

DHHS POLICIES AND PROCEDURES

Section VIII:	Privacy and Security
Title:	Privacy Manual
Chapter:	Administrative Policies, Privacy Safeguards
Current Effective Date:	10/24/03
Revision History:	10/24/03
Original Effective Date:	4/14/03

Purpose

The purpose of this policy is to establish privacy safeguards that protect individually identifiable health information from unauthorized use or disclosure and to further protect such information from tampering, loss, alteration, or damage. It is not the intent of this policy to address all of the safeguards necessary to protect electronic data containing individually identifiable health information since those safeguards are included in the Department of Health and Human Services (DHHS) Security Policies.

The policy is applicable to the following DHHS agencies:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered health care components;
- Internal business associates; and
- Non-covered health care components that maintain individually identifiable health information.

Background

The HIPAA Privacy Rule requires covered health care components to implement *appropriate* administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of individually identifiable health information. Agencies are not asked to “guarantee” the safety of individually identifying health information against all imaginable assaults; instead, agencies are instructed to use protections that are flexible, scalable, and provide reasonable safeguards. The safeguards implemented in different DHHS agencies will vary depending on factors such as agency size and the nature of its business. To implement reasonable safeguards, each agency should analyze its own needs and circumstances such as the nature of the information it holds, and assess potential risks to a client’s privacy. DHHS agencies should also consider the potential impacts on client care and other issues such as the financial and administrative burdens of implementing various safeguards.

Safeguards addressed in DHHS Privacy Policies include the administrative, physical, and technical protections necessary for safeguarding individually identifying health information as it is found in the working environment (e.g., oral communications, paper records, medical supplies/equipment, computer screens, etc.).

NOTE: The DHHS Security Policies address the administrative, physical, and technical mechanisms necessary for safeguarding electronic data containing individually identifying health information (e.g., software applications and systems).

Policy

DHHS agencies that maintain individually identifiable health information shall put into place appropriate administrative, physical, and technical safeguards to protect the privacy of such information. Agencies shall take steps to reasonably safeguard individually identifiable health information from intentional or unintentional use or disclosure that is in violation of departmental privacy policies.

DHHS has determined that the requirement to safeguard confidential health information should be extended to all agencies within the department that maintain individually identifiable health information.

Administrative Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each agency. Confidential information that is transmitted by facsimile (fax) machines, e-mail, printers, copiers, and by telephone or other oral means of communication shall be protected from unauthorized use and disclosure. DHHS agencies shall:

- Address measures to direct the conduct of agency staff in relation to the protection of individually identifiable health information; and
- Develop and implement agency safeguard procedures.

Physical Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each agency by establishing protections used for equipment/supplies/records/work areas to prevent unauthorized use or disclosure of individually identifiable health information maintained by the agency.

Technical Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each agency by addressing technical safeguards used for accessing confidential information maintained in computer systems and other electronic media through identification of staff who need access to electronic data and control of access through the use of unique user identifiers and passwords.

Implementation

DHHS agencies shall assess the nature of the individually identifiable health information that it receives, sends, uses, and/or maintains throughout the agency, and shall implement reasonable administrative, physical, and technical safeguards that will ensure such information is protected and is not subject to unauthorized use or disclosure.

Administrative Safeguards

- A. Authorized Disclosures of Individually Identifiable Health Information
- Disclosure of individually identifiable health information is essential to health care providers and health plans for a variety of reasons including treatment, payment of health care services, or health care operations (TPO) purposes. Safeguarding such information requires agencies to ensure the following prior to disclosure:
- The disclosure is permitted for TPO;
 - The disclosure is authorized by the client;
 - The disclosure does not violate a communications or use and disclosure restriction that the client has requested and the agency has granted; or
 - The disclosure is required or permitted by law.

(See the DHHS Privacy Policies [Use and Disclosure Policies, Authorizations; Use and Disclosure Policies, Use and Disclosure](#); and [Client Rights Policies, Rights of Clients](#) for more information).

- B. Safeguarding Methods for Disclosure of Individually Identifiable Health Information

DHHS agencies shall develop and implement procedures that ensure methods of disclosing individually identifiable health information outside the agency are safeguarded to protect client confidentiality.

Mail or Hand Delivery

Whenever feasible, documents containing individually identifiable health information should be hand delivered or mailed using the United States Postal Service (USPS), courier, or other delivery service. All documents containing individually identifiable health information shall be placed in a secure container (e.g., sealed envelope, lock box) that is labeled “Confidential”, is addressed to the recipient, and includes a return name and address. When transmitting individually identifiable health information via interoffice mail, the information shall be placed in a sealed envelope and then placed inside the interoffice envelope.

