

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Privacy Incident and Complaint Reporting
Chapter:	Privacy Manual
Current Effective Date:	4/1/12
Revision History:	11/1/03, 4/1/12
Original Effective Date:	4/14/03

Purpose

The purpose of this policy is to establish requirements for reporting, documenting, and investigating incidents and complaints resulting from suspected violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the North Carolina (NC) Identity Theft Protection Act, or the department's privacy practices, policies or procedures regarding confidential information.

This policy applies to the following DHHS agencies:

- Agencies covered by HIPAA;
- Agencies covered by the NC Identity Theft Protection Act; and
- Agencies that generate, use, collect, disclose or store confidential information.

Background

The department requires that its agencies develop procedures for reporting incidents and complaints and for responding to individuals who make inquiries, express concerns, and/or file complaints regarding the agency's privacy practices, policies, and procedures. Such communications may be rendered:

- In person;
- In writing (letter/e-mail/fax); or
- By telephone.

DHHS agencies shall respond to every identifiable privacy incident or complaint received. Each identifiable privacy incident or complaint shall generate an investigation, determination and a response. Ensuing investigations should focus on both the specific privacy incident or complaint and any patterns of similar privacy incidents or complaints.

Documentation of privacy incidents or complaints, investigative efforts, and incident or complaint determinations are considered administrative information and shall be maintained in administrative files for at least six (6) years. Documentation of privacy incident or complaint information **shall not** be filed in a client’s treatment, financial, or other designated record sets.

Definitions

Breach: The acquisition, access, use, or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. (**Note:** *The definition of “breach” applies with regard to the HIPAA Privacy Rule.*)

(1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

Confidential information: Information that is “non-public” or deemed confidential by state or federal law (i.e. state statute, administrative code, federal regulation, etc.), including social security numbers and other identifying information, protected health information, tax records, client program eligibility information, etc.

Health Information Portability and Accountability Act (HIPAA): A federal law that protects individually identifiable health information. Federal standards are now in place that ensure patients have access to their own medical records while adding new responsibilities to those charged with protecting this information.

Identifying Information: includes all of the items listed below (N.C.G.S. § 14-113.20(b)).

1. Social security numbers (SSNs) or employer identification numbers (EINs)
2. Drivers license¹, state identification card, or passport numbers
3. Checking and savings account numbers
4. Credit and debit card numbers
5. Personal Identification Number (PIN) code, as defined in N.C.G.S. § 14-113.8(6)
6. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names¹
7. Digital signatures
8. Any other numbers or information that can be used to access a person’s financial resources
9. Biometric data

10. Fingerprints
11. Passwords
12. Parent's legal surname prior to marriage¹

¹However, with regard to N.C.G.S. § 132-1.10, which applies to governmental agencies, “**identifying information**” does not include the items below:

1. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names.
2. Parent's legal surname prior to marriage, or
3. Drivers license numbers *appearing on law enforcement records*. (See *N.C.G.S. § 132-1.10(b)(5)*).

Non-public information: information that is not considered a “public record” as defined in N.C.G.S. § 132-1.

NC Identity Theft Protection Act: articulates when “businesses” and state or local governments can collect Social Security numbers (SSNs) and other identifying information, what they must do if they possess such information, and what notification responsibilities exist if “personal” or “identifying” information is disclosed without a valid authorization.

Personal Information: A person's first name or first initial and last name in combination with “identifying information,” as defined above in N.C.G.S. § 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made **lawfully** available to the general public from federal, state, or local government records (*See N.C.G.S. § 75-61(10)*).

Privacy complaint: An allegation made by an individual that there has been an unauthorized access to, or the use, disclosure, and/or collection of, confidential information.

Privacy incident: An event or action resulting from the unauthorized access, use, disclosure and/or collection of confidential information. A privacy incident includes “accidental disclosures” such as misdirected e-mails or faxes. A privacy incident can be reported by a DHHS workforce member, a business associate, or a vendor.

Protected health information: Individually identifiable health information, except specifically-listed exceptions, that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium (i.e. paper records, fax documents, and oral communications).

Security breach: An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal

information has occurred or is reasonably likely to occur or that creates a material risk of harm to an individual.

Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the department for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure (**Note:** *The definition of “security breach” only applies with regard to the North Carolina Identity Theft Protection Act; See N.C.G.S. § 75-61(14).*)

[Security] incident: A violation of DHHS computer security policies, acceptable use policies, or standard computer security practices. An adverse event where a NC information technology resource is accessed or used without authorization, attacked or threatened with attack, or used in a manner inconsistent with established policy with the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information (See NC DHHS Policies and Procedures Manual, Section VIII - Privacy & Security - Security Manual – Glossary).

Unsecured protected health information: Protected health information that is not secured through the use of a technology or methodology specified by the Secretary that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals.

Policy

DHHS agencies shall immediately report, investigate, and document all suspected privacy incidents or complaints electronically, ensuring that all required documents are attached to the electronic report. Although the incident or complaint reporting process to the DHHS Privacy and Security Office (PSO) is now electronic, agencies may accept incidents or complaints from DHHS workforce members and individuals using the revised [DHHS Privacy Incident Report](#) or [DHHS Privacy Complaint Report](#) form to document the incident or complaint and retain these documents for the agencies’ future reference. It is not necessary to attach these documents to the electronic report, however.

DHHS agencies shall develop procedures to respond to incidents or complaints whenever there is reason to believe that an agency’s privacy practices, policies or procedures have been breached in some manner. Privacy incidents or complaints shall be resolved in a timely manner, ensuring clients and other individuals that the department is committed to protecting their confidential information.

Each agency shall designate a staff member who is responsible for communicating and assisting workforce members or individuals who have questions or concerns, or who wish to file incidents or complaints regarding the agency’s privacy practices. When reporting

incidents or complaints electronically, the agency shall report its internal incident or complaint number, incident classification and severity, investigative analysis of the facts, description of the corrective actions taken, and mitigation efforts undertaken. The report shall be updated using the ticket tracking ID number, which is generated after submitting the incident or complaint until the investigation is completed and closed. In addition, any privacy incident or complaint that includes a disclosure for which an accounting is required must be documented and entered into the accounting of disclosures logs.

Implementation

Often it is difficult for an agency to determine when to report an event as either an incident or a complaint. The key difference between an incident and a complaint is who reports the event. An incident is reported when a DHHS workforce member, business associate or vendor reports a privacy violation. On the other hand, any individual within the general public (i.e., a client) typically files a privacy complaint.

If an individual chooses not to pursue filing a complaint with the department, or the agency is unable to complete the complaint process after obtaining some general information, the agency shall report and investigate the matter as an **incident**. This ensures that the event is investigated and mitigated.

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 or a complaint.

I. Reporting Incidents and Complaints

A. Communication Methods

Incidents: A DHHS workforce member, business associate or vendor shall report incidents to the agency's Privacy Official or Privacy Coordinator. The Privacy Official or Privacy Coordinator shall then report the incident to the DHHS PSO electronically.

Complaints: An individual can file a complaint with the agency directly, or with the department's Privacy Officer. The DHHS Privacy and Security Office is responsible for maintaining a current list of designated privacy contacts in each agency and; therefore, each agency is required to notify the DHHS Privacy and Security Office of any staff changes in their privacy official or privacy coordinator positions.

AGENCY: An individual may file a privacy complaint in person, in writing or by telephone directly with an agency. The Privacy Official or Privacy Coordinator shall immediately notify the complainant in writing that the agency has received his/her complaint, is investigating it and will notify the complainant of its resolution. DHHS

agencies shall not retaliate against any individual for filing a HIPAA privacy complaint with either the agency, the department, or the Secretary of the US Department of Health and Human Services

DEPARTMENT’S PRIVACY OFFICER: An individual may file a complaint with the DHHS Privacy and Security Office if, for some reason, the individual does not wish to speak to the agency Privacy Official or Privacy Coordinator. Such communication may be accomplished in person, in writing, or by telephone. If an individual contacts the DHHS Privacy and Security Office first, the DHHS Privacy and Security Office shall determine if the issue is agency-specific and shall attempt to refer the individual to the appropriate agency, as needed. If the individual does not wish to speak with agency staff directly, the DHHS Privacy and Security Office shall collect the complaint information and work with the agency Privacy Official or Privacy Coordinator to resolve the issue.

