Title:	**DPH Privacy and Security Manual**
Chapter:	**II. Administrative Policies, Privacy Safeguards**
Current Effective Date:	**September 22, 2003**
Original Effective Date:	**April 14, 2003**
Revision History:	**April 22, 2004**
	May 1, 2011
	January, 2014

Purpose

The purpose of the Division of Public Health (DPH) privacy safeguards policy is to establish the privacy safeguards that protect individually identifiable health information (IIHI) within DPH. This policy is in compliance with the DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, that establishes the NC Department of Health and Human Services (DHHS) requirements for privacy safeguards to protect IIHI. Privacy safeguards protect IIHI from unauthorized use or disclosure and from tampering, loss, alteration or damage.

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

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule requires covered health care components to implement ***appropriate*** administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of IIHI.

Safeguards addressed in this DPH Privacy Policy include the administrative, physical, and technical protections necessary for safeguarding all IIHI in all formats as it is found in the working environment (e.g., oral communications, paper records, medical supplies/equipment, computer screens, etc.).

Note: The DPH HIPAA Security Policies further define the administrative, physical and technical mechanisms necessary for safeguarding electronic data containing IIHI (e.g., software applications and systems).

Policy

DPH workgroups shall put into place appropriate administrative, physical, and technical safeguards to protect the privacy of individually identifiable health information. Workgroups shall take steps to reasonably safeguard IIHI from intentional or unintentional use or disclosure that is in violation of Departmental and Division privacy policies, federal and state laws and regulations, and program requirements. DHHS has determined that safeguarding confidential health information should be extended to all DHHS agencies within the Department that maintain IIHI. The Division has applied this policy to all workgroups within the Division that use, maintain, have access to, or come into contact with IIHI.

Administrative Safeguards

DPH workgroups shall safeguard IIHI that is generated, received, used, or maintained throughout their workgroup. Confidential information that is transmitted by facsimile (fax) machines, printers, copiers, telephone or other oral means of communication shall be protected from unauthorized use and disclosure.

Physical Safeguards

DPH workgroups shall safeguard IIHI that is generated, received, used, or maintained throughout their workgroup by addressing protections used for equipment/supplies and physical locations to prevent unauthorized use or disclosure of IIHI used or maintained by their workgroup.

Technical Safeguards

DPH workgroups shall safeguard IIHI that is generated, received, used, or maintained throughout their workgroup by addressing technical safeguards used for accessing confidential information maintained in computer systems and other electronic media by identifying staff who need access to electronic data and by following Division procedures for controlling access to electronic data.

Implementation

DPH workgroups shall assess the nature of the IIHI that it receives, sends, uses, and/or maintains throughout their workgroup and shall implement reasonable administrative, physical, and technical safeguards to ensure that such information is protected and is not subject to unauthorized use or disclosure.

The Division has developed protections that are flexible, scalable, and provide reasonable safeguards that realistically address most situations. The safeguards implemented in different workgroups within the Division may vary depending on their physical location, their interaction with clients, their specific legal and programmatic requirements, and other factors. Every DPH workgroup **must** implement the minimum reasonable safeguards and follow the basic guidelines in this policy to ensure that IIHI is protected. DPH Workgroups can implement more stringent safeguards, and when more than one policy or procedure exists, the stricter standards shall apply to the specific DPH workgroup.

A quick reference summary of reasonable safeguards is included with the safeguards policy. This document is called Summary Guidelines for Safeguarding the Privacy of Health Information.

The Division Privacy Office is available to consult with the DPH workgroups to implement appropriate and reasonable safeguards according to this policy.

Administrative Safeguards

Administrative Safeguards include the following:

- Authorized disclosures
- Minimum necessary for disclosures
- Safeguarding methods for disclosure
  - Mail or hand delivery
  - Facsimiles
  - Email
  - Telephone
  - Other oral communications
- Safeguards training.

Authorized Disclosures of Individually Identifiable Health Information

Disclosure and exchange of IIHI is essential to for the Division to fulfill its mission of protecting and improving the health of the people who live and work in North Carolina. Our public health partners require disclosures of IIHI for a variety of reasons including Treatment, Payment of health care services, or health care Operations (TPO) purposes. DPH is also authorized to disclose IIH for specific public health purposes.

