G2 INTELLIGENCE
A DIVISION OF PLAIN LANGUAGE MEDIA

G2 Compliance Advisor

For Clinical and AP Laboratories and Pathology Practices

October 2015

Inside this issue

www.G2Intelligence.com

Upcoming G2 Events

Lab Revolution
April 6-8, 2016
Sheraton Wild Horse Pass Resort & Spa, Chandler, AZ
www.labrevolution.com

WEBINARS:

Lab and Pathology Coding and Billing Update for 2016
Diana W. Voorhees, M.A., CLS, MT, SH, CLCP
Nov. 12, 2015, 2–3:30pm EST

New Date! Don't Let the Government "Take Down" Your Lab: Understanding and Responding to the Current Enforcement Environment
Gina L. Simms, Esq. & Robert E. Mazer, Esq.
Ober Kaler
Dec. 9, 2015, 2–3:30pm EST

HIPAA Compliance Enforcement to Escalate

Expect more government investigations of labs for HIPAA compliance. The government is more concerned than ever about the security of patient records and has signaled that it is ramping up enforcement against violators.

OCR enforcement to intensify

The Department of Health and Human Services' Office for Civil Rights (OCR), the agency that enforces HIPAA's privacy and security rules, has announced that it intends to be more punitive with HIPAA violators than it has in the past, according to OCR Director Jocelyn Samuels.

"We really do want to work with covered entities and [have their] voluntary compliance. But we have the authority to enforce and have the tools, including civil money penalties," she pointed out, speaking Sept. 2 at the eighth annual HIPAA security conference hosted by OCR and the National Institute of Standards and Technology in

Continued on page 9

How (& When) to Comply with New OSHA Chemical Safety Requirements

Over the next eight months, OSHA will be completing the phase-in of the Globally Harmonized System of Classification and Labelling of Chemicals (GHS), its most important new chemical safety rules in over a decade. Here's an overview of GHS, what clinical and anatomical laboratories must do and by when.

What's At Stake

If preventing chemical injuries and illnesses to lab workers is not motivation enough, complying with the new GHS rules is crucial to head off OSHA complaints, inspections, fines and other penalties. And don't forget about the negative publicity that comes with being charged with OSHA violations.

Failure to comply with GHS can also put your Medicare status in jeopardy. Explanation: In completing its 855b Medicare Enrollment Application, your lab must certify that it meets all applicable federal and state requirements, including OSHA. In addition to costing you your right to participate in Medicare, GHS violations can turn your certification of compliance into a false representation exposing your lab to liability (and the risk of triple damages) under the federal False Claims Act.

Continued on page 2

How (& When) to Comply with New OSHA Chemical Safety Requirements, *from page 1*

What GHS Is All About

Like other industrialized countries, the U.S. has adopted safety rules requiring employers to ensure their workers' "right to know" about the hazardous chemicals used, handled or stored in the workplace. Those rules are set out in the OSHA Hazard Communication standard (Hazcom). Because different countries follow different rules, the U.N. developed an international system called GHS to standardize workplace chemical safety rules around the world. OSHA adopted the GHS in May 2012 to bring Hazcom and U.S. rules into line with the UN system.

How GHS Affects Labs

GHS is not actually a new rule but a set of revisions to existing Hazcom rules. As those of you familiar with OSHA lab requirements may already know, chemical safety in clinical and anatomical labs is governed not by Hazcom but a separate, less rigorous regulation called the Occupational Exposure to Hazardous Chemicals in Laboratories standard (Sec. 1910.1450)) (Labs Standard). That means GHS has nothing to do with labs. Right? Wrong! Hazcom and GHS do affect labs, either directly or indirectly. Many labs subject to the Labs Standard are actually subject to Hazcom too. The chemical safety standard that applies, in other words, is determined not simply by the location being a lab but by the type of operation carried out there:

- **Laboratory operations are subject to the Labs Standard:** Such operations include handling and uses meeting all of the following four conditions: i. Chemical manipulations are carried out on a "laboratory scale," i.e., work with substances in which containers are designed for easy handling by one person; ii. Multiple chemicals are used; iii. The procedures aren't part of a manufacturing production process; and, iv. "Protective laboratory practices and equipment" are available to minimize risk of worker exposure.
- **Non-laboratory operations are subject to Hazcom:** Such operations include any other use of a hazardous chemical not defined above as a laboratory use, including use of chemicals for building maintenance, production of chemicals for commercial sale and quality control testing.

