G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

August 2018

INSIDE THIS ISSUE

www.G2Intelligence.com

Upcoming Events

Lab Institute 2018

Surviving Disruption: Rethinking Business Models, Technologies, and Competitive Strategies in a Changing Lab Market

Oct. 24-26, Washington, DC
www.labinstitute.com

The 10 Policies You Need to Stop Lab Employee PHI Breaches

Safeguarding personal health information (PHI) data from hackers, identity thieves and other cyber threats isn't just a legal obligation but a business imperative. Yet, with so much on the line, breaches keep happening, even at large and sophisticated labs that invest millions in data security.

The Problem: Employees

Many PHI breaches can be traced back to employees. Whether deliberate or inadvertent, acts or omissions of a single employee can undermine an elaborate data security system.

The Solution: Technology + Policies

While technology is part of the solution, you must also have the right personnel policies to prevent breaches and keep precious PHI secure.

Continued on page 2

HIPAA Briefing: Can Patients Sue Labs for Privacy Breaches?

Violating HIPAA restrictions subjects your lab to fines and other penalties dished out by the HHS Office of Civil Rights (OCR) and other regulators. But can the individual victims whose personal health information you compromise also sue you for damages under the law? It's a question that the HIPAA law does not expressly address. But a new federal case targeting LabCorp sheds light on this crucial question.

Spoiler Alert

The court confirmed what previous courts have said before, namely, that patients have no private right of action under HIPAA systems.

The Situation

The case began when a LabCorp technician instructed a Washington, D.C., hospital patient to key her private medical infor-

Continued on page 10

The 10 Policies You Need to Stop Lab Employee PHI Breaches, *from page 1*

1. Computer Use Policy

Computer use policies should define proper use of lab computer and digital resources and specify acceptable and unacceptable uses of fixed, laptop and mobile computing devices and network resources.

2. Email Use Policy

Employee email mishaps are a leading cause of PHI breaches. So, you need a policy explaining the proper use of your lab's email systems addressing:

- Information emails and attachments can contain;
- Replying and forwarding of emails and attachments, e.g., banning automatic forwarding of emails containing PHI;
- Measures to keep emails and attachments secure; and
- Retention of emails containing PHI.

3. Social Media & Blogging Policy

You also need a policy making it clear that employee blogging and social media use is subject to your lab's data security restrictions even when it occurs within their own home after work. Key provisions:

- Ban on disclosure of PHI and other confidential information;
- Require employees to behave in a professional manner and refrain from conduct that may harm the reputation, image or goodwill of the lab, its employees, patients or clients;
- Ban on discrimination and harassment;
- Ban on employees speaking on behalf of the lab without authorization.

Employee Computer, Email & Social Media Use IS Your Business

Be sure to specify in your computer use, email and social media use policy that the lab has the right to monitor employee compliance and that employees should have no expectation of privacy in how they use their work computers and email systems.

4. Clean Desk Policy

The purpose of this policy is to warn employees against carelessly leaving PHI out in the open and explain what they must do to secure PHI in their work area when they go home at night or leave their workstation for an extended period, including verifying that:

- Computers are shut down and secured;
- Hardcopy documents are removed and locked in secure files or drawers;
- Drawers and file cabinets are locked and the key isn't left unattended;
- Whiteboards are erased;
- Printers and fax machines are cleared of papers as soon as printing is done.

G2CA

Glenn S. Demby, Editor

Lori Solomon, Contributing Editor

Catherine Jones, Contributing Editor and Social Media Manager

Barbara Manning Grimm, Managing Editor

David van der Gulik, Designer

Randy Cochran, Corporate Licensing Manager

Myra Langsam, Business Development

Michael Sherman, Director of Marketing

Jim Pearmain, General Manager

Pete Stowe, Managing Partner

Mark T. Ziebarth, Publisher

G2 Compliance Advisor (ISSN 2332-1474) is published by G2 Intelligence, Plain Language Media, LLLP, 15 Shaw Street, New London, CT, 06320.
Phone: 888-729-2315
Fax: 855-649-1623
Web site: www.G2Intelligence.com.

Inadequate password protection by employees is a major weak spot in data security systems.