Before disclosing IIHI, DPH should make sure that the disclosure meets one (or more) of the following criteria:

- 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 Division has granted
- The disclosure is required by law
- The disclosure is permitted by law
- The disclosure is within the boundaries defined by applicable federal and state laws and regulations and specific public health program requirements
- The disclosure is for public health activities
- The disclosure is for public health program oversight and monitoring, as defined by program requirements.

The *DPH Privacy Policies, Use and Disclosures* provide guidelines on disclosures of IIHI.

To safeguard against unauthorized disclosure, DPH staff must understand the federal and state laws and regulations that apply to their program regarding use and disclosure of IIHI. Staff must also understand their specific programmatic reporting requirements regarding IIHI.

Minimum Necessary for Disclosures of Individually Identifiable Information

All DPH workgroups must make reasonable efforts to limit the use and disclosure of IIHI to that which is minimally necessary to support the intent of disclosure. Minimum necessary requirements are designed to limit access to IIHI to staff and others who have a "need to know" the information. Before disclosing IIHI, staff must evaluate the source and purpose of the disclosure and determine what is the minimum amount of IIHI required to fulfill the intent of the authorized disclosure. Staff should not disclose more than is required to fulfill the purpose of the disclosure. When requesting and using IIHI, staff should understand their program requirements and objectives and not request or access more detailed IIHI than required to complete their job responsibilities.

The DPH Privacy Policy, Minimum Necessary defines the minimum necessary policy and implementation procedures.

Safeguarding Methods for Disclosure of Individually Identifiable Health Information

DPH workgroups shall follow the guidelines described below to ensure that the methods used for disclosing IIHI provide safeguards to protect client confidentiality.

Mail or Hand Delivery

Whenever feasible, documents and other medium (e.g., diskettes, CDs) containing IIHI should be hand delivered or mailed using the US Postal Service, courier, or other delivery service. All documents and other media containing IIHI shall be placed in a secure container (e.g., sealed envelope, lock box), addressed to the recipient, and include a return name and address. It is recommended that you label the material containing the IIHI as "Confidential" whenever practical. IIH stored on electronic media should be password-protected.

Note: *On interoffice mail delivered via state courier services, the interoffice envelope does not provide a place for return address. Staff should include a return address within the package containing IIHI so misdirected information can be returned.*

Facsimiles

DPH workgroups must make every effort to designate specific fax machines that will be used to send and/or receive documents containing IIHI. Where possible, fax machines should be strategically located near the intended recipient(s) of the health information. Limiting the number of machines and housing those machines in a safe, non-public area will enable the Division to determine whether procedures for handling confidential information are being followed.

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

Staff shall initiate efforts to protect outgoing fax transmission of documents containing IIHI as follows:

- Where practical, documents containing IIHI should be labeled "Confidential."
- Before faxing such documents, staff should attempt to schedule the transmission with the recipient, so that the recipient can promptly retrieve the faxed document.

- Whenever feasible, routine destination fax numbers should be pre-programmed into fax machines. Staff should test pre-programmed numbers at regular intervals to reduce transmission errors. Staff should also request that routine recipients of faxed documents containing IIHI inform them immediately if their fax number(s) change so that DPH workgroup records and programmed numbers can be updated.

- Staff who send faxes with IIHI should check the recipient's fax number before transmittal and confirm delivery via telephone or review of the confirmation of fax transmittal where feasible.

- Each DPH workgroup should retain fax transmittal summaries and confirmation sheets for those fax transmittals that contain IIHI.

- In the event of a misdirected fax, the recipient must be contacted immediately and shall be asked to destroy the information. Misdirected faxes are considered accidental disclosures and must be accounted for in accordance to DPH Privacy Policy, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report in accordance with DPH Privacy Policy, Privacy Incident Reporting.

Fax Cover Sheet

All DPH workgroups shall include the following confidentiality statement on all fax cover sheets used when transmitting documents containing IIHI.

