HHS Strengthens Patients’ Right to Access Lab Test Reports

Provided by the Office for Civil Rights, 2/3/2014

As part of an ongoing effort to empower patients to be informed partners with their health care providers, the Department of Health and Human Services (HHS) has taken action to give patients or a person designated by the patient a means of direct access to the patient’s completed laboratory test reports.

The final rule announced today amends the Clinical Laboratory Improvement Amendments of 1988 (CLIA) regulations to allow laboratories to give a patient, or a person designated by the patient, his or her “personal representative,” access to the patient’s completed test reports on the patient’s or patient’s personal representative’s request. At the same time, the final rule eliminates the exception under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule to an individual’s right to access his or her protected health information when it is held by a CLIA-certified or CLIA-exempt laboratory. While patients can continue to get access to their laboratory test reports from their doctors, these changes give patients a new option to obtain their test reports directly from the laboratory while maintaining strong protections for patients’ privacy.

The final rule is issued jointly by three agencies within HHS: the Centers for Medicare & Medicaid Services (CMS), which is generally responsible for laboratory regulation under CLIA, the Centers for Disease Control and Prevention (CDC), which provides scientific and technical advice to CMS related to CLIA, and the Office for Civil Rights (OCR), which is responsible for enforcing the HIPAA Privacy Rule.

Under the HIPAA Privacy Rule, patients, patient’s designees and patient’s personal representatives can see or be given a copy of the patient’s protected health information, including an electronic copy, with limited exceptions. In doing so, the patient or the personal representative may have to put their request in writing and pay for the cost of copying, mailing, or electronic media on which the information is provided, such as a CD or flash drive. In most cases, copies must be given to the patient within 30 days of his or her request.

The final rule is available for review at: https://www.federalregister.gov/articles/2014/02/06/2014-02280/clia-program-and-hipaa-privacy-rule-patients-access-to-test-reports.

The rule change is effective April 7, 2014, to be implemented by October 6, 2014. Modifications to Purdue’s procedures to accommodate this change will be announced to the affected areas, in the near future.

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
Tips to Recognize Phishing Email

From SecurePurdue News

Purdue has recently been plagued with phishing emails. These were targeted to students at Purdue, something called spear phishing. Students were notified their certificate of authenticity would soon expire. They could easily fix the problem by sharing information to get everything updated.

Phishing emails have a pattern.

- They warn of dire consequences if you don’t do something immediately
- They ask for you to provide personal information back to them
- They may provide a link to a webpage where you can log in and fix whatever they say needs attention.
- They may offer something too good to be true. It IS too good to be true.

NEVER give private account information through email. Purdue will never send an email message asking users to reply with a password or other confidential personal information such as Social Security numbers or bank account numbers. Messages requesting such information are fraudulent and should be deleted.

Think before clicking on links in emails. Go to the source of the problem. If it is a bank email saying there is a problem, go to the bank website. If you have a voice mail stating a problem with your bank account, don’t call the number from the voice mail. Look at your credit card and call the number printed on the back of the card. Think before you act. If someone comes to your work environment, make sure they are who they say they are if you don’t know them personally.

For more information about data security at Purdue, access: http://www.purdue.edu/securepurdue.

FAQ’s from OCR

Provided by the Office for Civil Rights

Question:

Is a covered entity liable for, or required to monitor, the actions of its business associates?

Answer:

No. The HIPAA Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. Nor is the covered entity responsible or liable for the actions of its business associates. However, if a covered entity finds out about a material breach or violation of the contract by the business associate, it must take reasonable steps to cure the breach or end the violation, and, if unsuccessful, terminate the contract with the business associate. If termination is not feasible (e.g., where there are no other viable business alternatives for the covered entity), the covered entity must report the problem to the Department of Health and Human Services Office for Civil Rights. See 45 CFR 164.504(e)(1).

With respect to business associates, a covered entity is considered to be out of compliance with the Privacy Rule if it fails to take the steps described above. If a covered entity is out of compliance with the Privacy Rule because of its failure to take these steps, further disclosures of protected health information to the business associate are not permitted. In cases where a covered entity is also a business associate, the covered entity is considered to be out of compliance with the Privacy Rule if it violates the satisfactory assurances it provided as a business associate of another covered entity.

Question:

Does the HIPAA Privacy Rule permit a health care provider to disclose an injured or ill worker's protected health information without his or her authorization when requested for purposes of adjudicating the individual's workers' compensation claim?

Answer:

Covered entities are permitted to disclose protected health information for such purposes as authorized by, and to the extent necessary to comply with, workers’ compensation law. See 45 CFR 164.512(l). In addition, the Privacy Rule generally permits covered entities to disclose protected health information in the course of any judicial or administrative proceeding in response to a court order, subpoena, or other lawful process. See 45 CFR 164.512(e).