Fax

DHHS agencies must make every effort to designate specific fax machines that will be used to send and/or receive documents containing individually identifiable health information. Where possible, fax machines should be strategically located near the intended recipient(s) of the health information. Limiting the number of machines available to staff and housing those machines in a secured area (e.g., locked area, staffed area) or areas with controlled access (e.g., proximity card required to gain entrance into the area) will enable the agency to determine whether reasonable precautions for handling confidential information are being followed.

Incoming fax transmissions of documents that contain individually identifiable health information must be protected from unauthorized disclosure to staff or others who are not authorized to access the information. Each agency must determine the methods to be used in that agency to ensure the protection of incoming individually identifying health information via fax transmission. Staff should request that those faxing confidential information to the agency call in advance to schedule the transmission. Otherwise, incoming faxes containing individually identifiable health information must be promptly distributed to the appropriate party or placed in a secure place until the documents can be retrieved. This may require frequent monitoring of fax machines, security measures such as badges or door locks, as well as identification of staff that have been granted access to the area where the fax machine(s) is housed.

Efforts to protect outgoing fax transmission of documents containing individually identifiable health information shall be initiated by agency staff as listed below.

- Prior to faxing such documents, agency staff shall attempt to schedule the transmission with the recipient so that the faxed document can be promptly retrieved by the recipient.
- Whenever feasible, routine destination fax numbers should be pre-programmed into fax machines. DHHS agencies shall test pre-programmed numbers at regular intervals (e.g., monthly) to reduce transmission errors.
- Agencies should also request that routine recipients of faxed documents containing individually identifiable health information inform the agency immediately if their fax number(s) change so that agency records and pre-programmed numbers can be updated accordingly.
- Staff authorized to send faxes with individually identifiable health information shall check the recipient's fax number before transmittal and shall confirm delivery via telephone or review of the confirmation sheet of fax transmittal.
- Agencies shall implement procedures for maintaining and reviewing fax transmittal summaries and confirmation sheets.
- In the event of a misdirected fax, the recipient must be contacted immediately and shall be asked to destroy the information by burning or shredding the document. Misdirected faxes are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and

Disclosure Policies, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report in accordance with DHHS Privacy Policy, [Administrative Policies, Privacy Incident Reporting](#).

Fax Cover Sheet

DHHS agencies shall include the following confidentiality statement on all fax cover sheets used when transmitting documents containing individually identifiable health information. Other information may be added to this statement, if desired.

- Whenever documents accompanying a transmission contain confidential health information such documents are legally privileged. Such information is intended only for the use of the individual or entity named above. The authorized recipient of such documents is prohibited from disclosing this information to any other party unless required to do so by law or regulation. Recipients are required to destroy the information after its stated need has been fulfilled.
- If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, immediately notify the sender and arrange for destruction of these documents.

In addition to the required confidentiality statement, the fax cover sheet should contain:

- Sender's name, mailing address, e-mail address, telephone number, and fax number;
- Recipient's name, telephone number, and fax number;
- Number of pages transmitted, including coversheet; and
- Instructions for verification of fax receipt (e.g., phone call to sender to confirm receipt of the document).

E-Mail

Utilizing unencrypted e-mail transmissions to send individually identifying health information is strongly discouraged; however, it is recognized that there are times when such transmissions are necessary in order to efficiently operate business functions in the areas of treatment, payment, or health care operations. Prior to establishing e-mail communication containing individually identifying health information, DHHS agencies shall:

- Recognize that e-mail is considered public record but confidential information contained in or attached to an e-mail can be protected from public disclosure in accordance with NCGS 132-6(c).

- Recognize that e-mails containing individually identifying health information can be forwarded by the recipient to someone not authorized to have access to the information; therefore, DHHS agencies shall only transmit e-mails containing individually identifiable health information to persons within DHHS who are knowledgeable about DHHS Privacy Policies, to business associates, or to other covered entities (e.g., health plans, health care providers).
- Avoid using e-mail for particularly sensitive matters (e.g., HIV status, psychiatric disorders) and time-sensitive messages (e.g., appointment scheduled for next day).
- Avoid including individually identifiable health information in the subject line or body of an e-mail. If it is essential for the efficiency of business operations to send individually identifiable health information via e-mail, the information must be sent as a password protected attachment to the e-mail. Agencies are discouraged from using direct identifiers in the attached document (e.g., client name, social security number, address) and should de-identify the information whenever feasible in accordance with DHHS Privacy Policy, [Use and Disclosure Policies, De-Identification of Health Information and Limited Data Sets](#).
- In accordance with the State of North Carolina (NC) Enterprise Security Standard, S002, passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Passwords for e-mail attachments shall be provided to recipients in a secured manner (e.g., by phone, fax, or pre-assigned passwords provided to a receiving agency).
- Ensure that e-mails are addressed correctly by reviewing the recipient's e-mail address before sending the e-mail to ensure that the e-mail software did not automatically fill-in an incorrect e-mail address after the first few characters of the address were typed.
- When disclosing individually identifying health information to a third party for purposes other than treatment, payment, or health care operations, the disclosure must be documented and accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures.
- In the event of a misdirected e-mail with a file attachment that contains individually identifying health information, the recipient must be contacted immediately and shall be asked to delete the e-mail and attachment. Misdirected e-mails are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report in accordance with DHHS Privacy Policy, [Administrative Policies, Privacy Incident Reporting](#).