5. Workstation Security Policy

It takes more than physical barriers and technical safeguards like encryption to achieve workstation security. You also need a policy listing the measures employees must take to keep their workstations secure, such as:

- Allowing only authorized personnel into their workstations;
- Making sure workstations are locked when they're away;
- Logging off and securing their computers before leaving at night;
- Complying with password restrictions;
- Not installing unauthorized software;
- Not using personal devices or systems to store PHI.

6. Password Creation & Protection Policy

Inadequate password protection by employees is a major weak spot in data security systems. To address the problem, you need a policy requiring employees to create strong passwords that lists guidelines, including:

- Standards passwords must meet, e.g., at least 12 alphanumeric characters in length;
- Things to put in passwords, e.g., upper and lower case letters and characters like *&^%#;
- Things not to put in passwords, e.g., birthdates, names and other personal information.

There should also be a clear process for changing passwords and a policy requiring employees to keep their passwords secure that lists common mistakes to avoid, such as:

- Writing passwords on post-its or note pads and compounding the error by leaving the post-it out in the open or even under the desk or another obvious hiding spot;
- Sharing passwords with others;
- Including passwords in emails or disclosing them on the phone;
- Using the same password for multiple accounts.

7. Data Removal Policy

Many data breaches are the result not of hacking or deliberate cyberattack but lost and stolen laptops. So, you need a policy restricting employee removal of PHI, including:

- A requirement that removals be authorized;
- A clear process for granting such authorization;
- Limitations on what data can be removed; and
- Mandatory safeguards for protecting removed data.

8. Bring Your Own Device (BYOD) Policy

In an era of mobile computing, you should have a BYOD policy addressing:

- Whether employees can bring personal electronic devices to work for work-related uses;
- Which devices are approved for BYOD;
- Which uses are acceptable;
- Restrictions on uses, e.g., banning use of personal devices to download lab files containing PHI;
- Measures employees must take to keep their devices secure, e.g., use of passwords or encryption.

9. Remote Access Policy

While letting employees connect to your lab's network from remote locations boosts productivity, it can also compromise network security. So, you need a remote access policy explaining the requirements for connecting to the network from an external network or host, including:

- Who will have remote access privileges;
- Acceptable and prohibited uses for remote access;
- Required measures remote users must take to ensure the connection is at least as secure as the user's on-site connection; and
- Standards for connecting Bluetooth-enabled devices to the network or lab-owned devices.

10. Data Breach Response Policy

While prevention is the paramount objective, labs must also be prepared to respond effectively to any data breaches that occur. The key is finding out about the breach as swiftly as possible. And because employees are usually the first to know, they should be required to notify their supervisors immediately of any breaches they know about or suspect.

Labs IN COURT

A roundup of recent cases and enforcement actions involving the diagnostics industry

Ex-CEO of HDL Settles Bankruptcy Claims for $10 Million

Case: Health Diagnostic Laboratory co-founder and former CEO Tonya Mallory has agreed to pay $10 million to settle claims brought by the bankruptcy trustee in charge of liquidating HDL's assets. The case against Mallory is part of the trustee's larger $600 million suit targeting more than 100 HDL executives, directors, contractors and other defendants associated with the testing firm driven to bankruptcy by a massive kickback scheme involving bribes to physicians in exchange for orders of blood tests.

Significance: The newly approved bankruptcy settlement, which also covers her husband and former HDL shareholder, Scott, is far from the end of Ms. Mallory's legal problems. Last May, a federal court in South Carolina ordered Mallory and two principles of HDL's former contract sales organization, BlueWave Healthcare Consultants, to shell out $114.1 million after a jury found the three defendants liable for Medicare fraud for their part in the HDL scam. (See *GCA*, June 21, 2018, Case of the Month.) The defendants are appealing the verdict.

Former Patients Join the Legal Posse on the Trail of Theranos

Case: Nine ex-patients filed a class-action lawsuit against Theranos and its erstwhile retail partner Walgreens seeking damages for the harms they allegedly suffered as a result of inaccurate tests performed using Theranos diagnostic technology. The Arizona federal court dismissed seven of the claims but allowed the remaining 13 to proceed in a class action, which is currently in the evidence discovery phase.