> *The documents accompanying this facsimile contain confidential information that may be legally privileged and protected by federal and state law. This information is intended for use only by the individual or entity to whom it is addressed. The authorized recipient is obligated to maintain the information in a safe, secure, and confidential manner. The authorized recipient is prohibited from using this information for purposes other than intended, prohibited from disclosing this information to any other party unless required to do so by law or regulation, and is required to destroy the information after its stated need has been fulfilled.*
>
> *If you are in possession of this protected health information and are not the intended recipient, you are hereby notified that any improper disclosure, copying, or distribution of the contents of this information is strictly prohibited. Please notify the owner of this information immediately and arrange for its return or destruction.*

The text of the confidentiality statement is also included as an attachment to Summary Guidelines for Safeguarding the Privacy of Health Information so it can be copied onto a fax cover sheet.

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

- Sender's contact information (e.g., individual name(organization name not recommended), mailing address, e-mail address, telephone number, and fax number)
- Recipient's contact information (e.g., name, telephone number, and fax number)
- Number of pages transmitted, including coversheet
- Instructions for verification of fax receipt (optional).

Email

Using unencrypted email transmissions to send IIHI is discouraged, especially when communicating very sensitive identifying information such as HIV/STD, substance abuse, psychiatric disorders. In addition, it can sometimes be very difficult to control the distribution and disclosure of emails after they reach the recipient.

Before establishing email communications containing IIHI, DPH workgroups must:

- Recognize that while email is considered public record confidential information contained in or attached to an email can be protected from public disclosure in accordance with N.C. G.S. 132-6.
- Recognize that emails containing IIHI can be forwarded by the recipient to someone not authorized to have access to the information; therefore, communications via email shall only be sent to persons who understand the DHHS and DPH privacy policies and applicable federal and state laws regarding confidentiality.

If IIHI is transmitted via email, the following safeguards must be followed:

- Do not include IIHI in the subject line or body of an email. If it is essential for the efficiency of business operations to send IIHI via email, the information must be sent as a password protected attachment to the email.

  Notes: Do send document passwords in the same email as the password-protected attachment.

  Contact your IT support specialists for information about encrypting email attachments.

- Whenever possible, avoid using direct identifiers in the attached document (e.g., client name, social security number, address) and if possible further de-identify the information. Limit the information to the minimum necessary to accomplish the purpose.
- Notify the intended recipient of the information that the information will be forthcoming and provide the recipient with the password to open the file attachment.
- Ensure that e-mails are addressed correctly by reviewing the recipient's email address before sending the e-mail and making sure the e-mail client software did not automatically fill in an incorrect e-mail address after the first few characters were typed.

- Include your contact information on the email (name and phone number at a minimum).
- In the event of a misdirected email with a file attachment that contains IIHI, 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 DPH Privacy Policy, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report in accordance with DPH Privacy Policy, Privacy Incident Reporting.
- Where practical, label the attachment "Confidential."
- All email that includes IIIH as an attachment should include the following text:

  The documents accompanying this email contain confidential information that may be legally privileged and protected by federal and state law. This information is intended for use only by the individual or entity to whom it is addressed. The authorized recipient is obligated to maintain the information in a safe, secure, and confidential manner. The authorized recipient is prohibited from using this information for purposes other than intended, prohibited from disclosing this information to any other party unless required to do so by law or regulation, and is required to destroy the information after its stated need has been fulfilled.

  If you are in possession of this protected health information and are not the intended recipient, you are hereby notified that any improper disclosure, copying, or distribution of the contents of this information is strictly prohibited. Please notify the owner of this information immediately and arrange for its return or destruction.

  Staff should not include the confidentiality statement on routine emails that do not include IIHI.

Note: If staff have questions about emailing IIHI, they should discuss them with their supervisor. The DPH Privacy Office is also available to provide guidance regarding using email to communicate IIHI.

Telephone

When it is necessary for staff to discuss IIHI via the telephone with a client or a client's family members/friends, Division workforce members, Division business associates, public health partners, other health care providers, or health plans, staff must ensure that measures for protecting such information are followed.

Staff must confirm the identity of individuals to whom a specific client's health information may be released via the telephone. Where applicable, staff must 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 IIHI.

