

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Identity Theft and Security Breach Notification
Current Effective Date:	4/1/12
Revision History:	4/1/12
Original Effective Date:	6/25/08

Purpose

In an effort to reduce the risk of exposing its citizens to the possibility of identity theft and to an information security breach, the North Carolina (NC) General Assembly enacted the NC Identity Theft Protection Act which became effective on December 1, 2005.

The NC Identity Theft Protection Act is comprised of two (2) statutes, which articulate 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 valid authorization.

The purpose of the Identity Theft and Security Breach Notification Policy is two-fold:

- Protect SSNs and other identifying information that DHHS receives, collects, uses, stores, discloses and mails in compliance with North Carolina General Statute (N.C.G.S.) § 132-1.10; and
- Outline procedures and protocols for responding to a security breach involving the unauthorized disclosure of unencrypted personal information, in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

This policy is guided by the following objectives:

- To increase DHHS workforce members’ awareness about the confidential nature of SSNs and other identifying information;
- To reduce the reliance upon SSNs for identification purposes;
- To increase emphasis on the secure use, collection, transmission and storage of SSNs and other identifying information;
- To provide a consistent Department of Health and Human Services (DHHS) policy regarding the collection, usage, storage, transmission, mailing and disclosure of SSNs and other identifying information;
- To increase the confidence of clients and workforce members that SSNs and other identifying information are maintained in a confidential manner; and

- To institute consistent procedures for determining when a security breach has occurred and whether notice is required.

DHHS is dedicated to ensuring that its agencies protect SSNs and other identifying information of its clients and workforce members. **All** DHHS agencies, therefore, must comply with the Identity Theft and Security Breach Notification policy and immediately report any breach of security or compromise of systems containing this type of data to its designated personnel.

Policy

DHHS agencies should request an individual’s identifying information only when required to do so by federal or state law, or at the very minimum, only as necessary to conduct their legitimate business operations. Where the purpose of the identifying information can be satisfied by another personal unique identifier, reduced to the last four digits of the SSN or removed entirely, all DHHS agencies are expected to do so.

Definitions

Business: A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency (See N.C.G.S. § 75-61).

Collect: To request SSNs and other identifying information from a DHHS client or workforce member utilizing a paper document or a DHHS system application.

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 SSNs and other identifying information, PHI, tax records, client program eligibility information, etc.

Device: Computers and any other equipment or devices that store or display data such as PDAs, smartphones (Treos, Blackberry, Palm devices), copiers, printers, disk drives, diskettes, CDs, or USB (thumb) drives.

Disclose: To communicate or make available SSNs, other identifying information, or documents containing SSNs or other identifying information to third parties using verbal, written, or electronic means.

Encryption: The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key (*See N.C.G.S. § 75-61(8)*).

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

- SSNs or employer identification numbers (EINs)
- Drivers license, state identification card, or passport numbers
- Checking and savings account numbers
- Credit and debit card numbers
- Personal Identification Number (PIN) code, as defined in N.C.G.S. § 14-113.8(6)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage

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

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

Individual: A DHHS state employee, contractor, or volunteer or a client receiving services provided by DHHS.

Non-DHHS Organization: A government or governmental subdivision or agency, federal or state, and any “business” as defined above.

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, or collection of confidential information.

Redaction: The rendering of data so that it is unreadable or is truncated so that no more than the **last four (4) digits** of the identification number is accessible as part of the data (*See N.C.G.S. § 75-61(13)*).

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 (*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 Policy*).

Store: To maintain SSNs and other identifying information in a system application or keep documents containing SSNs and other identifying information in a locked file cabinet for future access and use.

Use: To utilize SSNs and other identifying information for some DHHS business purpose.

Implementation

DHHS agencies that maintain SSNs and other identifying information in paper form or electronic media shall adhere to the following procedures with regard to its collection, usage, storage, transmission, mailing and disclosure, in compliance with N.C.G.S. § 132-1.10. They shall also immediately report any breach of security or compromise of

systems containing personal information to designated personnel in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

A. Collection, Usage, Storage, Transmission, Mailing, Disclosure and Destruction:

1. Collection:

DHHS agencies shall not collect SSNs unless and until:

- The collection is authorized by law or imperative for the performance of the agency's duties and responsibilities as prescribed by law;
- The collection is relevant to the purpose for which it is collected;
- The need for the collection has been clearly documented;
- The SSNs have been segregated on a separate page so they are easy to redact when there is a valid public records request; and
- A statement of the purpose(s) for which the SSN is being collected and used is provided to the individual, upon their request, at the time of **or** prior to the agency's actual collection of the SSN.

2. Usage:

DHHS agencies shall not use SSNs for any purpose other than the purpose stated in this policy. Usage shall be for a legitimate business purpose, and a duty exists to safeguard this data and prevent unnecessary access thereto.