Significance: Up to now, the Theranos case has been mostly about money and the financial losses suffered by consumers, investors and business associates as a result of the firm's overhyped bloodless finger prick technology. But the patient class action is a poignant reminder of the human and patient safety dimensions of the story. The alleged victims' accounts set out in the court papers document harrowing tales of mental suffering and unnecessary testing and treatment as a result of false positives for disorders like the autoimmune disease, Sjörgen's syndrome and the thyroid condition known as Hashimoto's disease, not to mention the patient removed from blood thinner medication warfarin on the base of flawed Theranos test results. At its peak, Theranos operated 40 consumer test centers within Walgreen's in the metro Phoenix area, performing over 1.5 million blood tests for nearly 176,000 consumers.

Florida Lab Pays $100K to Settle Claims of Violating Bioterrorism Law

Case: The OIG claimed that a Florida lab violated Federal Select Agent regulations by transferring a select toxin to an entity not registered to possess, use or transfer it and failing to get Centers for Disease Control and Prevention (CDCP) for the transfer. Rather than chance an administrative proceeding, the lab has decided to settle the case for $100,000.

Significance: Jointly comprised of the CDCP/Division of Select Agents and Toxins and the Animal and Plant Health Inspection Service/Agriculture Select Agent Services, the Federal Select Agent Program regulates possession, use and transfer of biological select agents and toxins that pose a threat to public, animal or plant health and products established in the aftermath of the 9/11 terrorist attacks to head off threats of bioterrorism.

Cancer Center Hit with $4.3 Million HIPAA Fine for Failure to Encrypt

Case: The University of Texas MD Anderson Cancer Center was on the wrong end of the fourth largest HIPAA fine ever dished out by the HHS Office University of Civil Rights for a trio of incidents between 2012 and 2013:

- An employee's laptop was stolen;
- A trainee lost a thumb drive; and
- A visiting researcher lost another thumb drive.

Result: Personal data of 33,800 patients was compromised.

Significance: Theft and loss of devices containing patient data is an all too common occurrence. What made this case different and egregious enough to warrant a massive HIPAA fine was that Anderson failed to encrypt the data. MD Anderson implemented an encryption policy in 2006 but didn't begin actual encryption of PHI on its computers until 2011, an effort that took over two years to complete. It argued that since the data was used for research purposes, HIPAA requirements didn't apply. But the HHS administrative law judge disagreed finding the Texas hospital's "dilatory conduct shocking given the high risk to patients resulting from the unauthorized disclosure" of digital PHI. MD Anderson says it plans to appeal the ruling contending that there's no evidence that any unauthorized party actually viewed the PHI.

Whistleblower Sues Montana Health System Officials for Elaborate Kickback Scheme

Case: The CFO of a Montana hospital physician network filed a *qui tam* lawsuit against his employer for paying physicians above-market compensation in exchange for referrals to network labs, hospitals, clinics and specialists.

Significance: The network, the biggest in Montana, denies the charges and contends that the Work Relative Value Units (WRVU) system it uses to measure physician productivity is the same method commonly employed by other hospitals across the country. But the CFO contends that the WRVU system is just a smoke screen to conceal payments based on referrals rather than productivity, citing among other examples, a neurosurgeon paid $900K per year even though collections for his services ranged from $207K to $374K, which is roughly the 10th percentile for neurosurgeons in national productivity metrics.

Genetic Test Labs Face Growing Risk of Medical Malpractice Liability

Compliance managers of lab involved in the $3 billion consumer-based genetic testing business need to safeguard their flank against a growing legal risk: the threat of liability for malpractice. As genetic testing has prospered in the past decade, it was all but inevitable that patients and trial attorneys would begin seeking to hold labs and doctors legally responsible for faulty DNA test results. The latest test case comes from South Carolina and involves one of the nation's largest labs, Quest Diagnostics.