DHHS agencies shall include the following confidentiality statement on all e-mails containing individually identifiable health information as file attachments. Other information may be added to this statement, if desired.

- Whenever documents accompanying an e-mail contain confidential health information, such documents are legally privileged. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation. Recipients are required to destroy such information after its stated need has been fulfilled.
- If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and delete the e-mail and accompanying file attachment.

DHHS agencies shall safeguard client e-mail addresses and shall not use them for marketing or fundraising purposes or supply client e-mail addresses to any third party for advertising, solicitations, or any other use.

Telephone

Whenever it is necessary for agency staff to discuss individually identifiable health information via the telephone with a client or a client’s family members/friends, agency workforce members, business associates, other health care providers, or health plans, staff must follow the agency’s requirements for protecting such information.

Each agency shall develop and implement procedures for identifying individuals to whom a specific client’s health information may be released via the telephone. Each agency shall honor any agreed upon requests made by the client as to the use of alternate forms of communication (e.g., alternate telephone numbers) or restrictions regarding the use or disclosure of that clients individually identifying health information (see the DHHS Privacy Policy, [Client Rights Policies, Rights of Clients](#)). Agency procedures must include the stipulation that telephone conversations that include the use or disclosure of confidential information be conducted in private locations wherever possible and in a soft voice to ensure such information is shared with only the intended recipient.

Agency procedures should also include the following practices for receiving calls:

- Agency staff shall not discuss individually identifiable health information (e.g., client’s diagnosis or condition) until the following can be confirmed:
 - a. Identity of the caller (e.g., a “call back” to validate the number called or voice recognition) and
 - b. Verification that the caller has a need to know, and the use or disclosure of confidential information is permissible.
- If confirmation cannot be made, the agency shall not confirm or deny that the client has in the past or is currently receiving services from the agency. The

caller's information can be recorded and provided to the client for disposition.

Agency procedures should also include the following practices for making calls:

- Agency staff shall not discuss individually identifiable health information until the identity of the person on the phone line has been confirmed. This may be accomplished through voice recognition or call-back.
- In the event an answering machine/voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call. The message shall include **ONLY** the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313"). Messages left on an automatic answering machine or voice mail system shall not contain confidential health information (e.g., name of the client, diagnosis, test results).

Cellular/Wireless Telephones/Two-Way communication Devices

Agency staff shall be informed of the security risks of cellular/wireless phones. Communication via cellular and wireless phones should not be used to discuss confidential information as such communication is not secure, unless encrypted (transmissions via these devices can be intercepted using relatively simple 'listening' technology). Agency staff shall not use these devices to communicate confidential information unless there is an emergency and a wired, landline phone is not readily available.

Other Oral Communications

DHHS agencies must take reasonable steps to protect the privacy of all verbal exchanges or discussions of individually identifying health information, regardless of where the discussion occurs. Where possible, each agency shall make enclosed offices and/or interview rooms available for the verbal exchange of individually identifying health information.

In work environments that contain few offices or closed rooms, DHHS staff participating in the verbal exchanges of individually identifying health information shall conduct these conversations in a soft voice and as far away from others as possible.

C. Privacy Safeguards Training
DHHS agencies shall include training on safeguards in their privacy training required by the DHHS Privacy Policy, [Administrative Policies, Workforce](#). Staff shall be trained in the agency's procedures for carrying out all the administrative, physical, and technical safeguards the agency has in place to guard against unauthorized use or disclosure of individually identifiable health information.

D. Monitoring Compliance

Due to the complexity of this policy and the potential for relying on numerous clinical, professional, clerical and administrative staff, as well as business associates, each agency shall develop a system for monitoring compliance with this policy on an ongoing basis.