Result: A facility in which lab and non-laboratory operations are carried out would need two separate chemical safety systems—a Labs Standard system to protect workers performing the laboratory operations and a Hazcom system to protect workers who perform non-laboratory operations, such as custodians performing lab maintenance. Rather than going to the trouble of establishing and coordinating parallel systems, many labs use a single system for all workers and operations that is tailored to the requirements of Hazcom, since it is the more stringent of the two standards. Even labs that are subject to just the Labs Standard are indirectly affected by Hazcom. *Explanation:* GHS makes changes to the chemical labels and Material Safety Data Sheets, now simply referred to as Safety Data Sheets under the GHS (MSDSs/SDSs) required under Hazcom. And labs subject to the Labs Standard are also required to use these instruments.

The 3 Things You Must Do to Comply with GHS

Assuming that your lab is a downstream user, rather than a manufacturer, importer or distributor of hazardous products regulated by Hazcom, there are three things you need to do to comply with GHS:

1. Provide GHS Training. ***Deadline: Dec. 1, 2013 & Ongoing***

Labs must ensure that all workers exposed to hazardous chemicals receive proper GHS safety information and training. You should already be providing chemical safety training to exposed workers. GHS simply requires that your training account for the GHS changes, including at a minimum:

- Methods to detect and guard against chemical releases;
- Physical hazards posed by different chemicals;
- Health hazards posed by those chemicals;
- How to read the new GHS labels (see the section below); and
- How to access and read the new SDSs (see third section below).

What to Do: The deadline to provide initial GHS training was Dec. 1, 2013. Going forward, you must provide GHS training to workers on a continuing basis including initial training for new workers and current workers who are not currently exposed to hazardous chemicals when they are assigned to new jobs that involve exposure to hazardous substances (or whenever new chemical hazards for which they have not already been trained are introduced to their work areas). GHS training must be delivered to workers *before* they begin the job that involves exposure.

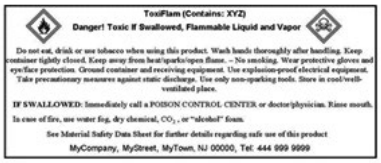
2. Replace Hazcom with GHS Labels. ***Deadline: June 1, 2016***

As before, all containers of hazardous chemicals used, handled or stored in your lab must be marked with a label displaying important safety information about the product. But while the label requirement is not changing, the label itself is:

Current Hazcom Label Elements	GHS Label Elements
▶ Identity of chemical ▶ Hazard warnings ▶ Name and address of manufacturer, importer or other responsible party	▶ Product identifier ▶ Signal word ▶ Hazard statement(s) ▶ Pictogram(s) ▶ Precautionary statement(s) ▶ Name, address phone number of manufacturer, importer or other responsible party

GHS labels will also have a new format and even a third color—red. Here's a side-by-side comparison with labelling examples OSHA uses for a fictitious product. The diamond shaped borders on the pictograms need to be in red:

HSC Label



GHS Label

What to Do: Although you have the option of creating it yourself, you can get a label for a particular chemical from the manufacturer or distributor that supplies the product to you. Between now and June 1, 2016, chemical labels can meet *either* current Hazcom *or* GHS requirements. After that date, only GHS labels will do.

Between now and June 1, 2016, your MSDS binder must contain up-to-date versions of *either* an MSDS *or* SDS for each hazardous chemical. After that date, hazardous chemicals must have an SDS and *only* an SDS.

3. Replace MSDSs with SDSs. *Deadline: June 1, 2016.*

Under current rules, all hazardous chemicals in your lab must have what's called a Material Safety Data Sheet, or MSDS, that describes the product, the hazards it poses and the safety precautions for using it. You must also keep and ensure workers have access to a binder containing up-to-date versions of each MSDS. The MSDS and MSDS binder will continue to be key elements of your lab safety program. But under GHS, the MSDS is morphing into the SDS—short for Safety Data Sheet. And it is not just the name. The new SDS has a different format and lists different information from the MSDS.

