

## Division of Public Health

### Summary Guidelines for Safeguarding the Privacy of Health Information (DPH Privacy Safeguards Policy)

These are guidelines centered on how to safeguard health information and ensure confidentiality when using normal business communications, such as conversations, telephone, faxes, mail, and electronic mail. Wherever practical, the material containing individual identifiable health information (IIHI) should be labeled as confidential on the document, diskette, CD, or other medium. IIHI maintained electronically should be password-protected in all media.

Also when using and disclosing (IIHI), 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 IIHI. Remember to limit your communications of IIHI 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 IIHI communications, please discuss them with your supervisor.

If discrepancies occur among health information policies on securing information, the stricter standards shall apply.

#### **Oral Conversations – in person**

- Discuss patient/client IIHI in 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 patient/client health information.
- Point out health information on paper or on-screen non-verbally when discussing patient/client health 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 IIHI over the phone when talking to unknown callers, but call back and verify phone number.
- Never leave IIHI 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 IIHI 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 IIHI. *See attachment B.*
- Include on the cover sheet instructions for verifying fax receipt, where applicable.
- Do not include or reference IIHI 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 patient health 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**

- Do not include IIHI in Subject-line or in Body of email.
- Transmit IIHI only in a password-protected attachment (MS Word and MS Excel provide password protection). *See attachment A.*
- Include a confidentiality statement on emails that contain any IIHI in email attachments. *See attachment B.*
- Do not send attachment passwords in the same email as the attachment.
- 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 patient data.
- Do not store emails or email attachments with IIHI 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 IIHI in any medium (paper, CDs, diskettes).
- Use sealed secured envelopes to send IIHI.
- Verify that the authorized person has received the package.
- Deliver all mail promptly to the recipient.
- Mailboxes must be in safe areas and not located in public or high-traffic areas.
- Locked mailboxes should be used where ever possible.

#### **Inter-Office Mail**

- Put IIHI in closed inter-office envelopes. As an added precaution, put IIHI 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.
- Where practical, use lockable containers (e.g. attaches) to transmit correspondence that contains patient/client IIHI.

#### **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 patient/client IIHI visible or unsecured in a car, home office, or in any public areas.
- Ensure that all IIHI used outside work premises is protected using appropriate measures such as locked home offices, desks, file cabinets.
- Never remove original copies of IIHI from the agency without your supervisor's approval for specific purposes.
- Store files that contain IIHI on a secure LAN, not on your workstation hard drive.

#### **Disposal of IIHI**

- Shred all hard copies containing IIHI 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 IIHI from your computer and from the server when the information is no longer needed within the record retention requirements.
- Destroy all floppy disks, CDs, etc., that contained IIHI before disposing them.
- Do not reuse floppies, CDs that contained IIHI 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 IIHI to the sender, if this requirement is stipulated in any contractual agreements.

#### **Work Areas**

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



## ***Privacy Safeguards Attachment A: Emailing Protected Microsoft Office Documents (DPH Privacy Safeguards Policy)***

***Note: If you have questions about how to apply password protections, please contact your DPH IT.***

***Important: Do not send document passwords in the same email as the password-protected attachment.***

### Password Protection – Excel 97

- 1) Open the MS Excel file to be protected.
- 2) Select **File | Save As** from the Menu. The Save As dialog box displays.
- 3) Click the **Options** button.
- 4) Enter a password in the **Password to open** field. Use a password with a minimum of eight characters, preferably with a combination of numbers as well as upper case and lower case letters (passwords are case sensitive).

**Note:** The document can also be password protected for modification by entering a password in the **Password to modify** field.

- 5) Click **OK**.
- 6) Re-enter the password in the **Confirm Password** dialog box and click **OK**.
- 7) Save and close the document.

### Password Protection – Excel 2000

- 1) Open the MS Excel file to be protected.
- 2) Select **File | Save As** from the Menu. The Save As dialog box displays.
- 3) Select the **Tools** option
- 4) Select the **General Options** option
- 5) Enter a password in the **Password to open** field. Use a password with a minimum of eight characters, preferably with a combination of numbers as well as upper case and lower case letters (passwords are case sensitive).

**Note:** The document can also be password protected for modification by entering a password in the **Password to modify** field.

- 6) Click **OK**.
- 7) Re-enter the password in the **Confirm Password** dialog box and click **OK**.
- 8) Save and close the document.

### Password Protection – Word 97

- 9) Open the MS Word file to be protected.
- 10) Select **File | Save As** from the Menu. The Save As dialog box displays.
- 11) Click the **Options** button.
- 12) Select the **Save** tab in the Options dialog box.
- 13) Enter a password in the **Password to open** field. Use a password with a minimum of eight characters, preferably with a combination of numbers as well as upper case and lower case letters (passwords are case sensitive).

**Note:** The document can also be password protected for modification by entering a password in the **Password to modify** field.

- 14) Click **OK**.
- 15) Re-enter the password in the **Confirm Password** dialog box and click **OK**.
- 16) Save and close the document.

### Password Protection – Word 2000

- 1) Open the MS Word file to be protected.
- 2) Select **File | Save As** from the Menu. The Save As dialog box displays.
- 3) Select the **Tools** option
- 4) Select the **General Options** option
- 5) Enter a password in the **Password to open** field. Use a password with a minimum of eight characters, preferably with a combination of numbers as well as upper case and lower case letters (passwords are case sensitive).

**Note:** The document can also be password protected for modification by entering a password in the **Password to modify** field.

- 6) Click **OK**.
- 7) Re-enter the password in the **Confirm Password** dialog box and click **OK**.
- 8) Save and close the document.

### Emailing protected documents

- 1) 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.

***Important: Do not send document passwords in the same email as the password-protected attachment.***

- 2) Attach the file to the email and send to the recipient.

### Opening protected documents

- 1) Double click on the attachment to access as you normally would.
- 2) Select the option to either open or save the document.
- 3) If you select to open the document, enter the password when prompted.
- 4) If you select to save the document, enter where you want to save the document.
- 5) Enter the password when you open the document.



***Privacy Safeguards Attachment B: Confidentiality Statement for Fax and Email with IIHI (DPH Privacy Safeguards Policy)***

- Include the following statement on your facsimile cover sheets for fax transmission that contain Individually Identifiable Health Information (IIHI). Do not include it on faxes that do not contain IIHI.
- Include the following statement in any emails that contain Individually Identifiable Health Information in password protected attachments. Remember: Do not include IIHI in the body or subject of the email and do not transmit the attachment password with the email. DO NOT INCLUDE this statement on emails that do not contain IIHI.

.....

The documents accompanying this (facsimile) (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 entity or individual 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.

.....