What Happened

Amy Williams was a sympathetic plaintiff with a highly compelling story. In 2005, the Myrtle Beach mom's 2-year-old son Christian began experiencing regular seizures. Suspecting a mutation in the SCN1A gene, doctors sent Christian's DNA for genetic testing to Athena Diagnostics (which Quest Diagnostics would later acquire in 2016). The report found a glitch in the gene but described it as a "variant of unknown significance" that, according to Athena's classification "often has no effect" on normal gene activity. What Christian really had, according to Ms. Williams' attorneys, was a rare condition called Dravet syndrome.

Athena could have and should have detected that Christian had Dravet, the complaint alleged; instead, the lab's report led doctors to rule out Dravet and treat him with sodium-channel-blocking medications, which worsened his condition and intensified his seizures. A proper diagnosis would have prevented the fatal seizure Christian suffered on Jan. 5, 2008, according to the complaint.

The Plaintiff's Legal Conundrum

After initially blaming herself for Christian's death, Ms. Williams finally decided to sue Athena and its now parent company Quest (which for simplicity's sake, we'll refer to collectively as "Quest"). *The problem:* In South Carolina, the statute of limitations for medical malpractice is six years. However, the statute of limitations for negligence and wrongful death is three years from the date the plaintiff discovers he/she has a cause of action. Ms. Williams contended that she didn't discover that she had a legal case against Quest and thus still had time to file her suit as a wrongful death action.

Not so fast, countered Quest, who claimed the case was essentially wrongful death based on medical malpractice and thus subject to the hard six-year cap. *The key question:* Was Quest was acting as a licensed healthcare provider when it performed genetic testing on Christian? If so, the six-year medical malpractice statute of limitations would apply.

The Ruling

On June 27, 2018, the South Carolina Supreme Court ruled 4 to 1 in favor of Quest. "A genetic testing laboratory that performs genetic testing to detect

'Wrongful Birth' Litigation Scorecard

Malpractice lawsuits against labs and providers for failing to provide accurate DNA testing information during pregnancy

Florida: Plaintiff Wins $21 Million Malpractice Award (July 2007)
Parents sue Univ. of South Florida doctor for failing to diagnose their son's genetic disorder (called Smith-Lemli-Optiz syndrome) impairing his ability to synthesize cholesterol, leading couple to have a second child with same disorder. **Ruling:** Jury finds malpractice and awards couple $21 million but state law caps damages at $200K.

Virginia: LabCorp Can Be Sued for Malpractice (November 2011)
Parents who are both "carriers only" of thalassemia beta decide to continue their pregnancy after genetic testing confirms that their unborn fetus is also "carrier only." But when the results turn out to be wrong and the child has the more serious "affected person" version of the disorder, they sue LabCorp for "wrongful birth" malpractice. Ruling: The federal court refuses to dismiss the case but also finds that LabCorp is a "health care provider" and thus covered by the medical malpractice damages caps under state law.

Montana: Giving Pregnant Mom Pamphlet Defeats Claim of Negligently Failing to Provide Screening Test Info (February 2016)
After giving birth to a daughter with cystic fibrosis, a mother sues her doctor and prenatal care nurse for $14 million for not providing her any information on the availability of cystic fibrosis carrier screening testing. Ruling: The jury doesn't buy it and finds the defendants did meet the standard of care in delivering prenatal treatment, including giving the patient a cystic fibrosis pamphlet during her first appointment that she never bothered to read.

an existing disease or disorder at the request of a patient's treating physician is acting as a 'licensed health care provider' under [state law]," the Court reasoned. As a result, the case was time-barred.

Takeaway: Risk to Labs

While Quest came away with the win, the significance of the ruling is limited to the extent it was based on procedure and thus didn't address the substance of the malpractice claim. Moreover, the case is legally binding within South Carolina and will likely have little influence in other states.

The real significance of the case is that it portends the larger trend of holding providers of genetic testing to the standards of medical malpractice. This is not the first time that labs and physicians have been sued for malpractice for making a faulty diagnosis from DNA test results.

