

## Release of Anatomic Pathology Medical Records

**KEY WORDS:** medical records, HIPAA, PHI

### DEFINITIONS:

Pathology Medical Records	may include, but are not limited to: written or electronic media that document the health care experience of a patient at The Johns Hopkins Hospital, slide/s, embedded block/s of tissue, photograph/s, photomicrograph/s, etc.
HIPAA	The Health Insurance Portability and Accountability Act of 1996
PHI	Protected health information, i.e. individually identifiable health information

### POLICY

It is the policy of The Johns Hopkins Hospital, Department of Pathology, to provide authorized individuals with copies of their Pathology Medical Records. Refer to the ICPM Policy No PME001, The Medical Record.

All original Medical Records and/or specimens are the property of The Johns Hopkins Hospital and shall be maintained to serve the patient, health care providers and the institution in accordance with HIPAA, legal, accrediting and regulatory agency requirements.

All diagnostic materials must be organized in a retrievable manner and stored to prevent damage and ensure diagnostic value. Stained slides must be retained for 10 years and specimen blocks for 10 years from the examination date.

When copies or duplicate material are not available or are available as the only original record, the original record will not leave the possession of The Johns Hopkins Hospital, Department of Pathology\*. The unique medical records are available for review, on site, by appointment, in the Department of Pathology Medical Records Office, Monday - Friday 8:30 am - 4pm.

\*Exception: An outside physician or Medical Facility may request original Medical Records on a patient, for whom duplicate material is not available. If re-examination of these records is required for patient care, the appropriate Division Director may approve the request with the following provisions: adherence to a strict Chain of Custody; original material is sent by courier to the requesting physician; any original medical record must be returned to JHH within 5 working days, unless other arrangements have been made.

Only authorized Anatomic Pathology Medical Records Archival Office staff may release Department of Pathology Medical Records.

### Release of Medical Information

Faculty or staff receiving a subpoena for medical records should send the subpoena to:

Pathology Consult Office  
Reed Hall 315  
Attn: Medical Legal

The Department of Pathology is required to honor a Maryland State Subpoena or a Federal Courts Subpoena within a 100 mile radius of Baltimore. If the Department of Pathology receives an out of state subpoena, the Custodian of Pathology Medical Records must notify the party that they are

required to obtain a Maryland State Subpoena. The subpoena is faxed to the HIPAA law office for approval before any action is taken.

The medical legal clerk is responsible for securing all subpoenaed records, will work with the individual and legal office to insure proper procedures are followed and documented.

**For uses and disclosures of the medical record for treatment, payment and healthcare operations purposes (see ICPM PME001).**

**Automatic Faxing of Patient Reports**

It is the policy of the Johns Hopkins Hospital, Department of Pathology, Divisions of Anatomic Pathology to provide the authorized individuals with faxed copies of their Pathology Medical Report.

All Medical Records and/or specimens are the property of The Johns Hopkins Hospital and shall be maintained to serve the patient, health care providers and the institution in accordance with accrediting and regulatory agency requirements.

Upon a request for a faxed copy of a Medical Record:

See JHML Policy, faxed Documents Containing Patient Data.

**Reporting of Patient Results via Email**

**E-PHI and E-mail** This guideline may be found: <http://www.insidehopkinsmedicine.org/hipaa/guideemail.cfm>

Questions continue to be raised, both at Johns Hopkins and elsewhere, about sending PHI electronically, particularly by e-mail. There is no easy, practical, clear cut answer. Neither the HIPAA Security Rule, nor the HIPAA Privacy Rule, provides clear guidance. The strategies and practices of other institutions are all over the map. E-mail presents some serious security issues, including among others:

- misaddressed/misdirected messages
- e-mail accounts that are shared with others
- messages forwarded by patients to others
- possible interception of clear text messages
- inboxes (either the clinician's or the patients) locally storing sent or received messages (often as insecure portable devices)

The "safe" answer is that PHI may not be sent by unencrypted inter-net e-mail. However, the speed and accessibility of electronic communications makes its use a current day necessity. There is no turning back the tide.

The issue of sending PHI electronically is that of security. Under both the general standards for electronic security, as well as the HIPAA security regulations, fundamental guiding concepts are those of risk analysis (i.e., identifying risks and vulnerabilities) and risk management (i.e., reducing risks and vulnerabilities to a reasonable and appropriate level in light of the risks involved). Stated differently, a balance must be struck between making information available and the risk of data loss, misdirection or theft.

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;
- if possible; encrypting E-PHI in an attachment using a product like Winzip 9.0 (with AES).

Even with these precautions we strongly discourage **starting** an e-mail communication with a patient or another party that is likely to include E-PHI at some point.

However, whenever

1. large amounts of PHI are involved, or
2. on-going feeds of PHI are involved

Johns Hopkins policy prohibits any transmission (including e-mail) across the Internet unless sent in encrypted form and 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.).

With all the security baggage that e-mail carries, users should consider whether it would be better to use alternate means.

Revised 10/5/05