Current Hazcom MSDS Elements	GHS SDS Elements
▶ Identity of hazardous chemical	▶ Chemical identification
▶ Physical & chemical characteristics	▶ Hazard identification
▶ Physical hazards	▶ Information about chemical composition or ingredients
▶ Primary route(s) of entry	▶ First-aid measures
▶ Exposure limit, e.g., PEL, TLV	▶ Fire-fighting measures
▶ Whether chemical is listed in National Toxicology Program Annual Carcinogens Report	▶ Accidental release measures
▶ General precautions for handling & use	▶ Handling & storage information
▶ General control measures	▶ Exposure controls & personal protection
▶ Emergency & first aid procedures	▶ Physical & chemical properties
▶ Date of preparation or latest change	▶ Stability & reactivity
▶ Name, address & phone number of manufacturer, importer, employer or other responsible party that prepared or distributed MSDS	▶ Toxicological information
	▶ Ecological information
	▶ Disposal considerations
	▶ Transport information
	▶ Regulatory information
	▶ Other information including date of preparation or latest change

What To Do: As with the MSDS, the chemical's manufacturer or importer is responsible for preparing the SDS, although you can prepare your own SDS if you prefer. Between now and June 1, 2016, your MSDS binder must contain up-to-date versions of *either* an MSDS *or* SDS for each hazardous chemical. After that date, hazardous chemicals must have an SDS and *only* an SDS.

Takeaway: Laboratories must make sure chemical labels and safety data sheets are up-to-date before next June. G2

Compliance *Dos* & *Don'ts* Revealed By Experts Throughout 33rd Annual Lab Institute

For two and a half days on Capitol Hill, compliance concerns permeated G2 Intelligence's 33rd Annual Lab Institute. Beginning with a compliance-focused workshop and continuing through keynote addresses and panel discussions, industry stakeholders and experts shared their perspectives on how to ensure laboratory and pathology groups comply with the myriad of existing and developing rules and regulations governing the sector. Here's an overview of the compliance *do*s and *don't*s our presenters had to share regarding the top compliance issues currently facing laboratories.

DON'T Overlook Kickback Risks Hidden in Marketing and Promotion Activities

Opening a pre-conference workshop devoted to discussion of legal and compliance risks arising in lab and pathology arrangements, health care attorney Danielle Sloane, of Bass, Berry & Sims PLC in Nashville, spotlighted several general fraud and abuse issues for labs—among them, arrangements with marketing personnel. Sloane quoted the Department of Health and Human Services Office of Inspector General (OIG) as saying "many marketing and advertising activities may involve at least technical violations of the [Anti-Kickback] Statute." The concern is that marketing services are paid specifically to recommend services reimbursed by federal programs. Sloane recommended three issues to watch out for when structuring marketing arrangements:

- Incentive compensation—Outside the bona fide employee safe harbor this payment method raises kickback risks.
- Variable fee arrangements—per click, percentage or volume based payments raise kickback concerns.
- Arrangements including OIG "suspect characteristics" such as direct-to-patient marketing.

The Stark Law only permits labs to supply referring physicians with free items that are used "solely" to collect, store, process, or transport a specimen.

On a related note, Sloane also called attention to the risks related to the employee or independent contractor status of sales agents and marketing professionals—a subject which is gaining a lot of attention lately from the Department of Labor and Internal Revenue Service (see *GCA, Compliance Perspectives*, Aug. 2015, p. 5). She highlighted that the OIG has noted the potential for "abusive practices by salespersons who are independent contractors" and recommended that employing sales professionals increases control and supervision and protects incentive arrangements. So laboratories and pathology groups must consider their use of sales and marketing professionals, the employment status of those professionals and then ensure their activities aren't giving rise to kickbacks for the business they attract to the lab or pathology practice.