3. Storage:

- DHHS agencies shall first evaluate and determine whether there is a legitimate business need to store SSNs before this data can be stored in DHHS system applications, locked file cabinets, or other storage containers.
- DHHS agencies should reduce the SSN to the last four (4) digits, whenever possible, or replace it with a random identification number. When storage of the entire SSN is necessary, DHHS agencies should implement appropriate safeguards to prevent the possibility of workforce member misuse.

4. Transmission:

All DHHS agencies shall not:

- Require an individual to transmit a SSN over the Internet unless the connection is secure **or** the SSN has been encrypted; or
- Require an individual to use a SSN to access an Internet Web site unless a password, unique identification number or other authentication device is also

required.

5. Mailing:

All DHHS agencies shall not:

- Intentionally print or imbed a SSN on any card required to access government services (i.e. Medicaid, food stamps, etc.);
- Print a SSN on any mailed materials, unless state or federal law requires it;
- If required, print a SSN (in whole or in part) on a postcard or other mailer not requiring an envelope;
- Make a SSN visible on an envelope; or
- Make a SSN visible without the envelope having been opened.

6. Disclosure:

All DHHS agencies may disclose SSNs, other identifying information or documents containing SSNs or other identifying information only in the following instances:

- Disclose to another governmental entity or its agents, employees, or contractors if disclosure is necessary for the receiving entity to perform its duties and responsibilities.

NOTE: The receiving governmental entity and its agents, employees, and contractors shall maintain the confidentiality of this information.

- Disclose pursuant to a court order, warrant, or subpoena;
- Disclose for public health purposes, pursuant to and in compliance with Chapter 130A;
- Disclose documents where SSNs or other identifying information have been redacted;
- Disclose SSNs or other identifying information on *certified* vital records issued by the NC State Registrar or authorized officials, pursuant to N.C.G.S. § 130A-93(c);
- Disclose any identifying information, other than SSNs, on *uncertified* vital records; or
- Disclose SSNs or other identifying information in a recorded document in the official records of the NC Register of Deeds office or in the Courts.

7. Destruction:

All DHHS agencies must take reasonable measures to protect SSNs, and personal information against unauthorized access to or use of the information in connection with or after its disposal.

The reasonable measures may include:

- The burning, pulverizing or shredding of papers containing SSNs or personal information so this information cannot be practicably read or reconstructed; or
- The destruction or erasure of electronic media and other non-paper media containing SSNs or personal information so the information cannot practicably be read or reconstructed.

DHHS agencies may, after due diligence, enter into a written contract with, and monitor compliance by, a third party engaged in the business of record destruction to destroy SSNs or personal information. Due diligence should ordinarily include one or more of the following:

- Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review; or
- Taking other appropriate measures to determine the competency and integrity of the disposal business.

NOTE: It is the department's preference that the record destruction company shred documents containing SSNs and other confidential information onsite at the DHHS agency's location.

B. Security Breach:

N.C.G.S. § 132-1.10(c1) states that “if an agency of the state or its political subdivisions, or any agency or employee of a government agency, experiences a security breach, as defined in Article 2A of Chapter 75 of the G.S., the agency shall comply with the requirements of N.C.G.S. § 75-65.”

The NC General Assembly enacted N.C.G.S. § 75-65 to require “businesses” and state or local governments to give individuals early warning when their personal information has been accessed by an unauthorized person, so they can take steps to protect themselves against identity theft or to mitigate the crime’s impact.

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 on 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.

1. Reporting disclosures or possible disclosures involving identifying information:

Any DHHS agency which becomes aware of a disclosure or possible disclosure of identifying information shall **immediately** report the privacy incident or complaint to the DHHS Privacy and Security Office (PSO) and provide answers to the following questions, if known:

- What types of identifying information were involved (i.e. SSN, driver’s license, etc.);
- Was health or financial information involved;
- Was the individual's first name **or** first initial **and** last name included;
- Was the identifying information in electronic or paper form;
- Was the information or the laptop encrypted (128-bit encryption);
- Was the identifying information stolen, lost, misplaced or other; and
- Was the information disclosed to the public?

NOTE: Reporting to the DHHS PSO shall not be delayed for investigative reasons. If definite answers to all of the questions above are not available at the time the disclosure or possible disclosure is immediately reported to the DHHS PSO, the DHHS agency shall provide the remaining answers no later than three (3) business days after the event has been reported to the DHHS PSO.

2. Privacy Official or Privacy Coordinator:

When a disclosure or possible disclosure of identifying information is suspected to have occurred, the Privacy Official or Privacy Coordinator will be charged with reporting to the DHHS PSO and coordinating the division or office’s investigation. All DHHS agencies are encouraged to implement their own internal reporting and investigative procedures to ensure all essential personnel are included in the process and events are reported timely.