II. Documenting, Investigating, and Resolving Incidents and Complaints:

A. Documentation

The **DHHS Privacy Complaint** form shall be used to document an individual’s complaint. Complaints do not require a signature; however, agencies shall make a good faith effort to have the DHHS Privacy Complaint form signed by the complainant and should use the same procedures for obtaining signatures for privacy complaints as they use to obtain signatures for authorizations and consents. Generally, it is not the department’s practice to accept anonymous complaints. However, DHHS agencies can investigate the complaint as an incident if the complainant does not wish to be identified.

If a complainant appears in person to file a privacy complaint against a DHHS agency, the complainant should complete and sign the DHHS Privacy Complaint form. If the agency receives a complaint by US mail, e-mail, or facsimile from the complainant, the written complaint shall constitute his/her signature.

The DHHS agency shall document all telephone complaints and send complainant a **DHHS Privacy Complaint** form to complete and sign. If the complainant fails to return the signed complaint within the requested time, the event shall be investigated as an incident.

B. Investigation and Resolution

Investigation of privacy incidents or complaints must begin immediately following receipt of an expressed incident or complaint. Investigative actions and resolution shall be documented electronically using the link <http://www.ncdhhs.gov/psso/incidents.htm>. It is important to write down and maintain the ticket tracking ID number, which is generated automatically after the DHHS agency submits its incident or complaint. The DHHS agency will need the ticket tracking ID number to update its report. The DHHS agency should avoid

identifying clients by name or using complete names of employees in their reports. However, it is important to provide detailed information, including dates, locations, titles, types of identifiers involved and attach documents, since this will be the DHHS agency's main record of the investigation. The DHHS Privacy and Security Office will have access to this report online, so it will no longer be necessary to mail in documents and attachments.

Incident or complaint resolution shall be completed no later than thirty (30) days after receipt of the incident or complaint by the Privacy Official or Privacy Coordinator, unless there is a justifiable reason for the delay. If the delay is justified, the agency director may grant a sixty (60) day extension.

The Privacy Official or Privacy Coordinator shall notify the complainant of his or her findings in writing unless the complainant failed to provide his/her contact information.

C. Responsibility of Privacy Official or Privacy Coordinator

Each agency shall determine its procedures for investigating and resolving privacy incidents or complaints. However, each agency must designate an individual as *Privacy Official* (if covered by HIPAA) and/or as *Privacy Coordinator* (if not covered by HIPAA), who will be responsible for reporting, investigating and documenting privacy incidents or complaints.

If an individual contacts the agency directly, the agency's Privacy Official or Privacy Coordinator shall determine if the issue can be resolved at the agency level. If so, the Privacy Official or Privacy Coordinator shall be responsible for investigating and documenting the concern until the issue is resolved. Agencies operated by the Division of State Operated Healthcare Facilities are encouraged to involve their internal client advocates in the complaint investigation process when deemed appropriate.

If the Privacy Official or Privacy Coordinator determines the issue involves other agencies in the department or if he/she is unable to obtain resolution at the agency level, the issue shall be forwarded to the DHHS Privacy and Security Office.

D. DHHS Privacy and Security Office Review

The DHHS Privacy and Security Office shall review the reporting, documentation and resolution of all privacy incidents or complaints. If the agency has not resolved the incident within a reasonable time, the DHHS Privacy and Security Office shall involve anyone determined to be necessary to assist in resolution of the incident or complaint, including the Attorney General's Office. If the DHHS Privacy and Security Office has comments, suggestions, questions, etc. about the investigation and resolution of the incident or complaint, he or she shall document this information within the report for consideration by the agency.

E. *Training*

Whenever a privacy incident or complaint has occurred, the DHHS agency must evaluate the occurrence to determine if additional staff training is necessary. Depending upon the situation, it may be determined that the entire agency should receive training that is specific to the privacy incident or complaint. The Privacy Official or Privacy Coordinator shall review any privacy training developed as part of the privacy incident or complaint resolution to ensure the scope of the training adequately addresses the subject of the incident and reinforces the DHHS and agency privacy practices, policies and procedures.

NOTE: The DHHS agency is responsible for providing its employees privacy and security training at first hire and then annual training thereafter.