Physical Safeguards

A. Assessment

A physical safeguards assessment shall be conducted and the associated documentation maintained by each agency to demonstrate due diligence in complying with DHHS physical safeguards requirements. DHHS agencies may use the [NC DHHS Work Area Physical Safeguards Assessment for HIPAA Privacy Compliance](#) to assess their work areas for privacy and physical safeguards of individually identifiable health information. The information collected via this tool will assist each agency in determining where physical safeguard deficiencies exist and in identifying the measures necessary to secure the area. Agencies shall identify in their procedures the frequency and/or circumstances (e.g., office relocations or agency reorganizations that result in changes in the security of individually identifiable health information) that would require a review and updated physical safeguards assessment.

B. Physical Access

Each agency shall identify those areas wherein agency staff routinely maintain, transmit, and receive individually identifiable health information on paper, biomedical equipment, or other non-electronic medium (e.g., prescription bottles, test tubes, specimen vials). (**NOTE:** the Business Information Flow Assessment completed by each DHHS agency during the HIPAA assessment phase may help satisfy this requirement). Agencies must ensure these areas are routinely manned or physically secured as appropriate during business and non-business hours and that such areas are accessed only by authorized staff. Securing confidential information may be as simple as employing locks on file cabinets, safes, and desk drawers or as complex as relocating equipment or an entire work area to a more secure location.

Each agency shall develop and implement procedures for limiting physical access to individually identifiable health information maintained throughout the agency while ensuring that properly authorized access is allowed. Physical security of health information is most vulnerable in the following areas:

- Client records storage areas;
- Shared office areas containing faxes, copiers, and printers; and
- Open work areas or workstations.

Areas that use white boards, chalk boards, posters, etc. must be evaluated to ensure individually identifiable health information is not displayed or unintentionally disclosed through these devices. For example, agencies may develop the following procedures:

- Post client first name and last initial (or vice versa) on boards.
- Cover information identifying clients with a cover sheet.
- When a client's record is placed in a bin outside an examination/treatment room, position the record so that the client's name is not visible.

Biomedical devices such as electrocardiograph machines and medical imaging systems must be safeguarded from unauthorized access if they display memory, connect to another system, or transfer data.

Each agency shall maintain documentation of building repairs, workspace modifications, and equipment purchases that are instituted to cure physical safeguard deficiencies. Such records will serve as documentation of due diligence for physically safeguarding the health information maintained by the agency.

Safeguarding Confidential Information Displayed on Computer Screens

DHHS agencies shall ensure that observable individually identifying health information displayed on computer screens is adequately shielded from unauthorized disclosure. Agencies shall safeguard individually identifiable health information displayed on computer monitors by:

- Relocating the workstation or repositioning the computer monitor so only the authorized user can view it;
- Installing polarized screens (also referred to as privacy or security screens) or other computer screen overlay devices that shield information on the screen from persons who are not directly in front of the monitor; and
- Clearing information from the computer screen when it is not actually being used, turning off computer when not in use, or by activating a password-protected screen-saver.

1. C. Safeguard Measures

Each agency shall take reasonable steps to ensure the privacy of client information in treatment areas and other areas in the agency where visitors, repairmen, vendors, and family members are permitted. General safeguards shall include measures the facility has implemented that protect individually identifiable health information from unauthorized use or disclosure.

1. Facility Safeguards

- c. Sign-in Sheets – Ensure sign-in sheets that are viewed by multiple clients do not contain health information (e.g., reason for visit) and unnecessary identification information (e.g., address, Social Security Number).
- d. Client/Staff Conversations – Establish precautions to prevent conversations regarding client information from being overheard by others. Designate an area away from waiting areas to have conversations involving confidential information. See the [Administrative Safeguards, Other Oral Communications](#) section above for additional information concerning safeguarding verbal exchanges of individually identifying health information.
- e. Intercom – Limit information given over an intercom system. For example, do not instruct specific clients to report to a certain testing or procedure area.
- f. Treatment Areas – Limit access to treatment areas. Individuals that are not essential workforce members (e.g., clients, family members, drug reps) should be escorted in all treatment areas.
- g. Client Records – Assure clients records used in treatment areas are reasonably protected to prevent inadvertent disclosures. This may include placing a cover sheet over records sitting on a desk or positioning a client’s record so that the client’s name is not visible. Client records shall be maintained in areas that can be secured (e.g., locked office/nursing station, locked file cabinet).