3. Evaluation and Response to reported disclosure:

Once reported, the DHHS PSO, in conjunction with the DHHS agency’s Privacy Official or Privacy Coordinator and other necessary staff, will make an initial evaluation to determine the following:

- If the matter should be reported to the NC Office of Technology Services (ITS) as a [security] incident;
- If the disclosure or potential disclosure involved confidential information;
- If the disclosure or potential disclosure involved protected health information or electronic protected health information; and
- If the disclosure or potential disclosure involved unencrypted and unredacted records or data containing “personal information.”

4. Reporting security incidents to the Office of ITS:

All security incidents must be reported to the Office of ITS and must include the information required on the incident reporting form. DHHS must ensure that all security incidents occurring within the department are reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, within 24 hours of incident confirmation (*See Statewide Information Security Manual, Chapter 13 - Detecting and Responding to ITS Incidents Standard, Section 01:130101 - Reporting Information Security Incidents*).

In order to comply with ITS' Detecting and Responding to ITS Incidents Standard, ""requires that [security] incidents classified as severity level 3, 4, or 5 be reported to the DHHS PSO and the DHHS agency's Information Security Official (ISO) within a period of 24 hours from the time the incident was discovered (*See NC DHHS Policies and Procedures Manual, Section VIII – Privacy and Security, Security Manual, DHHS Information Incident Management policy*). The DHHS agency is required to report the incident to the DHHS PSO at the following site:

<https://security.dhhs.state.nc.us/incidents/security/index.php>

NOTE: *There can be a difference between a security incident reportable to ITS and a security breach reportable to those affected persons. For example, 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 security breach will depend upon whether the stolen laptop contained personal information (i.e. a type of identifying information together with a person's first name or first initial and last name) and whether the laptop was encrypted. If personal information was present and the laptop not encrypted, this event could be both a [security] incident and a security breach.*

If you are unsure how to report the event, please contact the DHHS PSO for assistance.

5. Reporting Disclosures or Potential Disclosures Involving PHI:

If a DHHS division or office is covered by HIPAA and determines that it has disclosed protected health information (PHI) or electronic protected health information (ePHI) without authorization, a HIPAA privacy incident should be reported, investigated and mitigated as required by the Privacy Incident and Complaint Reporting policy (*See the HIPAA Breach Notification for Unsecured PHI policy*).

6. Reporting Disclosures or Potential Disclosures Involving Unencrypted and Unredacted Records or Data containing Personal Information:

If, after making an initial evaluation, the DHHS PSO determines that there has been a disclosure or potential disclosure of unencrypted and unredacted records or data containing personal information, the DHHS PSO shall refer the event to the Office of General Counsel to determine whether a security breach has occurred. If the DHHS General Counsel, with assistance from the DHHS PSO and DHHS agency staff, determines that a security breach has occurred, a decision regarding notification of affected persons will be made by the DHHS General Counsel without unreasonable delay.

If it is determined that the security breach may require a press release, the DHHS PSO or the DHHS General Counsel shall notify the Deputy Secretary, the Director of the Office of Public Affairs (PAO), and the DHHS agency Director.

NOTE: There may be instances when overlapping issues arise and DHHS agencies are unsure about whether any given event could be considered a security incident, a HIPAA Privacy incident, a security breach or a combination thereof. In these instances, please contact the DHHS PSO for assistance.

C. Reporting of Incident by a Non-DHHS Organization:

N.C.G.S. § 75-65(b) requires that a non-DHHS organization that maintains or possesses records that DHHS owns or licenses notify DHHS of any security breach immediately following discovery of the breach. DHHS agencies enter into contracts with other non-DHHS organizations to perform specific tasks, involving the non-DHHS organization's use of DHHS identifying information. If, in the performance of this contract, DHHS identifying information is lost, misused, disclosed without authorization, etc., the non-DHHS organization is required to do the following:

1. Notify the DHHS agency:

The non-DHHS organization shall notify the DHHS agency immediately, but no later than twenty-four (24) hours after discovery of an incident involving the DHHS agency's identifying information. The DHHS agency is required to notify affected persons without unreasonable delay. Therefore, it is imperative that the non-DHHS organization conducts an investigation immediately and provides the DHHS agency with answers to the following questions:

- What types of identifying information were involved (i.e. SSN, driver's license, etc.);
- Was health or financial information involved;
- Was the individual's first name **or** first initial **and** last name included;

- Was the identifying information in electronic or paper form;
- Was the information or the laptop encrypted (128-bit encryption);
- Was the identifying information stolen, lost, misplaced or other; and
- Was the information disclosed to the public?

There may be times when answers to the questions above are not yet available. In these instances, the non-DHHS organization shall report the incident to the DHHS agency and update the DHHS agency immediately as information becomes available. Reporting the incident to the DHHS agency shall not be delayed by the non-DHHS organization for investigative reasons or contacting law enforcement.