Telephone conversations that include the use or disclosure of confidential information be conducted in private locations wherever possible and in a low voice to ensure such information is shared with only the intended recipient.

Receiving Calls

Staff shall not discuss IIHI until the following can be confirmed:

- Identity of the caller (this may require a "call back" to validate the number called)
- Verification that the caller has a need to know and that the use or disclosure of confidential information is permissible.

Making Calls

Staff shall not discuss IIHI until the identity of the person answering the phone has been confirmed.

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. Staff should not leave the name of your program or other information that could compromise client confidentiality if someone other than the recipient were to listen to message. Messages left on an automatic answering machine or voice mail system shall not contain IIHI (e.g., name of the client, diagnosis, laboratory results).

Cellular/Wireless Telephones

Staff shall be aware 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. Staff shall not use these devices to communicate confidential information unless there is an emergency and a wired, land-based phone is not readily available.

Other Oral Communications

Staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of IIHI, regardless of where the discussion occurs. Where possible, each DPH workgroup should make enclosed offices and/or interview rooms available for the verbal exchange of IIHI.

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

Safeguards Training

DPH safeguards training is included in the DPH Basic Privacy Training, which is required by the DPH Privacy Policy, Workforce. Staff shall be informed about the procedures for carrying out all the administrative, physical, and technical safeguards the Division has in place to guard against unauthorized use or disclosure of IIHI. Staff shall also be informed about the specific safeguards implemented within their workgroup.

Physical Safeguards

Physical safeguards include the following:

- Physical safeguards assessment
- Physical access
- Safeguarding confidential information on premises
- Facility safeguards and client areas
- Visitor safeguards
- Securing confidential information on computer screens
- Disposal of Paper Documents/Supplies
- Working outside the secured work environment.

Physical Safeguards Assessment

A physical safeguards assessment shall be conducted and the associated documentation maintained by the Division to demonstrate due diligence in complying with DHHS and DPH physical safeguards requirements. The DPH Privacy Office conducts this assessment and maintains this documentation centrally. The Division uses the NC DHHS Work Area Privacy Physical Safeguards Assessment for HIPAA Privacy Compliance tool to assess their work areas for privacy and physical safeguards of IIHI. The information collected with this tool helps the Division determine where physical safeguard deficiencies exist and identify the measures necessary to secure the area.

As part of compliance for privacy, baseline assessments have been completed for DPH locations where IIHI is used or maintained. Physical assessment of locations containing IIHI continues as part of ongoing privacy compliance. The DPH Privacy Office will re-assess work locations periodically.

The DPH Privacy Office may elect to conduct physical assessments whenever major changes occur in physical locations (for example relocation of workgroups, significant changes in office layout). Also, as the ongoing physical safeguards assessment, the DPH Privacy will use the NC DHHS Work Area Privacy Physical Safeguards Assessment for HIPAA Privacy Compliance tool to track and note improvements and other measures taken to address physical safeguards. This will serve as documentation of due diligence for physically safeguarding the health information maintained by the agency. The DPH Privacy Office maintains this documentation centrally.

Physical Access

Each DPH workgroup agency shall identify those areas where staff routinely maintain, transmit, and receive IIHI on paper, biomedical equipment, or other non-electronic medium. Workgroups must ensure these areas are routinely secured as appropriate during business and non-business hours and only authorized staff accesses these areas.

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 area to a more secure location.

Each DPH workgroup shall implement procedures for limiting physical access to IIHI maintained throughout their area, 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
- Open work areas or workstations.

Safeguarding Confidential Information on Premises

DPH workgroups shall take reasonable steps to ensure the privacy of client information in areas where visitors, repairmen, vendors and others are permitted. General safeguards must be implemented that protect IIHI from unauthorized use or disclosure.

DPH workgroups must use the following safeguards:

- Always store client information securely in locked drawers, file cabinets, offices, or office suites when the work area is unattended
- Post only client first name and last initial (or vice versa) on boards
- Always erase client information from boards, making sure the information is thoroughly erased using cleaning solvent if necessary
- Use a cover sheet to mask information that can identify individuals.
- Do not leave client information unattended in public or other open areas such conference or meeting rooms
- When a client's record or other identifying information is placed in a bin or mailbox outside an area that is visible to visitors or others, position the record so that the client's information is not exposed.