As with the Quest suit, these cases have turned on whether the lab constitutes a health care provider for purposes of state licensing and malpractice laws. While Quest claimed it was, labs typically take the opposite position and claim they're not licensed providers to avoid accountability under the

malpractice laws. But courts have consistently found that DNA testing labs is, in fact, a form of health care covered by state licensing. Consequences:

1. The testing lab is subject to medical malpractice liability;
2. The liability risk period is prolonged because the statute of limitations for medical malpractice tends to be longer than for other state tort actions (although that wasn't the situation in the Quest case); however,
3. Labs also get to benefit from tort reform measures designed to limit medical provider malpractice liability, e.g., caps on damages.

Previous Cases

So far, most of the medical malpractice cases against labs have alleged not wrongful death but *wrongful birth*, i.e., failure to diagnose pre-natal genetic disorders resulting in births that should and would have been aborted had the correct genetic information about the fetus been provided. (See the Scorecard on page 7 for a summary of the leading cases.)

Medicare Reimbursement: New HOPPS Date of Service Rules for ADLTs & Molecular Pathology Tests Take Effect

Here's what labs that bill Medicare for outpatient lab tests need to know about the new CMS rules exempting advanced diagnostic laboratory tests (ADLTs) and molecular pathology tests from Hospital Outpatient Prospective Payment System (HOPPS) laboratory 14-day date of service rules.

General Rules

The date of specimen collection is normally the date of service (DOS) for outpatient lab services. *Exception:* The DOS is the date the test is performed if:

- The doctor orders the test at least 14 days after a patient is discharged from the hospital;
- The specimen is collected during a hospital surgical procedure;
- Collecting the sample at another time would be medically inappropriate;
- Test results don't guide treatment provided during the hospital stay; and
- The test is reasonable and necessary for treating an illness.

When the "14-day rule" applies, the test is paid separately under Part B; in all other cases, it's bundled into the payment for the hospital stay.

CRITERIA FOR DIRECT BILLING OF OUTPATIENT ADLTs

Under new HOPPS rules, labs can directly bill Medicare under the CLFS for ADLTs delivered to outpatients less than 14 days after hospital discharge if either of the following criteria applies:

Criterion 1: The test:

- Analyzes multiple biomarkers of DNA, RNA or proteins;
- When combined with an empirically derived algorithm, yields a result predicting the probability of an individual patient's development of a certain condition(s) or response to a particular therapy(ies);
- Provides new clinical diagnostic information that can't be obtained from any other test or combination of tests; and
- May include other assays

Criterion 2: The test is cleared or approved by the FDA.

The ADLT & Molecular Pathology Test Exception

Under the new rules, the DOS for roughly 300 molecular pathology tests and ADLTs is the date of testing provided the tests are both:

- Excluded from OPPS packaging rules; and
- Ordered *less than* 14 days after a patient's hospital discharge.

Impact

The new CMS rule enables labs to bill Medicare for exempted ADLTs and molecular pathology tests directly under the Clinical Laboratory Fee Schedule.

Implementation

Although the new rules officially took effect on Jan. 1, 2018, CMS didn't begin implementing them until July 2. To give labs leeway to get used to the rules, the agency will exercise enforcement discretion until Jan. 2, 2019.

Compliance Perspectives: Respiratory Protection Program, From Page 1

mation into an on-premises computer intake station. The patient complained that the intake station was within eye and earshot of the adjacent station and snapped off photographs of the two stations with her smart phone just in case she needed evidence to document her privacy complaint later on. After the OCR and DC Office of Human Rights rejected her privacy claim, the patient decided to take LabCorp to court.

Many states have adopted their own privacy laws to protect patients, including mandatory breach notification.

The Ruling

LabCorp claimed that the patient had no right to sue for a HIPAA violation. Or, to state it in legal terms, LabCorp argued that even if the adjacent intake stations did violate HIPAA rules, the patient had no legal case because the HIPAA statute neither expressly nor implicitly grants individuals a "private cause of action," i.e., the right to sue a provider in civil court for money damages. The court agreed and dismissed the case without a trial [*Thomas v. LabCorp*, U.S. District Court for the District of Columbia, No. 18-591 (RC), June 25, 2018].

The Law

The *Thomas* ruling is in line with previous cases ruling against individual plaintiffs seeking to sue providers for money damages for HIPAA violations. In other words, any penalties to be imposed on providers under HIPAA must come from the regulators, not the individual victims.