2. Complete Risk Assessment:

After notifying the DHHS agency about the incident, DHHS agencies should require that the non-DHHS organization complete a risk assessment immediately, but no later than five (5) business days, to determine whether there has been a “security breach.” If definite answers to all of the questions above are not available at the time the incident is reported, the non-DHHS organization shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from the breach is on the DHHS agency - not the non-DHHS organization. Therefore, a non-DHHS organization **should not** have the discretion to determine whether notification will occur.

3. Contract language:

DHHS agencies shall include appropriate language in all contracts with non-DHHS organizations to reflect their responsibilities to do the following:

- notify the DHHS agencies of incidents immediately, but no later than 24 hours;
- investigate the incident;
- complete a risk assessment;
- update the DHHS agency as more information becomes available; and
- pay all costs of notification or provide the notification, at the discretion of the DHHS agency.

4. Notification:

When an incident is reported by a non-DHHS organization, DHHS agencies, in consultation with the DHHS PSO and DHHS General Counsel, shall review information provided by the organization to determine whether notification is required. If there is disagreement between the DHHS agency and the non-DHHS organization, the DHHS agency’s decision shall control when DHHS owns the identifying information and is responsible for providing the notification as the owner of the information.

D. Duty to Notify the Attorney General's Office:

Although N.C.G.S. § 75-65 applies to a "business" and the definition of "business" excludes any government or governmental subdivision or agency, N.C.G.S. § 132-1.10(c1) specifically states that if an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, the agency shall comply with the requirements of N.C.G.S. § 75-65. Accordingly, DHHS agencies are obligated to notify the Consumer Protection Division of the Attorney General's Office pursuant to N.C.G.S. § 75-65(e1), without unreasonable delay, when there is a security breach and notice to affected persons is required. DHHS agencies shall complete the "North Carolina Security Breach Reporting Form" on the NC Attorney General's Office's website at <http://www.ncdoj.gov/getdoc/81eda50e-8feb-4764-adca-b5c47f211612/Report-a-Security-Breach.aspx> and ensure that they include the following information in the form:

- nature of the breach,
- the number of consumers affected by the breach,
- steps taken to investigate the breach,
- steps taken to prevent a similar breach in the future, and
- information regarding the timing, distribution, and content of the notice.

The DHHS General Counsel will notify or delegate the responsibility to notify the Consumer Protection Division of the NC Attorney General's Office.

E. Duty to Report to both the Attorney General's Office and Consumer Reporting Agencies:

N.C.G.S. § 75-65(f) requires that in the event DHHS provides notice of a security breach to more than 1,000 persons at one time, it shall notify, without unreasonable delay, the Consumer Protection Division of the NC Attorney General's Office **and** all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

If more than 1,000 affected persons at one time must be notified, DHHS agencies shall follow the procedure outlined in Section D above and report the security breach to the three credit reporting agencies, Equifax, TransUnion, and Experian.

Equifax Fraud Division

P.O. Box 740250

Atlanta, GA 30374

(800) 525-6285

Website: www.equifax.com

Experian Fraud Division

P.O. Box 1017
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion Fraud Division

P.O. Box 6790
Fullerton, CA 92634
800-680-7289
www.transunion.com

F. Duty to Report to the General Assembly:

N.C.G.S. § 120-270 requires all agencies of the state to evaluate and report to the General Assembly about the agency's efforts to reduce the dissemination of identifying information, as defined in N.C.G.S. § 14-113.20(b) by December 31st of each year. The evaluation should include a review of the agency's public forms, the use of its random personal identification numbers, the restriction of access to its personal identifying information, and the reduction of use of its personal identifying information when it is not necessary. Special attention should be given to the agency's use, collection, and dissemination of SSNs.

In order to ensure compliance with this statute, the DHHS PSO shall coordinate the evaluation and reporting of the department's efforts to reduce the dissemination of SSNs and other identifying information.

G. Communications with the Media or Outside Agencies:

With the exception of the DHHS PSO, the Office of the General Counsel, and the NC Office of Public Affairs, DHHS workforce members **are not** authorized to speak on behalf of the department to media personnel or representatives of other outside agencies concerning privacy or security incidents that have or have not been reported. For more information, please consult the following web site address:

http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-30/man/Media_Policy1.htm.

If you need additional help in understanding the document indicated above, please contact the NC Office of Public Affairs at (919) 855-4840.

Enforcement

The department expects that all workforce members will comply with all laws, standards, policies, procedures, guidelines and expectations regarding the security of confidential information. Violation of this policy may subject a workforce member to disciplinary action up to and including dismissal, as well as any potential civil or criminal sanctions under the law.

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](#)