Facility Safeguards and Client Areas

The following facility safeguards must be implemented by DPH workgroups in locations where clients visit to discuss confidential information:

- Client 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).
- Client/Staff Conversations – Establish precautions to prevent conversions regarding client information from being overheard by others. Designate an area away from waiting areas to have conversations involving confidential information. See the *Other Oral Communications* section above for additional information concerning safeguarding verbal exchanges of IIHI.
- Intercom or Calling out - Limit information given over an intercom system or called out in a waiting area. For example, do not instruct clients to report to a certain testing or procedure area.
- Treatment or other Examination Areas – Limit access to treatment areas. Individuals who are not essential workforce members (e.g., clients, family members, others) should be escorted to all treatment or examination areas.
- Client Records – Assure clients records used in treatment or examination 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).

Visitor Safeguards

DPH workgroups must take reasonable measures to control and monitor visitor access to locations where IIHI is used and maintained. The measures required to safeguard visitor access will of necessity vary depending on the physical location where the workgroup is located, the type of access required for the location, and the type of work being conducted at the location. Administrative offices, for example, might require less stringent measures than the State Laboratory for Public Health.

At a minimum, DPH workgroups must follow all the safeguards for securing IIHI on premises to ensure that visitors do not unintentionally observe client information to which they do not require access. Staff should also be aware of visitors or those they don't recognize in their area and ask politely if they can be of help. This can often either confirm that the visitor should be in the area or can point the visitor to an area they are looking for.

Other measures that may be implemented include:

- Locked facilities (via key, swipe card or other methods) requiring that visitors request entry.
- Secure areas within facilities where access to the whole facility cannot be restricted. Examples include lockable office suites, lockable offices, posting restricted access notices.

- Sign-in Logs – Using sign-in logs to record the visitor's name, company, area visited, time in, time out, and person visited, if appropriate.
- Visitor Badges – Using visitor badges to identify visitors.
- Escort – Providing visitors with an escort in cases where access must be restricted. In these locations, unescorted visitor access should be limited to those areas that do not contain IIHI. Areas with IIHI such as treatment areas and client records storage areas should not be available to visitors without an escort.
- Prevent Tailgating - Do not allow others without proper security credentials to enter secure areas behind.
- External doors must not be propped or otherwise left open.

Safeguarding Confidential Information on Computer Screens

DPH workgroups shall ensure that observable IIHI displayed on computer screens is adequately shielded from unauthorized disclosure. DPH workgroups shall safeguard IIHI displayed on computer monitors by:

- Relocating the workstation or repositioning if necessary the computer monitor so only the authorized user can view it
- Clearing information from the computer screen when it is not actually being used
- Using password-protected screen savers or turning off computer when not in use
- Securing access to the computer with a password and change the password regularly (90 days recommended)
- Logging out of the network when the computer is not in use.

As an option where appropriate, polarized screens (also referred to as privacy or security can screens) or other computer screen overlay devices can be installed to shield information on the screen from persons who are not directly in front of the monitor

Disposal of Paper Documents / Supplies Containing IIHI

DPH workgroups must ensure the safe disposal of paper and other materials containing IIHI. Paper records consist of, but are not limited to, client records, billing records, computer-generated reports, client listings, and correspondence. Other materials consist of, but are not limited to, consumables and non-durable medical equipment such as x-ray films, identification bracelets, identification-plates, IV bags, prescription bottles, syringes, etc. Refer to the NC General Schedule for State Agency Records or the Division's record retention and disposition schedule, before disposing of any documents or other material containing IIHI.

DPH workgroups should:

- Shred all paper materials containing IIHI, using a cross-sectional paper shredder whenever practical.

- Ensure that all steps in the shredding process are protected, including any shred boxes, bins, and bags containing IIHI to be shredded. Containers with material waiting to be shredded should be lockable.
- Have a staff member monitor shredding by any contracted onsite-shredding firm. If a contract company is used for disposal and a staff member workforce cannot monitor the disposal, the disposal company must sign a business associate agreement.
- Return all material with IIHI to the sender if copies are not required for DPH purposes. Many contracts and other stipulations required that material with IIHI be returned after it is no longer needed.
- Follow all legal and medical requirements for the safe disposal of medical consumables and non-durable medical equipment.