DO Use Caution Providing Freebies

Sloane also discussed the perennial compliance problem of providing freebies to referral sources. The Stark Law only permits labs to supply referring physicians with free items that are used "solely" to collect, store, process, or transport a specimen. Free items also can be considered improper remuneration for referrals under the Anti-Kickback Statute.

COMPLIANCE PERSPECTIVES

Freebies have received significant attention recently with the litigation between Ameritox and Millennium Health (see *G2 Compliance Advisor*, Sept. 2015, p. 3 and *G2 Compliance Advisor*, Feb. 2015, p. 1) and Millennium Health's recently announced settlement of allegations that its provision of free point of care testing (POCT) cups to physicians violated the Anti-Kickback Statute and Stark Law (see page 12). In the Ameritox/Millennium Health litigation, the Department of Justice filed a brief stating its position on the matter of what "solely" means—not even a very small benefit can be conferred on the receiving physician if the item conveys tangible benefits not related to permissible collection, transport, and storage purposes. Sloane highlighted factors the OIG considers: the tangible benefit the physician could receive from the freebie, whether the physician would otherwise need to pay for the item or service, and whether the freebie effectively offers a discount to referring physicians or their patients. She also provided examples of items that are acceptable—urine collection cups not having a point of care testing feature, vials for transporting blood, access to interfaces for communicating orders and results—contrasted against those the government has found improper: sterile gloves, biopsy needles, reusable needles, snares, and professional courtesy lab tests for health care providers.

What's a laboratory to do when it finds itself on the outside of an exclusive payer relationship?

DON'T Routinely Waive Charges for Out of Network Services

Another pre-conference workshop presenter, health care attorney Peter Kazon of Alston & Bird in Washington, D.C. quipped that he drew the short straw on the panel as his topic had no easy answers: compliance problems related to out of network services. What's a laboratory to do when it finds itself on the outside of an exclusive payer relationship? He said laboratories must balance both legal and business risks and are often caught between the payers who want to protect their networks and physicians who don't want their patients billed significant charges because the service was out of network. Clearly, what not to do is routinely waive copays and deductibles because doing so can run afoul of federal and state laws regarding waivers. The OIG has warned against waivers in the 1994 Fraud Alert as well as this year's OIG Advisory Opinion 15-04. Kazon noted that this year's Advisory Opinion is the first time the OIG has looked at convenience in finding remuneration; however, it was a combination of factors that the OIG cited as the reason it found impropriety in that opinion. He added that state law complicates the issue for laboratories by often ambiguously addressing the issue. Finally, private payers are also stepping into the fray, taking action themselves to counter routine waivers that threaten their exclusive networks.

Kazon's advised laboratories should 1) look closely at the factors highlighted in the OIG's most recent Advisory Opinion about waiving charges for out-of-network services and don't adopt a policy of generally refraining from billing out of network services; 2) consider applicable state law provisions regarding waivers; 3) not discuss waivers in the context of referrals; 4) take care that marketing statements and sales professionals don't state or imply that the laboratory will accept payer reimbursement as payment in full; 5) establish policies addressing out of network services; 6) communicate with physicians about the rules; 7) bill patients for their copays and deductibles but consider financial hardships and work with patients to appeal claims or work out payment plans.

DO Consider Compliance Issues Raised by Client Billing Arrangements

Health care attorney Jane Pine Wood of McDonald Hopkins discussed client billing—that is, labs billing other labs, physicians or hospitals, for laboratory services. The compliance issue raised in these arrangements is the "usual charge" issue that was a focus of the OIG's Advisory Opinion 15-04 earlier this year. Wood noted that while we haven't seen enforcement actions relating specifically to the usual charge issue, the concern is whether a laboratory's usual charge is "well below Medicare." Wood also cautioned attendees to be aware of differing state laws on client billing and particularly laws regarding markups. Referencing the recent announcement of Strata Pathology Laboratory's settlement resolving kickback allegations relating to billing arrangements between Strata and physicians who paid Strata to perform pathology services, Wood noted that case indicates that the client billing issue is clearly on the list of items the government is looking at.