The First Caveat: Risk of Damages Under State Privacy Laws

Of course, there's more to medical privacy than HIPAA. Many states have adopted their own privacy laws to protect patients, including mandatory breach notification. In addition to providing for stiff penalties, some states provide broader remedies to individual victims, including a private cause of action for failure to provide timely notification of a privacy breach. Thus, while the doors to federal court may be barred, individuals victimized by lab privacy snafus may be able to sue and win big damages in state court.

The Second Caveat: Risk of Collateral Liability

The other thing labs need to keep in mind is how committing a HIPAA breach can heighten liability risks under other laws. For example, failure to properly protect PHI can serve as powerful evidence in a negligence, malpractice or consumer fraud case against a lab.

3 TAKEAWAYS

1. Patients can't sue labs for HIPAA violations
2. Patients may be able to sue you for state privacy violations
3. HIPAA violations may make it easier for patients to sue for negligence and other violations

OIG Work Plan Monthly Review: July 2018

None of the six new items that OIG added to its Work Plan in July directly impact labs.

1. Identification of HHS Cybersecurity Vulnerabilities

Questions: Where are the cybersecurity vulnerabilities in the HHS's Secretary Office and Operating Divisions' IT systems?

OIG Action: The OIG will perform a series of IT audits to find out.

2. Review of Post-Operative Services Provided in the Global Surgery Period

Issue: Section 523 of MACRA requires CMS to collect data on post-operative services included in global surgeries and requires OIG to audit and verify a sample of the data collected.

OIG Action: The OIG will review a sample of global surgeries to determine the number of post-operative services documented in the medical records and compare it to the number of post-operative services reported in the CMS data to verify the accuracy of the number of post-operative visits reported to CMS by physicians and determine whether global surgery fees reflected the actual number of post-operative services that physicians provided to beneficiaries during the global surgery period.

The OIG will determine how much Medicare could have saved had it implemented the same requirements for 3D-CRT planning services.

3. Review of Outpatient 3-Dimensional Conformal Radiation Therapy (3D-CRT) Planning Services

Issue: Hospitals use CPT code 77295 to bill Medicare for developing a 3D-CRT treatment plan. Automated prepayment edits prevent additional payments for separately billed radiation planning services billed on the same date of service as the 3D-CRT treatment plan. Additional payments are allowed if they're billed on a different date of service. For a form of radiation similar to 3D-CRT, Medicare bans payments for separately billed radiation planning services billed on a different date of service.

OIG Action: The OIG will determine how much Medicare could have saved had it implemented the same requirements for 3D-CRT planning services.

4. Increased Payments for Transfer Claims with Outliers

Issue: Under the transfer rule, CMS reduces the DRG payment by applying a graduated per diem payment on the Medicare claim of the hospital transferring the patient to another setting early in the hospital stay. Since DSH and IME payments are a percentage of the reduced DRG payment, they're also reduced. By contrast, by reducing the threshold above which a claim qualifies as an outlier, the outlier methodology may cause an increase in the outlier payment in transfer cases.

OIG Action: The OIG will do a report describing the extent to which additional Medicare outlier payments negate the reduction in DRG, DSH and IME payments of transfer claims.

5. HRSA Oversight of Funds for Access Increases in Mental Health and Substance Abuse Services (AIMS)

Issue: In 2017, HRSA awarded $200.5 million in AIMS grants to 1,178 health centers nation-wide to expand access for existing Health Center Program grant recipients to mental health and substance abuse services, focusing on treatment, prevention and awareness of opioid abuse.

OIG Action: The OIG will review HRSA's internal controls to determine if they're suitable for: (1) awarding AIMS grants; and (2) monitoring AIMS grant recipients.

6. SAMHSA's Oversight of Accreditation Bodies for Opioid Treatment Programs

Issue: SAMHSA issued final regulations establishing an oversight system for treatment of substance use disorders with Medication-Assisted Treatment, including procedures for an entity to become an approved accreditation body for evaluating opioid treatment programs (OTPs).

OIG Action: The OIG will perform a series of audits on SAMHSA-approved accrediting bodies with accredited OTPs to determine if SAMHSA's oversight of accreditation bodies met federal requirements.