Who's Responsible When a Lab Has a Data Breach?

Surprisingly, in terms of informing patients, you are!

BY MICHAEL L. BRODY, DPM

Do you send patients for laboratory tests or send specimens to laboratories directly? Do you use either Labcorp or Quest? We have recently seen massive data breaches at both Quest and Labcorp. Many of us send patients or specimens to these labs; therefore these breaches require some special attention.

It may seem strange that two large laboratory companies experienced data breaches at the same time. Did a hacker target laboratories and hit both at the same time? What is the connection?

For Labcorp, 7.7 million patients had their information breached and Quest experienced a breach of almost 12 million patients. The common thread is the collection agency that Labcorp and Quest use. That company is the American Medical Collection Agency.

The Labcorp breach included patient demographic information and financial data but not laboratory results. The Quest breach included the same information and patients' social security numbers. These breaches raise some very interesting and potentially complex questions on how they might impact your office. We will start with some important information on the companies involved in this breach.

Both Labcorp and Quest are 'covered entities' in that they do not have a direct relationship with patients. Whenever there is a breach, the individual or organization that is ultimately responsible for it is the covered entity. According to the *HHS* website, a covered entity is one of the following:

- A healthcare provider (doctor, dentist, chiropractor, pharmacy, nursing home) who transmits information in an electronic form in connection with a transaction for which HHS has adopted a standard claims form. Both Quest and Labcorp are healthcare providers that submit electronic claims so they are covered entities.
- A health plan that receives the electronic files.
- The clearinghouses that sit between the healthcare provider and the health plan.

For Labcorp, 7.7 million patients had their information breached and Quest experienced a breach of almost 12 million patients.

The collection agency is a business associate of both Quest and Labcorp. According to the *HHS* website, a business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

So what do the breaches at Quest and Labcorp mean to you if you have sent patients or patient specimens to either Labcorp or Quest? You shared information with a 'covered entity'. Sharing this information is an allowed disclosure under the HIPAA regulations as you were sharing patient information with another medical provider who was involved in the care of the patient.

Since they are both 'covered entities', they then became directly responsible for the data that they held. Since they are directly subject to the HIPAA rules and regulations, you are not responsible for the security of the data that they received.

Under the HIPAA regulations, you are responsible to keep a log of every electronic disclosure of patient information, and patients are entitled to receive an accounting of disclosures of their data. A patient may ask you what you sent to Labcorp or Quest and you would be required to inform the patient what information was shared, when and why. This is your responsibility.

Patients may call you and ask if you use Quest or Labcorp and what you know about the breach. It is best if you answer if you have sent their information to the lab with a yes or no and then direct them to reach out to Quest and/or Labcorp for more information on the breach.

For Labcorp, direct them to the following webpage:

https://www.labcorp.com/

Continued on page 38

Data Breach *(from page 37)*

hipaa-privacy/hipaa-information

For Quest, direct them to the following web page:

https://www.questdiagnostics.com/home/privacy-policy/notice-privacy-practices.html

You will notice that both of these pages are the Notice of Privacy Practices for both Quest and Labcorp. Your practice is required to have your own Notice of Privacy Practices and it is a good idea to have that on your practice website; you need to have printed copies of this document in your office. If a patient asks for a copy of your Notice of Privacy Practices, you must provide it to the patient. Failure to provide the Notice of Privacy Practices is a HIPAA violation.

Labcorp and Quest are also required to notify all patients who were involved in the breach about it within 30 days of discovery of the breach, so your patient should have already received such a letter.

Even though the breach happened at the American Medical Collection Agency, it is Quest and Labcorp who are responsible for it. If a breach occurs at a business associate of yours, it is your practice that will be responsible for the breach.

Steps to take today to better protect your practice:

- Make sure that you have copies of your Notice of Privacy Practices available in your office.
- Have a copy of your Notice of Privacy Practices on your website.
- Make sure you have signed and dated Business Associate Agreements in place with all of your Business Associates.
- Make sure your cybersecurity policy has enough coverage to protect you in case of a breach—at least a one-million-dollar policy.
- Make sure your HIPAA Security Policy and HIPAA risk mitigation plans are up-to-date. They must be reviewed at least once a year and more often if circumstances dictate. If you have a breach and you do not have an up-to-date HIPAA security policy and HIPAA risk mitigation plan, you may be looking at very high fines should you or one of your business associates experience a breach. **PM**

Dr. Michael Brody has presented webinars for the e-Health initiative, (www.ehealthinitiative.org/) and is active in the EMR workgroup of the New York E Health Collaborative (www.nyehealth.org/). He has provided consulting services to physicians for the implementation of EHR software and to EHR vendors to assist in making their products more compatible with CCHIT and HIPAA guidelines. Dr. Brody is a member of AAPPM.