She also highlighted some common compliance traps for laboratories related to billing other parties for testing services:

- state law provisions prohibiting mark-ups (for example, California prohibits a mark-up on lab-to-lab billing arrangements);
- the Medicare 70/30 rule – which requires 70% of testing be done in house by a laboratory or it can lose its Medicare eligibility;
- marketing arrangements—Wood raised the question of whether a lab that refers work to another lab is marketing for that lab and giving rise to potential problems regarding payments involved;
- in-office ancillary services exceptions—having a separate legal entity perform test services creates risk as shown by the settlement announced earlier this year concerning referrals to a dermatology practice's in house pathology laboratory;
- anatomic pathology Medicare anti-markup rules imposing physician supervision requirements for the technical services.

DON'T Forget It's Not Just Business: Consider Fraud, Abuse and Antitrust Implications of Transactions

Amid discussions throughout the conference about health care reform and the shift from volume to value-based reimbursement, antitrust lawyer Dionne Lomax and health care lawyer Karen Lovitch of Mintz Levin Cohen Ferris Glovsky and Popeo reminded attendees of compliance issues that can arise while strategizing partnerships and ventures that will help laboratories and pathology groups survive in this new environment. Lomax explained recently heightened Federal Trade Commission (FTC) attention to health care transactions, providing some assurance that laboratory transactions can be achieved without raising significant antitrust hurdles if careful attention is paid to factors that concern the FTC. Lomax advised attendees to always consider their market, their share of that market, activities undertaken within the arrangement, and how a transaction will affect that market. For example, exclusive arrangements can be lawful, advised Lomax, but their duration, other competitors in the marketplace and availability of less competitively restrictive arrangements must be considered.

COMPLIANCE PERSPECTIVES

Karen Lovitch cautioned laboratories to consult counsel earlier rather than later in developing a transaction or agreement. For example, she related that laboratories are often unaware that the structure of a deal can trigger change of ownership notification requirements and licensure issues. Finding out about these requirements late in the game can delay deal closure. Another critical step to ensuring compliant transactions, advised Lovitch, is to engage third party valuation consultants to provide guidance on fair market value for all compensation to avoid running afoul of fraud and abuse laws.

DO Prepare Now to Comply With Expected Changes to Oversight of LDTs

Several presentations addressed the current status of laboratory developed test (LDT) oversight, potential alternatives or alterations to the FDA framework issued last year, and what laboratories should be doing now. Peter Kazon indicated Congress may act to take the place of what the FDA has proposed and at the same time, the FDA is looking to revise its guidance and the result "may look significantly different" than what came out last year. "This is an area in tremendous flux," he concluded.

Prepare for FDA inspections by developing procedures and conducting internal audits.

In a panel discussion, Allison Fulton and James Stansel, health care lawyers with Sidley Austin in Washington D.C., advised laboratories on practical steps they can take now in anticipation of more significant oversight of LDTs. Some of the steps they recommended include:

1. **Take stock.** Evaluate the LDTs the laboratory currently has and the claims they make with regard to each of those LDTs. Consider existing IVDs that are similar in intended use and their risk classification to gain insight on potential future classification of LDTs. Consult the existing FDA proposed framework to get a sense of potential obligations—whether notification or full approval.
2. **Focus on Quality Systems.** Fulton emphasized the onerous nature of FDA quality systems requirements, noting that both the house bill and the Diagnostic Test Working Group alternatives to the FDA framework also include quality systems requirements. So laboratories should take time now to survey what quality systems they already have in place and what they would need to do to comply with FDA quality system regulations. Begin crafting a strategy for meeting FDA quality system requirements including evaluating what expertise you will need on your team. Fulton suggests you may need to hire consultants.
3. **Gear up for inspections.** Prepare for FDA inspections by developing procedures and conducting internal audits. Also, appoint someone to be the contact person for the FDA and review FDA enforcement actions to get a sense of trends in current enforcement.
4. **Update compliance plans.** Fulton and Stansel emphasized the need to add LDT-related compliance concerns to the laboratory's overall compliance program including issues such as off-label promotion and similar marketing concerns as well as potential fraud and abuse issues raised by arrangements with consultants and other providers related to commercializing LDTs.

