NC Division of Public Health
Summary Guidelines for Safeguarding the Privacy of Confidential Information

These are guidelines centered on how to safeguard confidential information and ensure privacy when using normal business communications, such as conversations, telephone, faxes, mail, and electronic mail. Wherever practical, the material containing confidential information should be labeled as confidential on the document, diskette, CD, or other medium. Confidential information maintained electronically should be password-protected.

Also when using and disclosing confidential information, you must take reasonable measures to ensure the information is protected. Below are simple safeguarding tasks that should be used when communicating in a work environment that necessitates access to and use and disclosure of confidential information. Remember to limit your communications of confidential information to the minimum necessary for the intended purpose. Restrict your communications to those who have a valid "need to know" the information. If you have questions about these safeguards and how to protect confidential communications, please discuss them with your supervisor.

What is confidential information:

- Protected health information (including medical and financial information)
- SSN and other individual identifiers (potential for identity theft)
- User logon IDs and passwords
- Personnel records, including employee personal contact information
- Information related to security (facilities, networks, etc.)
- Specifics about emergency response and continuity of operations plans
- Details about IT configurations (IP addresses, server and network details)

Oral Conversations – in person

- Discuss confidential information private. Use an office with a door whenever possible, or leave areas where others can overhear.
- Be aware of those around you and lower your voice when discussing confidential information.
- Point out confidential information on paper or on-screen non-verbally when discussing confidential information.

Oral Conversations – telephone

- Follow the above guidelines for "Oral Conversations"-in person"
- Don't use names instead say; "I have a question about a client".
- Never give confidential information over the phone when talking to unknown callers, but call back and verify phone number.
- Never leave confidential information on voice messages; instead leave a message requesting a return call to discuss a client giving only your name and phone number.
- Do not discuss confidential information over unencrypted cellular or portable (wireless) phones or in an emergency, as the transmissions can be intercepted.

Fax

- Put fax machines in a safe location, not out in the open or in a public or area with high-traffic or easy access and visibility.
- Use a cover sheet clearly identifying the intended recipient and include your name and contact information on the cover sheet.
- Include a confidentiality statement on the cover sheet of faxes that contain confidential information.
- Include on the cover sheet instructions for verifying fax receipt, where applicable.
- Do not include or reference confidential information on cover sheet.
- Confirm fax number is correct before sending.
- If option is available, pre-program fax numbers in the auto dialer.
- Send fax containing confidential information only when the authorized recipient is there to receive it whenever possible.
- Verify that fax was received by authorized recipient; check the transmission report to ensure correct number was reached and when necessary contact the authorized recipient to confirm receipt.
- Deliver received faxes to recipient as soon as possible. Do not leave faxes unattended at fax machine.

Email Data Transfer

- Do not send confidential information via unsecured email. Email must be secure to federal/state encryption standards.
- Encrypt to federal/state standards email attachments containing information.
- Do not include confidential information in Subject-line or in Body of email.
- Transmit confidential information only in a password-protected encrypted attachment.
- Include a confidentiality statement on emails that contain any confidential information in email attachments.
- Do not send attachment passwords via email, but call the recipient to provide password.
- Include your contact information (name and phone number minimum) as part of the email.
- Use verified email distribution lists whenever possible.
- Set email sending options to request an automatic return receipt from your recipient(s).
- Request that email recipients call to discuss specific confidential data.
- Do not store emails or email attachments with confidential information on your hard drive but copy and store to a secure server. Delete the email and the attachments when they are no longer needed.

Courier and Regular Mail

- Use courier or mail to send confidential information in any medium (paper, CDs, diskettes).
- Use sealed secured envelopes to send confidential information.
- Verify that the authorized person has received the package.
- Deliver all mail promptly to the recipient.
- Mailboxes must be in safe areas, avoiding public or high-traffic areas.
- Locked mailboxes should be used where ever possible.

NC Division of Public Health
Summary Guidelines for Safeguarding the Privacy of Confidential Information

Inter-Office Mail

- Put confidential information in closed inter-office envelopes. As an added precaution, put confidential information in a sealed envelope inside the inter-office envelope.
- Identify recipient by name and verify mail center address.
- Distribute inter-office mail promptly to recipients.
- Do not leave unattended in mailboxes.

Computer Workstations and Remote (or home-based) Workers

- Use password protected screen savers, turn off the computer, or log out of the network when not at your desk.
- Position screens so they are not visible to others.
- Secure workstations and laptops with password.
- Change passwords on a regular basis (90 days recommended).
- Do not leave laptop or work-related confidential information visible or unsecured in a car, home office, or in any public areas.
- Ensure that all confidential information used outside work premises is protected using appropriate measures such as locked home offices, desks, file cabinets.
- Never remove original copies of confidential information from the agency without your supervisor's approval for specific purposes.
- Store files that contain confidential information on a secure LAN, not on your workstation hard drive.
- When absolutely necessary to store confidential information locally on your workstation temporarily, encrypt desktops in high risk, remote locations to specified standards (See DPH IT)

Disposal of confidential information

- Shred all hard copies containing confidential information when the copies are no longer needed, using a cross-sectional shredder if available.
- Place hardcopies to be recycled in locked recycle bins if available.
- Delete all soft copy files containing confidential information from your computer and from the server when the information is no longer needed within the record retention requirements.
- Destroy all disks, CDs, etc., that contained confidential information before disposing them.
- Do not reuse disks, CDs that contained confidential information without sanitizing them first.
- Contact DPH IT before transporting or transferring equipment for proper procedures to move equipment and to sanitize hard drives and other media.
- Return the confidential information to the sender, if this requirement is stipulated in any contractual agreements.

Work Areas

- Do not leave confidential information (files, records, Rolodex, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.
- Store all confidential information securely in locked file cabinets, desk drawers, offices, or suites when you are not in your work area.

Laptops and Removable Storage

- All laptops must be encrypted to specified standards (see DPH IT).
- All removable storage devices (disk drives, USBs, DVDs/CDs) containing confidential information must be encrypted to specified standards (see DPH IT).

Data Transfer

- Use secure encrypted data transmissions to specified standards for all electronic data transfers (see DPH IT).

Data in Transit

- Secure all data in transit if using removable storage devices (encryption required)
- Lock laptop in auto and make sure it is out of line of sight (e.g., in trunk or under seat)
- Use a lockable storage case when transporting paper records and case in locked auto out of line of sight.
- Never leave any device or file unattended at anytime (laptops, storage devices, files in attaché case or storage case).

Physical Security

- 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 confidential information should not be available to visitors without an escort.
- Prevent tailgating – do not allow others without proper security credentials to enter secure areas behind.
- Do not prop open external doors.