Patient Requests for Lab Reports

As of October 6, 2014, HIPAA covered entities must comply with changes to the HIPAA and CLIA laws, 45 CFR Part 164, CLIA Program and HIPAA Privacy Rule; Patients’ Access to Test Reports; requiring certain laboratories to provide access to protected health information upon request by individuals who are the subject of this information or to their legal representatives.

This final rule amends the Clinical Laboratory Improvement Amendments 1988 (CLIA) regulations to specify that, upon the request of a patient (or the patient’s personal representative), laboratories subject to CLIA may provide the patient, the patient’s personal representative, or a person designated by the patient, as applicable, with copies of completed test reports that, using the laboratory’s authentication process, can be identified as belonging to that patient.

Subject to conforming amendments, the final rule retains the existing provisions that require release of test reports only to authorized persons and, if applicable, to the persons responsible for using the test reports and to the laboratory that initially requested the test. In addition, this final rule amends the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to provide individuals (or their personal representatives) with the right to access test reports directly from laboratories subject to HIPAA (and to direct that copies of those test reports be transmitted to persons or entities designated by the individual) by removing the exceptions for CLIA certified laboratories and CLIA-exempt laboratories from the provision that provides individuals with the right of access to their protected health information. These changes to the CLIA regulations and the HIPAA Privacy Rule provide individuals with a greater ability to access their health information, empowering them to take a more active role in managing their health and health care.

A number of states have laws that prohibit a laboratory from releasing a test report directly to the individual or that prohibit the release without the ordering provider’s consent. Upon the effective date of this final rule, the Privacy Rule preempts these laws and HIPAA covered laboratories should begin to come into compliance.

With respect to those commenters requesting clarification on HIPAA preemption, we note that HIPAA preempts only state laws that are contrary to the Privacy Rule. ‘Contrary’ generally means a covered entity would find it impossible to comply with both the state and HIPAA requirements. Further, we clarify that this final rule applies only to laboratories. State laws that place requirements on other types of health care providers, such as those requiring a provider to discuss with and counsel a patient on HIV test results are not preempted by this final rule.

Procedures are currently under review at Purdue to identify the necessary modifications to be made, in order to come into compliance by the October compliance date.

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: http://www.purdue.edu/hipaa

or contact: Joan Vaughan, HIPAA Privacy Officer

telephone: (765) 496-1927
e-mail: jvaughan@purdue.edu
A security flaw affecting most versions of Microsoft Internet Explorer has been resolved, and Purdue security experts say faculty, staff and students may resume using the Web browser.

The flaw, which could have allowed an attacker to run remote code on an individual’s computer, was a risk if someone visited a site where malicious code was present. For those using Internet Explorer to access Purdue sites such as University Web pages, the SAP employee portal or Blackboard Learn, there was no concern.

Still, Purdue’s interim chief information security officer, Greg Hedrick, recommended individuals avoid using Internet Explorer to access all sites external to Purdue until the issue was corrected. That’s because legitimate websites often use advertisement distribution networks to manage ads, which have been known to distribute malware and take advantage of browser weaknesses.

Although no problems were reported as a result of the vulnerability, ITAP’s Security and Policy unit reminds individuals to exercise caution when clicking on links and reviewing emails.

Additionally, Microsoft encourages customers to review and follow the guidance in the Microsoft Safety & Security Center (https://www.microsoft.com/security/pc-security/protect-pc.aspx) for enabling a firewall, applying software updates and installing anti-malware software.

What to do if you receive a phishing email: When you see suspicious email in your Purdue inbox, report it to abuse@purdue.edu and to is-spam@purdue.edu with the original email attached to preserve its header information. Doing so helps Purdue’s security team review the message and advise if it is legitimate. The security team also can take measures to block fraudulent websites, while the messaging team can blacklist fraudulent email accounts.

To attach an email in Windows using Outlook with Purdue’s Exchange service, create a new message and choose “Attach Item” from the dropdown list on the message menu bar. Then select “Outlook item,” and attach the email in question. On a Mac, right click or control click on the suspicious message and choose “Forward Special” and “As Attachment” from the dropdown list.

(Continued left-FAQ’s from OCR)

Security Series 3: Security Standards – Physical Safeguards. In addition, for practical information on how to handle sanitization of PHI throughout the information life cycle, readers may consult NIST SP 800-88, Guidelines for Media Sanitization.

Other methods of disposal also may be appropriate, depending on the circumstances. Covered entities are encouraged to consider the steps that other prudent health care and health information professionals are taking to protect patient privacy in connection with record disposal. In addition, if a covered entity is winding up a business, the covered entity may wish to consider giving patients the opportunity to pick up their records prior to any disposal by the covered entity (and note that many states may impose requirements on covered entities to retain and make available for a limited time, as appropriate, medical records after dissolution of a business).

Question: Provided by the Office for Civil Rights
What do the HIPAA Privacy and Security Rules require of covered entities when they dispose of protected health information?

Answer:

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. See 45 CFR 164.530(c). This means that covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the HIPAA Security Rule requires that covered entities implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use. See 45 CFR 164.310(d)(2)(i) and (ii). Failing to implement reasonable safeguards to protect PHI in connection with disposal could result in impermissible disclosures of PHI.

Further, covered entities must ensure that their workforce members receive training on and follow the disposal policies and procedures of the covered entity, as necessary and appropriate for each workforce member. See 45 CFR 164.306(a)(4), 164.308(a)(5), and 164.530(b) and (i). Therefore, any workforce member involved in disposing of PHI, or who supervises others who dispose of PHI, must receive training on disposal. This includes any volunteers. See 45 CFR 160.103 (definition of “workforce”).

Thus, covered entities are not permitted to simply abandon PHI or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons. However, the Privacy and Security Rules do not require a particular disposal method. Covered entities must review their own circumstances to determine what steps are reasonable to safeguard PHI through disposal, and develop and implement policies and procedures to carry out those steps. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the form, type, and amount of PHI to be disposed. For instance, the disposal of certain types of PHI such as name, social security number, driver’s license number, debit or credit card number, diagnosis, treatment information, or other sensitive information may warrant more care due to the risk that inappropriate access to this information may result in identity theft, employment or other discrimination, or harm to an individual’s reputation.

In general, examples of proper disposal methods may include, but are not limited to:

- For PHI in paper records, shredding, burning, pulping, or pulverizing the records so that PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Maintaining labeled prescription bottles and other PHI in opaque bags in a secure area and using a disposal vendor as a business associate to pick up and shred or otherwise destroy the PHI.
- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more information on proper disposal of electronic PHI, see the HHS

(Continued left-FAQ’s from OCR)