2. Visitor Safeguards

- h. Sign-in Logs – Ensure sign-in logs are used that record the visitor’s name, company, area visited, time in, and time out.
- i. Badges – Provide visitors with identification badges.
- j. Escort – Establish procedures for when visitors must be escorted within the agency. Unescorted visitor access should be limited to those areas that do not contain individually identifying health information. Areas containing confidential information, such as treatment areas and client records storage areas, should not be

available to visitors without an escort.

2. D. Disposal of Paper Documents and Supplies Containing Individually Identifiable Health Information

Each agency shall establish a process for safely disposing of paper and other materials containing individually identifiable health information. Paper records include, but are not limited to, client records, billing records, and correspondence. Other materials include, but are not limited to, client consumables and non-durable medical equipment such as x-ray films, identification bracelets, identification plates, IV bags, prescription bottles, syringes, diskettes, disk drives, etc. Refer to the [NC General Schedule for State Agency Records](#) or the individual agency record retention and disposition schedule, before disposing of any documents containing individually identifying health information. (NOTE: The disposal of electronic information will be addressed in the DHHS Security Policies.)

It is recommended that, where practical and when permitted, paper materials containing individually identifiable health information be shredded or burned. All steps in the shredding or burning process shall be protected, including any shred/burn boxes, bins, and bags containing individually identifying health information to be destroyed. When shredding or burning of paper and other materials is not possible or permissible (e.g., disposal of x-rays containing silver), a reasonable process should be developed that ensures health information is otherwise destroyed or de-identified in a manner that prevents unauthorized disclosure.

If a contract company is used for disposal wherein the disposal is not monitored by a member of the agency workforce, the company must sign a business associate agreement (see DHHS Privacy Policies, [Administrative Policies, Business Associates \(Internal/External\)](#)).

3. E. Working Outside the Secured Work Environment

Allowing DHHS workforce members to remove individually identifying health information from a DHHS agency premises for purposes other than treatment or in response to a court order, or allowing workforce members to access individually identifiable health information outside of the secured work environment, is strongly discouraged. However, it is recognized that there may be circumstances where work outside of the secured environment is necessary (e.g., performing transcription of client information from home). DHHS agencies shall develop and implement procedures to ensure the security of confidential information taken outside the secured work environment, including, but not limited to, the following guidelines.

1. Ensure privacy and security of remote work area;

2. Restrict telephone conversations to a private area using a wired, landline phone;
3. Ensure faxed documents are handled according to the guidelines in this policy; and
4. Secure confidential information in locked rooms or locking storage containers (e.g., filing cabinets, safes, desk drawers) when not in use.

Original client medical or financial records in paper format shall never be removed from the DHHS agency responsible for safeguarding the records unless under order of the court or when necessary for treatment purposes (which includes autopsies).

Technical Safeguards

A. Granting Access to Individually Identifying Health Information

Each agency shall determine which workforce members, or classes of workforce members based on job responsibility, require access to individually identifiable health information. Privileges shall be established on a “need to know” basis for each user relative to their specific relationship with clients and specified business needs for accessing individually identifiable health information. It will be the responsibility of each agency to determine the level of individually identifiable health information detail a workforce member can access, such as an entire record, department files, individuals’ files, workstation, software applications, electronic data, electronic report files (e.g., X/PTR), etc. The access level of individually identifiable health information granted to an individual shall be the minimum necessary needed to do his/her job (see DHHS Privacy Policy [Use and Disclosure Policies, Minimum Necessary](#)).

Agencies shall establish a process for evaluating members of their workforce and their internal and external business associates regarding their need for access to individually identifying health information and for ensuring that the minimum necessary access requirement is employed.

4. B. Password Management

DHHS agencies shall require its staff to use personal passwords in situations determined appropriate by the agency. Agencies shall develop procedures to ensure passwords are protected and define situations or circumstances when a supervisor or other designated staff may have access to a user’s password. In special cases where a user is required to divulge his/her personal password such as for system support, the user shall immediately change the password.

5.

Passwords shall not be included in e-mail messages or unencrypted computer files; nor shall passwords be stored in a location readily accessible to others (e.g., desk drawer, note on a computer, bulletin board in office).

Agencies shall require staff with access to individually identifiable health information to change their password at least every 90 days or immediately if the security of a password has been jeopardized.

Additional information regarding password protections can be found in the ITS Statewide Information Security Manual, Chapter 2, "[Controlling Access to Information and System](#)", Section 0106, "Managing Passwords."

Reference

DHHS Directive Number III-11; 45 CFR 164.530(c); NCGS 132-6; 10A NCAC 26B .0105; State of N.C. Enterprise Security Standard, S002

For relevant forms:

[NC DHHS Work Area Physical Safeguards Assessment for HIPAA Privacy Compliance](#)

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](#).