	The Johns Hopkins Health System	<i>Policy Number</i>	SYS032
	PFS Policies and Procedures Manual	<i>Effective Date</i>	01/09/2006
	<i>Subject</i>	<i>Page</i>	1 of 2
	HIPAA Security – E-PHI	<i>Revised</i>	

PROCEDURE

This procedure applies to the Johns Hopkins Health System (JHHS) Patient Financial Services (PFS) Division servicing Johns Hopkins Hospital, Johns Hopkins Bayview Medical Center, and Howard County General Hospital.

PURPOSE

The purpose of this procedure is to protect PHI sent through electronic communications.

POLICY REFERENCE

Technical Security Policy C.4.1, Part E – Transmission Security
HIPAA Office Guidance: <http://www.insidehopkinsmedicine.org/hipaa/guidance.cfm>

PROCEDURES


E-PHI and E-Mail

Because e-mail is such a common and useful form of communication, Johns Hopkins has not invoked a blanket prohibition on the Internet e-mail of PHI. Judgment must be exercised in all instances when deciding whether to send PHI by unencrypted e-mail. Note that sending e-mail on Johns Hopkins e-mail systems such as GroupWise is not totally secure since links can and have been made by many system users that may take a given transmission outside of that system. Common sense steps should be taken:

- verifying the correct e-mail address each time used;
- if the address is pulled from a directory, double checking to make sure the correct person's address is inserted, particularly with fairly common names;
- obtaining some type of approval from the recipient of the communication to send the information electronically;
- including the warning and disclaimer required by the Johns Hopkins HIPAA policies;
- sending only the minimum amount of PHI necessary to achieve the purposes of the communication;
- Use password protection and if practical use encryption of E-PHI in an attachment by using a product like WinZip 9.0 (with AES).

Internal Communications

- Use the patient's account number and initials and not the patient's name whenever possible.

	The Johns Hopkins Health System	<i>Policy Number</i>	SYS032
	PFS Policies and Procedures Manual	<i>Effective Date</i>	01/09/2006
	<i>Subject</i>	<i>Page</i>	2 of 2
	HIPAA Security – E-PHI	<i>Revised</i>	

External Communications to Payors

- Never use the patient’s social security number
- Try not to use the patient’s medical record number
- Use the patient’s insurance member number
- Use the patient’s account number
- At the minimum, password protect any attached file

Johns Hopkins policy prohibits any transmission (including e-mail) across the Internet unless sent in encryption form for large amounts of PHI, or ongoing feeds of PHI to a known recipient. Such transmissions are significant security risks, and it is almost always possible to use a more secure means (e.g., SSL, secure FTP, etc.).

Note: Passwords should never be included in the body of an email message.

E-Mail Warning and Disclaimer should be attached to all e-mails containing E-PHI. The message below should be added to your signature in GroupWise.

WARNING: E-mail sent over the Internet is not secure. Information sent by e-mail may not remain confidential.

DISCLAIMER: This e-mail is intended only for the individual to whom it is addressed. It may be used only in accordance with applicable laws. If you received this e-mail by mistake, notify the sender and destroy the e-mail.

SPONSOR

Senior Director, Patient Financial Services, JHHS

REVIEW CYCLE

Three (3) years

APPROVAL

Senior Director of PFS, JHHS

Date