HIPAA Compliance Enforcement to Escalate, *from page 1*

Washington, DC. OCR is also more likely to require bigger fines and formal "resolution agreements" with a covered entity than informal corrective action when an investigation uncovers multiple HIPAA violations and little attempt to comply with the law.

For instance, OCR's most recent settlement agreement, with Indiana based Cancer Care Group, a 13-physician radiation oncologist practice, involved "widespread" noncompliance with HIPAA's security rule. OCR launched an investigation after the medical group reported the theft of unencrypted back up files of 55,000 patients from an employee's car. The agency found that the group had never conducted a risk analysis of vulnerabilities of electronic patient data, a requirement of HIPAA since 2005. The group also had no written policies and procedures regarding the protection of electronic patient data taken out of the office even though employees routinely took laptops and other hardware home or elsewhere. The group agreed to pay $750,000 and enter into a corrective action plan to settle the allegations, according to OCR's August announcement.

"Remember the HIPAA rules are flexible and scalable and can be customized [based on the size of the entity]."

—Jocelyn Samuels, OCR Director

And Brighton Massachusetts-based St. Elizabeth's Medical Center agreed in July to pay $218,400 after it exposed electronic records of its patients on the internet by using an unauthorized, unsecured, internet-based document sharing application to store the documents. The medical center, which had suffered at least two other security breaches, then compounded its violation by failing to handle the security breach as required by HIPAA, including timely reporting and mitigating the potential harm to patients whose records had been compromised. OCR launched an investigation after receiving a complaint about the security breach.

More than 1,300 security breaches of 500 or more patient records have been reported to HHS since reporting was required in September 2009, and more than 157,000 reports of breaches affecting fewer than 500 individuals have been submitted, Samuels reported. While most breaches affect just one or two patients, 2015 has been a banner year for very large "high profile" breaches affecting millions at a time, such as the hacking of Anthem's system, compromising 80 million records, and the most recent attack on Excellus Blue Cross Blue Shield, which exposed 10 million records. OCR will open an investigation into all reports of breaches of 500 or more individuals, as well as of complaints filed.

Samuels recommended that covered entities be "vigilant" in protecting patient information, with strong controls, self-auditing, allowing only permissible uses and disclosures of information, and patching out-of-date software. She also noted that patient information on mobile devices is also subject to HIPAA and must be protected.

And while OCR will investigate providers of all sizes, it does recognize that there is not a one-size-fits-all requirement regarding compliance. "Remember the HIPAA rules are flexible and scalable and can be customized [based on the size of the entity]," she noted.

Samuels also reported that OCR is "hard at work" on the launch of the permanent audit program, and that most of those audits will be desk audits. OCR will soon post an audit protocol on its website, which entities can use to conduct a self-audit. The permanent audit program, required by the HITECH Act of 2009 which amended HIPAA, is slated to begin early in 2016.

OIG blasts OCR's performance

OCR's enforcement will likely be fueled further by the Office of Inspector General's (OIG) recent criticism of OCR's HIPAA enforcement. In two reports issued in Sep-

tember, the OIG chastised OCR for both its inadequate oversight of compliance with HIPAA's privacy rule and poor follow up of reported breaches of protected health information. The OIG found, among other things, that:

- OCR was primarily reactive, investigating in response to complaints, and should be more proactive;
- Documentation of corrective actions and follow up of security breaches was incomplete;
- Its case tracking system had limited search functionality;
- Many providers were noncompliant with HIPAA; and
- OCR staff were not always checking to see if an entity being investigated had previously been investigated or if one reporting a breach had reported one in the past.

The OIG recommended that, among other things, OCR get a permanent audit program up and running, improve its current investigatory process, and increase its education and outreach to improve HIPAA compliance.

The OIG recommended that, among other things, OCR get a permanent audit program up and running, improve its current investigatory process, and increase its education and outreach to improve HIPAA compliance.

