



## 4 Policy for Handling and Safeguarding of Protected Health Information (PHI)

Under section 13402 of the HITECH Rule for standards and guidance on encryption, WinZip and ZixMail have both been approved by the National Institute of Standards and Technology (NIST) as two forms of encryption to use when e-mailing electronic data. HP Enterprise Services uses ZixMail to encrypt the content and prevent unauthorized access to PHI data transmitted by e-mail.

Only HP Enterprise Services staff members, as well as contractors employed on the Georgia Title XIX account with a need to know, have access to PHI data. Employees use various procedures to prevent access to others without that need to know. These procedures include access control to personal computers (PCs), securing paper documents, and access to sensitive areas of the account.

### 4.1 Verbal Conversations

When discussing and sharing information with others, be sure that they are entitled to it. For example, it would not be appropriate to share details about a member's medical history with a neighbor or friend.

Make wise decisions about how much information is relevant when discussing information at work. For example, staff in the Prior Authorization team may have received pictures of a member's wound or injury in order to validate the need for a procedure, but those pictures would not be necessary to share or discuss if Provider Services was asking about the member's other request for a hearing aid.

When discussing information with outside parties, such as a provider, member or authorized member representative, or a vendor, validate their identity to a reasonable degree, such as by having them give their provider number and address or the billed amount on a particular claim. The provider is verified by their provider ID. If you question the veracity of the information the individual has provided, request their name and number and let them know that you will call them back. Before returning the call, report the incident to your leader to determine the next steps.

### 4.2 E-Mail

1. Encrypt all e-mail containing PHI—When e-mailing PHI, it is critical to encrypt the content of the e-mail. ZixMail should be used when e-mailing information to HP Enterprise Services team members, DCH, providers, or any others authorized to receive PHI.

If ZixMail is temporarily not an option, place the information in a WinZip file and password-protect it (which also encrypts it). Communicate the password verbally, not through e-mail. Below are instructions for how to password-protect a WinZip file:

To place a file into a WinZip file:

- a. Click Start > Programs > WinZip from the desktop.
- b. Click the New button.



- c. Navigate where you want to save the new archive. HP Enterprise Services recommends your network home F: drive.
- d. Type the name of the file.
- e. Click the OK button.
- f. Navigate to the files to zip.
- g. Select one file at a time.
- h. Click the Add button and the file lists in the WinZip window.
- i. Click the Add button on the WinZip window to select another file. Repeat to include all necessary files.
- j. Click the Encrypt button from the WinZip window.
- k. Click the OK button in the WinZip Caution dialog box.
- l. Type a password in the text box, and retype the password in the verification text box.
- m. Click the OK button.

The files in the WinZip window display an asterisk next to them indicating that they're encrypted. You can now close the WinZip file and attach it to the e-mail you are preparing. Be sure to communicate the password to the person to whom you're sending it, but do so by verbal means and not through e-mail.

2. **No PHI in Subject Line**—Do not include PHI or sensitive information, such as an MID or member, in the subject line of an e-mail; even when the contents are encrypted, the subject line still comes through clearly.
3. **Confirm Addressees**—When e-mailing any sensitive information (to individuals inside or outside the account), always double-check the names to whom you are sending the information. It is much easier to handle an incorrect addressee before you send the e-mail.
4. **Do not use Home Computer or Personal E-mail**—Do not send or receive PHI using your home computer or personal e-mail address.
5. **E-mail only the Minimum Necessary Data**—Just like verbal conversations, make sure you're only e-mailing the minimum data necessary. If the e-mail trail began regarding a particular procedure, but now the real question is about this provider's bank account number, remove the procedure information since it is no longer necessary or applicable.
6. **Add Privacy Notice to all E-mails**—Be sure to incorporate the following text into the signature of your e-mail messages:



"This message and accompanying documents are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, and contain information intended for the specified individual(s) only. This information is confidential. If you are not the intended member or an agent responsible for delivering it to the intended member, you are hereby notified that you have received this document in error and that any review, dissemination, copying, or the taking of any action based on the contents of this information is strictly prohibited. If you have received this communication in error, please notify us immediately by e-mail, and delete the original message."

### 4.3 Faxing

1. **Confirm FAX Number and Receipt of FAX**—When faxing PHI, be sure to confirm the fax number to which you're sending, and give the other person a call that you're sending the fax. If it's the first time you're faxing to that number, follow up with your contact on the receiving end to be sure they received the fax successfully.
2. **Use a Cover Sheet**—Be sure to include a cover sheet, as it may help to cloak the start of the data on the receiving end (depending on the fax machine).
3. **Include Privacy Notice**—Ensure that the cover sheet includes the following text at the bottom:

"This message and accompanying documents are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521 and contain information intended for the specified individual(s) only. This information is confidential. If you are not the intended member or an agent responsible for delivering it to the intended member, you are hereby notified that you have received this document in error and that any review, dissemination, copying, or the taking of any action based on the contents of this information is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone (preferred) or returned fax, and shred the original message."

### 4.4 Printing

1. **Promptly Pick-Up Printed Documents Containing PHI**—Promptly pick up printed documents containing PHI from all printers. Documents should normally not be left sitting on the printer for longer than 30 minutes. The printers should be checked at the end of each day by a department staff member and any documents left on the printer should either be delivered to the individual who printed them or properly disposed of in a recycle bin.
2. **Only print what you need**—If you only need one page from a 10-page report, only print the one page.
3. **Confirm the Printer you Are Using**—Be sure you know to which printer you sent the document to. If you travel between offices, it is easy to mistakenly print to the wrong location and then forget to pick up the print-out.