informed of the privacy incident, the DPH Privacy Official/designee will consult with the DHHS Privacy Official to determine who will contact the client to explain the findings and any possible repercussions. The client should be provided with a summary of the findings and any actions taken. The client's response should be documented, including whether the client was satisfied or dissatisfied with the disposition of the privacy incident, in the Communications Log section of the Privacy Incident Report form. If the client was not satisfied with the disposition of the privacy incident, the Department's legal counsel shall be informed of the incident, in the event the client takes legal action.

For relevant documents:

Privacy Incident Report

References: **DHHS Directive Number III-11; DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, DPH HIPAA Compliance Statement, 42 CFR 164.530**

For questions or clarification on any of the information contained in this policy, please contact the DPH Privacy Office at HIPAA.DPH@ncmail.net.