FBI issues warning about 'Internet of Things'

If that was not enough, the Federal Bureau of Investigation (FBI) issued an alert September 10 warning providers and consumers that devices and objects that connect to the internet to send and receive data are vulnerable to cyber attack. While some of the devices the FBI referenced in its alert are more consumer oriented, such as "smart" televisions, wearable fitness devices and baby monitors, some of the objects of concern include ones common in labs and other businesses, such as printers, security systems and thermostats.

"Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety," the FBI says in the alert. The cyber criminals can also take advantage of these devices by rendering the device inoperable or interfering with business transactions.

The FBI recommended that steps be taken to reduce the risk of being a victim of such cyber crime, including:

- Protect wireless networks with strong passwords
- Isolate devices on their own protected networks
- Use security patches when available

Revisit HIPAA compliance

Now is a good time for labs to review whether they're in compliance with HIPAA. Consider these six tips:

1. Conduct a self-appraisal of compliance with HIPAA's privacy and security rules. For instance, conduct a risk analysis of patient information in electronic form to check for vulnerabilities, such as lack of firewalls or weak passwords. Take steps to reduce or eliminate any vulnerabilities identified. Make sure that staff are trained in HIPAA compliance. Some safeguards are required by HIPAA; others are "addressable" but not necessarily required to be implemented.

2. Make sure you've entered into business associate agreements with any entity or individual handling patient protected information on the lab's behalf, such as a billing company. HIPAA requires labs and other covered entities to enter into business associate agreements with business associates to ensure that the business associate will safeguard the patient information adequately. OCR has provided sample business associate agreement language on its website.
3. Consider encrypting patient information. Encryption is technically not required by HIPAA. However, a lab that opts not to encrypt has to at least address why it isn't encrypting and document what alternative it will use instead to protect the data, according to Deven McGraw, deputy director, health information privacy division for OCR, also speaking at the OCR/NIST conference. "'Addressable' does not mean optional. It never has. We expect you to address it," she explains. Note that patient data that is lost or stolen but has been encrypted in accordance with NIST standards is "secure" and does not need to be reported to patients or HHS.
4. Have an action plan to handle a breach of unsecured patient information. There are steps a lab needs to take, such as conducting an assessment of the likelihood that the information was compromised, timely notifications to HHS, patients and in some cases the media, and corrective action to forestall future breaches. You don't want to be caught scrambling to comply once a breach has occurred.
5. Don't forget state law. State laws are often broader than HIPAA. For instance, labs suffering a breach of patient information may have to report it more quickly to state authorities than to HHS.
6. Keep an eye out for future developments. There's a lot of activity concerning the privacy and security of patient data. In addition to the revised audit protocol expected this year, OCR is planning on releasing new guidance on patient access to their data. Other guidance or rules that are still forthcoming include clarification on what disclosures of patient information are the "minimum necessary" and a proposed rule on how individuals that have been harmed by a data breach should receive a portion of the penalty imposed on the violator. Both of those are part of the HITECH Act of 2009 that amended HIPAA

Takeaway: Labs should make sure that they have a robust HIPAA compliance program, especially since even the most diligent lab may suffer a breach of patient information via hacking, user error or other event.

G2 Compliance Corner

Promote Cyber Security Awareness

In the health care industry, October is perhaps most commonly identified with Breast Cancer Awareness. Certainly it's a topic worthy of laboratory sector attention given the industry's role via BRCA testing in identifying breast cancer risk. But the month also serves as an opportunity to draw awareness to some non-diagnostic issues less often discussed among laboratorians and pathologists but which can still impact operations. October is also National Cyber Security Awareness Month, sponsored by the Department of Homeland Security and the National Cyber Security Awareness Alliance. The issue of cyber security affects all industries and businesses but none more than the keepers of sensitive health information—health care providers such as laboratories and pathology groups who gather increasing amounts of data and are being challenged to improve health care delivery with increased interoperability and data sharing. Noting that technology has "spearheaded advancements in healthcare" and other industries, the Department of Homeland Security's web site cautions that no industry is "immune to cyber risks" and because we are so dependent on "critical infrastructure and the digital technology that operates it," cyber security is critical and "cyber security is a shared responsibility."