III. **Types of Incidents and Complaints**

Currently, there are three types of privacy incidents or complaints: HIPAA, NC identity theft, and departmental practice, policy or procedure violations. There may be times when these three types of privacy incidents or complaints overlap, and agencies are unsure about whether any given event could be considered a breach of unsecured PHI, a security breach, a departmental practice, policy or procedure violation, or a combination thereof. In these instances, please contact the DHHS Privacy and Security Office for guidance.

A. *HIPAA incidents and complaints (breach of unsecured PHI):*

The **HIPAA Breach Notification for Unsecured PHI policy** outlines the procedures HIPAA covered DHHS agencies should follow when they evaluate and report an unauthorized acquisition, access, use, or disclosure of protected health information (PHI). These procedures include information about to whom an impermissible acquisition, access, use, or disclosure of PHI should be immediately reported, who should be involved in determining if a breach of unsecured PHI has occurred and if the affected individual(s) should be notified.

HIPAA covered agencies which become aware of an unauthorized acquisition, access, use, or disclosure of PHI shall **immediately** notify the DHHS Privacy and Security Office (PSO) by reporting the incident or complaint to the following link:

<http://www.ncdhhs.gov/psso/incidents.htm>

and complete the applicable sections (*See HIPAA Breach Notification for Unsecured PHI policy* for further guidance at <http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/>).

B. *NC Identity Theft Protection Act incidents and complaints (security breach):*

The **Identity Theft and Security Breach Notification policy** outlines the procedures all DHHS agencies should follow when they report a disclosure or possible disclosure of identifying information. These procedures will include information to whom a disclosure or possible disclosure of identifying information should be immediately reported; who should be involved in determining if a security breach has occurred and if the affected persons should be notified.

Any DHHS agency which becomes aware of a disclosure or possible disclosure of identifying information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to the following link:

<http://www.ncdhhs.gov/ps0/incidents.htm>

and complete the applicable sections (*See the DHHS Identity Theft and Security Breach Notification policy* at <http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/> for further guidance).

C. *Departmental policy or procedure violation incidents or complaints*

There are DHHS agencies that maintain confidential information, but may not be covered by HIPAA. The Privacy Safeguards policy specifically addresses how divisions and offices should protect confidential information from unauthorized use or disclosure.

Any DHHS agency which becomes aware of an unauthorized use or disclosure of confidential information shall **immediately** notify the DHHS PSO by reporting the incident or complaint to the following link:

<http://www.ncdhhs.gov/ps0/incidents.htm>

and complete the applicable sections.

D. *Overlapping incidents and complaints*

There may be instances when overlapping issues arise and agencies are unsure about whether any given event could be considered a HIPAA privacy incident, a security breach, or a combination thereof. There could also be situations where privacy and security incidents overlap.

When evaluating incidents or complaints, the Privacy Official or Privacy Coordinator should look for key words such as “health information”, “SSN”, or “laptop”, and consider how these words might suggest which type of incident or complaint to report.

If:

health information
laptop or other DHHS-owned technology resource
SSN or other financial identifiers

Consider:

→ HIPAA
→ security incident reportable to DHHS PSO and ITS
→ NC Identity Theft Protection Act

EXAMPLE: There can be differences and similarities between a [security] incident reportable to ITS, a security breach and a breach of unsecured PHI. If a DHHS-issued laptop is stolen from a hotel, this event should be reported as a [security] incident to the DHHS PSO, since an information technology resource has been accessed or used without authorization. Whether this event is also a breach of unsecured PHI will depend upon whether the stolen laptop contained PHI (i.e. a type of health information together with an identifier). The “Privacy Risk Assessment” form should be completed to determine whether notification of the affected client(s) is required. Whether the DHHS agency will have to notify affected persons will depend upon whether the laptop was encrypted or another exception to the notification rule exists. If PHI was present, the unauthorized access posed a significant risk of financial, reputational, or other harm to the individual, and no exception exists, the agency will have to notify. In addition, if the event involves “personal information” and the laptop was not encrypted, this event could also be a security breach.

References

- DHHS Directive Number III-11
- Identity Theft and Security Breach Notification policy
- HIPAA Breach Notification for Unsecured PHI policy
- N.C.G.S. § 75-65; § 132-1.10
- HIPAA, 45 CFR § 164.530
- Privacy Risk Assessment forms, HIPAA-covered and Non-covered divisions/offices
- DHHS Privacy Incident Report form
- DHHS Privacy Complaint form

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