Privacy and Security of Protected Health Information

Background

The Health Insurance Portability & Accountability Act (HIPAA) requires, among other things, that health plans and health care providers maintain the privacy and security of "individually identifiable health information." This includes information about a person's past, present or future physical or mental health, the provision of health care, or the payment for health care. It identifies the individual, or provides a reasonable basis that could identify the individual.

Under HIPAA, this information becomes "protected" when a covered entity transmits or maintains the information by electronic media, or in any other form or medium such as paper or spoken word.

Health plans under HIPAA include hospital, medical, prescription drug, dental, and vision care plans.

Staff members who work in Personnel offices and/or administer Research Foundation health insurance plans may have access to Protected Health Information (PHI), and therefore must take special care to maintain its privacy and security.

Situations In Which Protected Health Information (PHI) Must Be Protected

The following are examples of ways in which PHI may be transferred or maintained as part of health plan administration. Care must be taken to protect the privacy and security of an individual's health information in all of these situations:

- Health care claims
- Medical records
- E-mail and fax transmissions
- Computer screens
- Phone messages
- Letters and memos
- Conversations

  Since claims are normally filed by patients or providers directly with the health plans, it should be unusual for Research Foundation staff to have access to PHI in connection with health plan administration. If and when this does occur (e.g., when a claimant asks for assistance in settling a claim with a health plan), the staff member assisting should ask the patient to complete an Authorization for Health Care/Health Insurance Advocacy form. This form should then be kept on file.

Privacy and Security of Written Health Information

The following guidelines should be followed to ensure the privacy and security of written health information:

Health care claims

Obtain written authorization from the patient before you discuss PHI with the claims administrator. See Authorization for Health Care/Health Insurance Advocacy form.

Health information on paper

Maintain in locked file drawer, separate from other employment records.

PHI in e-mail and e-files

Maintain on secure drives that others can't access. Don't include health information in e-mail unless encryption is used. Delete PHI from forwarded e-mail. If encryption is not available, include the following confidentiality statement at the top of the e-mail:

Privacy & Confidentiality of Information Notice: This communication may contain non-public, confidential, or legally privileged information intended for the sole use of the designated recipients.

If you are not the intended recipient, or have received this communication in error, please notify the sender immediately by reply email at _____ or by telephone at _____, and delete all copies of this communication, including attachments, without reading them or saving them to disk.

If you are the intended recipient, you must secure the contents in accordance with all applicable state or federal requirements related to the privacy and confidentiality of information, including the HIPAA Privacy guidelines.

PHI on computer screens

Make sure screen is not visible to those passing by.

PHI in faxes

Include the following confidentiality statement on the fax cover sheet. Use private fax machine if possible, or stand by for immediate pick-up if fax machine is used by others:

Privacy & Confidentiality of Information Notice: This communication may contain non-public, confidential, or legally privileged information intended for the sole use of the designated recipients.

If you are not the intended recipient, or have received this communication in error, please notify the sender immediately by reply email at _____ or by telephone at _____, and destroy all copies of this communication, including attachments, without reading.

If you are the intended recipient, you must secure the contents in accordance with all applicable state or federal requirements related to the privacy and confidentiality of information, including the HIPAA Privacy guidelines.

If it is necessary to transmit PHI (for any reason) to the central office, Benefits Unit, there is a separate fax machine set up for this purpose. The HIPAA fax number is: (518) 434-8498.

Documenting Disclosures of PHI

Whenever an individual's PHI is disclosed outside of the office that administers the health, prescription, dental, or vision plan, the disclosure should be documented in the file. Documentation should include what was disclosed, when, for what reason, and to whom.

Disposing of Protected Health Information (PHI)

When the need for having an individual's PHI has passed, the paper records should either be returned to the individual or shredded (their choice). Electronic records should be deleted. The disposition of the PHI should be noted in the file.

Privacy and Security of Spoken Health Information

The following guidelines should be followed to ensure the privacy and security of spoken health information:

- "Need to know" basis – Discuss only the minimal information needed for health plan administration.

- Speak quietly, in a private place if possible – Be careful that conversations are not overheard by others.
- Don't take it out of the office – PHI must not be shared with anyone who doesn't require it specifically for health plan administration. That includes the employer, employees who don't need to know it, or family members.

  Let your supervisor know if you overhear any PHI – If you overhear someone else discussing PHI, let your supervisor know so that improvements can be made in the privacy practices of the workplace.

Employer vs Health Plan Administration

There must be a separation or "firewall" between employer functions and PHI within health plan administration. The employer has no right to know about PHI that is used for health plan administration, or to use such information to make employment decisions. The employer may, however, continue to have access to health information that is needed to administer FMLA, Workers' Comp, Disability, or ADA rules.

This means that PHI used for health plan administration must be kept separate from FMLA, Workers' Compensation, Disability, and Americans with Disabilities Act (ADA) records. See the document titled "Personnel Files" under Sponsored Program Mgt: Personnel Administration, Record Administration.

Individuals Rights Concerning Their PHI

Employees and dependents covered by a health plan have rights concerning access to, restrictions on, and complaints about handling of their PHI. They are informed of these rights in the Notice of Privacy Practices. These rights are described in the form "Request for Special Handling of Protected Health Information," which is in EPSS under Employees: Benefits and Retirement, Forms. An individual wishing to invoke one or more of these rights should complete and submit the form to the health plan administrator at the operating location. If help is needed in meeting the request, please contact central office.

Change History

- **March 31, 2003** - New document.
- **April 30, 2003** - Revised to add fax number for transmitting PHI to central office.

Feedback

Was this document clear and easy to follow? Please send your feedback to webfeedback@rfsuny.org.