

## DHHS POLICIES AND PROCEDURES

---

<b>Section VIII:</b>	<b>Privacy and Security</b>
<b>Title:</b>	<b>Privacy Manual</b>
<b>Chapter:</b>	<b>Administrative Policies, Privacy Incident Reporting</b>
<b>Current Effective Date:</b>	<b>5/1/05</b>
<b>Revision History:</b>	<b>11/1/03</b>
<b>Original Effective Date:</b>	<b>4/14/03</b>

---

### **Purpose**

The purpose of this policy is to establish 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, as identified by divisions and offices in the NC Department of Health and Human Services (DHHS).

*This policy applies to the following DHHS agencies:*

- *HIPAA covered health care components;*
- *Internal business associates; and*
- *Non-covered health care components that maintain individually identifiable health information.*

### 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 individually identifiable health information 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**

DHHS agencies shall immediately investigate and attempt to resolve all reported suspected privacy incidents wherein the individually identifiable health information of a client has not been used or disclosed in accordance with DHHS privacy policies and there is potential harm to the client.

Each agency shall develop a *Privacy Incident Report* form, based on the [DHHS Privacy Incident Report](#) to be completed when a privacy incident is suspected or has been reported. Initiation of this report shall require an agency investigation and documentation of the privacy incident and attempted resolution that ensures the incident has been remediated. Resolution should be completed within 30 days of the reported incident.

If the client is not aware of a privacy incident, the Agency 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 Agency 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 Agency Privacy Official/designee, but resulting communications with the client must be documented in the Communications Log section of the *Privacy Incident Report* form. 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.

**NOTE:** Non-covered health care components that maintain individually identifiable health information but are not required to designate an Agency Privacy Official must determine how privacy incidents will be handled in their agencies. Such privacy incidents may be managed internally or referred to the DHHS Privacy Officer for investigation.

DHHS agencies 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

### Documentation

DHHS agencies 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 Privacy Official and in the office of the DHHS Privacy Officer and shall be retained for at least six (6) years from the date of the investigation. Such documentation is not considered part of the client's health record.

### Suspected Privacy Incident

Agency staff may verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a client's individually identifiable health information. If the supervisor determines that further investigation is warranted, the staff member shall be instructed to complete Section I – General Information and Section II – Incident Information of the agency's *Privacy Incident Report* form. The supervisor shall review and sign the report and forward the report to the Agency Privacy Official or designee for resolving privacy incidents.

## Agency Privacy Official/Designee Review

The completed *Privacy Incident Report* form shall be reviewed by the Agency Privacy Official or designee, who will assign the tracking code and number, classify the incident and its severity, analyze the situation, and document the information in Section III of the *Privacy Incident Report* form. If the Agency Privacy Official/designee is able to resolve the incident, he/she 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.

## Agency Review

Each agency shall determine their procedures for investigating and resolving privacy incidents; however, the agency must provide a review team to assist the Agency Privacy Official or designee in investigating those privacy incidents that cannot be readily resolved by the Agency Privacy Official/designee. If the agency team is able to resolve the incident, the Agency 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 agency review team and the Agency Privacy Official/designee are unable to resolve the violation, the Agency 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 agency resolution, if any. If the agency 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 review comments and/or resolution shall be documented by the DHHS Privacy Officer in Section IV of the *Privacy Incident Report* form and a copy of such documentation shall be returned to the sending agency's designated staff responsible for privacy incident reporting. The incident file shall be maintained by the DHHS Privacy Officer.

## Communications Log

Section V of the *Privacy Incident Report* form provides a record of communications relating to the resolution of the privacy incident. This log shall be maintained from the beginning of the investigation through the resolution phase, providing the agency and department with a comprehensive accounting of the measures taken while seeking resolution.

## Training

Whenever a privacy incident has occurred, the agency must evaluate the occurrence to determine if additional staff training is in order. Depending upon the situation, it may be determined that the entire agency workforce should receive training that is specific to the privacy incident. The Agency Privacy Official/designee shall 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 DHHS privacy policies and agency procedures.

## Client Notification

Each agency shall 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 agency must 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 Agency Privacy Official/designee should contact the client or personal representative and 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 agency's legal counsel shall be informed of the incident in the event the client takes legal action.

## Reference

DHHS Directive Number III-11; 45 CFR 164.530

## For Relevant Documents

[DHHS Privacy Incident Report](#)

*For questions or clarification on any of the information contained in this policy, please contact [DHHS Privacy Officer](#). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#).*