When shredding of paper and other materials is not possible, a reasonable process should be developed that ensures health information is otherwise destroyed or de-identified in a manner that prevents unauthorized disclosure.

Disposal of Electronic Media Containing IIHI

DPH workgroups must ensure the safe disposal of IIHI on electronic media such as floppy disks, CDs, zip drives, and desktop hard drives. Refer to the NC General Schedule for State Agency Records or the Division's record retention and disposition schedule, before disposing of any media containing IIHI.

Note: The disposal of electronic information is addressed more fully in the DPH Security Policies.

DPH workgroups should:

- Never store files, emails, etc., containing IIHI on their hard drives except temporarily while they are being worked on. Files with IIHI should be stored on secure network drive and the material deleted from local drives or email server on which the data resides.
- Not reuse portable storage media such as floppy disks or CDs that contain IIHI without sanitizing them first. Contact DPH IT for procedures on how to sanitize portable storage media.
- Destroy portable storage media such as floppy disks and CDs before disposing them.

DPH staff should contact DPH IT before moving a computer or transferring it to another user. DPH IT will ensure that proper procedures are followed to secure the information in transit or to sanitize the hard drives before reassigning the computer.

Working Outside the Secured Work Environment

Staff shall take measures to ensure the security of confidential information taken outside the secured work environment, including, but not limited to, the following guidelines.

- Original client medical, financial, or other records should not be removed from the DPH workgroup area responsible for safeguarding the records unless approved by the appropriate DPH management responsible for the program area.
- Ensure the privacy and security of remote work areas, including locked remote (home) offices, locked file cabinets and locked desks.
- Secure confidential information in locked rooms or locking storage containers (e.g., filing cabinets, safes, desk drawers) when not in use.
- Secure the information when in transit, making sure that it is not visible in a car. Make sure the car is locked and material stored in the trunk whenever possible. Otherwise, if information must be kept in the car, store it in lockable attaches, lock boxes, or other secure opaque containers.
- Restrict telephone conversations involving IIHI to a private area using a wired, land-based phone.
- Ensure that when using remote fax machines, faxed documents are handled according to the guidelines in this policy.

Technical Safeguards

Technical safeguards include the following:

- Granting Access to IIHI
- Password Management.

Granting Access to Individually Identifiable Health Information

Each DPH workgroup shall determine which workforce members, or classes of workforce members based on job responsibility, require access to IIHI. 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 IIHI. It is the responsibility of each workgroup to determine the level of IIHI detail a workforce member can access, such as an entire record, department files, individuals' files, workstation, software applications, electronic data, electronic report files, etc. The access level of IIHI granted to an individual should be the minimum necessary needed to do his/her job.

Within the Division, access to computer systems containing IIHI is limited through reasonable access controls wherever technically feasible:

- Business owners are responsible for each application and they coordinate access control with the appropriate staff responsible for supporting the specific application.
- The appropriate administrators responsible for managing the technical environment and applications containing IIHI implement access controls.
- Users are assigned the applicable access rights based on their job function when they are set up to use the specific application.
- Users access rights are changed when necessary and as appropriate based on changes in their job function or responsibilities.

Password Management

The Division requires all staff to use personal passwords when accessing any electronic media containing IIHI. Passwords should never be revealed to anyone, including family members or co-workers. DPH workgroups can define specific requirements and situations where their supervisor or program backup requires access to an individual's password, for example, when a worker is absent and access to protected information is essential to meet program objectives or serve clients. In other 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.

Passwords shall not be stored in a location readily accessible to others (e.g., desk drawer, note on a computer, bulletin board in office).

Staff with access to IIHI should change their password often (90 days recommended) and whenever they think the security of their password has been jeopardized.

References: DHHS Directive Number III-11; DHHS Policy and Procedure Manual, Section VIII, Security and Privacy, DPH HIPAA Compliance Statement, 42 CFR 164.530(c), NC General Statutes 132-6, NC General Statutes 130A, 10A NCAC

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