Cyber Security to do: This month, review your information security programs, policies and procedures for gaps. Develop and implement training to keep information security in the front of everyone's minds. Reiterate the importance of using strong passwords and changing them frequently. Remind all those using your systems to take care with suspicious emails, avoid phishing traps and be careful with the sites they visit if you allow them to use work-related devices for personal use. Protecting your lab and your patients from cyber crime is required by HIPAA (see Page 1 for more information about HIPAA enforcement) and other federal and state laws. But it's also important for protecting your employees and your business operations as well.

News at a Glance

Millennium Settles False Claims Allegations for $256 Million. Millennium Health announced it will pay $256 million and enter into a corporate integrity agreement with the Department of Justice to resolve False Claims Act and Anti-kickback statute allegations. Payment of $227 million settles False Claims allegations of unnecessary urine drug testing through use of custom profiles and standing orders rather than individualized patient need assessment and claims that point of care testing (POCT) cups were provided to physicians in exchange for referral of urine specimens in violation of the Anti-kickback statute and Stark Law (see *GCA*, Sept. 2015, p. 4). Millennium will also pay $10 million to settle False Claims allegations relating to genetic testing the government claimed was routinely performed without regard to individualized need assessment. Finally, a $19.2 million settlement payment to the Centers for Medicare and Medicaid Services concerns urine drug test billing. The settlement of the claims, however, involves no determination of liability and Millennium Chief Executive Officer Brock Hardaway indicated the company "may debate some of the merits of the DOJ's allegations" but respects the government's enforcement role and sought to bring closure to a lengthy investigation. The organization has also revamped its board of directors with mostly new independent members and indicated intentions to pursue financial restructuring.

Proposed Changes to Research Rules Affect Biospecimens. The Office for Human Research Protections held a town hall this month to discuss proposed changes to rules governing human research. The proposed changes require a general informed consent for secondary research using a stored biospecimen (for example, the remains of a blood sample originally drawn for clinical purposes) even when the investigator isn't given information that can identify the donor. Separate consent wouldn't be required for each specific research use of the biospecimen. Consent would also be subject to public scrutiny and privacy safeguards would be required for research using biospecimens. The storing or maintaining of biospecimens and identifiable private information for future unspecified research, or the research itself, would be exempt from IRB review. Consent will not be waived for research involving biospecimens except in "very rare circumstances." Public comments to the proposed rule changes are due by Dec. 7, 2015.

OIG Advisory Opinion Reacts Favorably to Free Transport for Health System Patients. A program designed to provide transportation within a healthcare system, in the absence of public transportation, won't be subject to sanction according to Office of Inspector General Advisory Opinion 15-13. The free van shuttle service would transport patients to medical facilities within an integrated health system, including a medical center, two small community hospitals and an ambulatory surgical center. The system also includes a multispecialty clinic comprised of 1,000 physicians. Limited public transportation and private taxi services were locally available and the health system argued the "lack of affordable transportation … constitutes a barrier to health care access." Transportation would be provided to patients of the system facilities without regard to ability to pay for health care services, health insurance status, or reference to volume of federal health care program business for the system. The OIG also found transport wasn't advertised to the general public, would only serve the system's facilities, didn't bring patients from outside the system's primary service area and wasn't likely to "subsidize the practices of Private Physicians." Therefore, the OIG indicated that while the arrangement could provide prohibited remuneration, there was minimal risk of fraud and abuse, so it wouldn't impose sanctions. G2

Kelly A. Briganti, JD, Editorial Director, Kelly@plainlanguagemedia.com; Barbara Manning Grimm, Managing Editor; Marla Durben Hirsch, Contributing Writer; Glenn S. Demby, Contributing Writer; Stephanie Murg, Managing Director, G2 Intelligence; Kim Punter, Director of Conferences & Events; Randy Cochran, Corporate Licensing Manager; Jim Pearmain, General Manager; Michael Sherman, Marketing Director; Pete Stowe, Managing Partner; Mark T. Ziebarth, Publisher.
Receiving duplicate issues? Have a billing question? Need to have your renewal dates coordinated? We'd be glad to help you. Call customer service at 1-888-729-2315.