The mounting scrutiny over HIPAA privacy and security enforcement this year — combined with the now astronomical fines you can incur — means that you can’t let your guard down at all where protected health information is concerned.

If you want to reduce your HIPAA breach dangers, tighten up your electronic health record (EHR) privacy, update business associate agreements, and learn how to create a good risk analysis plan, you’ll need the expert guidance offered in this HIPAA Handbook 2015.

Brought to you by The Coding Institute, our handbook includes field-tested best practices from nationally-recognized HIPAA compliance experts to help you manage your privacy and security risks in 2015.
## Breaches

- **Case Study: How Much Could You Pay For Your BA’s Mistakes?** ........................................ 1
- **Case Study: Follow 3 Steps To Avoid Laptop HIPAA Breaches** ........................................ 3
- **Case Study: Learn These Lessons From The Biggest HIPAA Settlement To-Date** ............... 5
- **Enforcement News: How Liability Insurers Try To Get Out Of Paying Your HIPAA Defense Costs** ........................................ 7
- **Case Study: Don’t Forget About The Privacy And Security Of Your Paper Records** ........... 8
- **Enforcement News: How Access Controls And Employee Training Are Key To Preventing Breaches** ........................................ 10
- **Case Study: Learn 4 Lessons To Secure Your Backup Tapes** ........................................ 13
- **Lawsuits: How Potential Precedent-Setting Court Ruling Is Good News For You** ............. 15
- **Theft Risk Is Always Present: Encrypt All Laptops** ....................................................... 17
- **Case Study: Watch Out For Sophisticated Malware Breaching Your Systems From Overseas** ........................................ 18
- **Ask Yourself 5 Questions To Gauge Your Breach Vulnerabilities** ................................... 20
- **Enforcement News: How Data Breach Settlement Sets ‘Unfortunate Precedent’** ............... 21
- **Case Study: Don’t Overlook Data Breach Risks From Desktop Thefts** ............................ 25
- **Enforcement News: Can PHI Really End Up On Google? Yes, This Happened** ................. 26
- **Case Study: Understand HIPAA’s Evolving Impact On Med Mal Lawsuits** ...................... 28
- **Enforcement News: How You Can Overcome HIPAA Lawsuits Based On ‘Speculative’ Claims** ........................................ 30
- **Case Study: Don’t Cut Any Corners In Your Security Rule Compliance Practices** ............ 32
- **Learn 7 Big Lessons From HIPAA Breaches** ............................................................... 34
- **Enforcement News: When HIPAA Trumps State Law Privacy Claims** ............................ 35
- **Case Study: Watch Out: Data Breach Litigation Is Getting More Creative** ...................... 38
- **Enforcement News: No ‘Present Injury,’ No Grounds For Lawsuit, State Court Says** ......... 40

### Reader Questions

- **Will Your General Liability Policy Cover Security Breaches?** ........................................ 43
- **No Breaches — Do You Still Need To Submit An Annual Report?** ................................ 43
- **Does Breach Of Single Person’s PHI Require Notification?** ........................................ 44

## Policies & Procedures

- **Check Out These Free Compliance Tools** ............................................................... 45
- **Enforcement News: Make Photography And Recordings Part Of Your HIPAA Policies** .... 46
- **HIPAA Compliance: How Your HIPAA Obligations Regarding Same-Sex Marriage Have Changed** ........................................ 47

### Reader Questions

- **Can You Let NPP Rules Slide In This Situation?** ........................................ 49
- **Is A ‘Consent Form’ A Good Idea For Email Communications?** ................................. 49
- **Is Signing NPP Acknowledgement Enough For Communication Permission?** ................ 50
### Risk Analysis

- **Enforcement News:** Check Out The New Risk Assessment Tool For iPad & Windows .......................... 51
- **Risk Assessment:** Understand The 6 Major Risk Categories For Your Risk Assessment .......... 52
- **Tool:** Use This Cheat-Sheet To Mitigate Your Security Risks .................................................. 54

### Reader Questions

- What’s The Biggest HIPAA Issue For EHR Implementation? .............................................................. 55
- Which Comes First: Compliance Or Strategic Risk? ........................................................................ 55
- How Can You Make Continuous Monitoring Feasible? ...................................................................... 56
- What Are Some Tips To Elicit More Support For Risk Management? .............................................. 56

### EHRs/Meaningful Use

- **EHRs:** Good News: You Could Get Some Breathing Room For EHR Compliance ....................... 58
- **Not Ready?** Get A Meaningful Use ‘Hardship Exception’ ................................................................. 60
- **EHRs:** Meaningful Use: Get Your 2014 CEHRT Now .................................................................... 61
- **Try Decision-Point Maps To Help Justify Not Meeting MU Deadlines** ........................................ 63
- **Why EPs Are Failing MU Audits** .................................................................................................... 64
- **No Electronic Records Causes Sperm Bank Mix-Up** ...................................................................... 65

### HIPAA Audits

- **Enforcement News:** Watch Out: Upcoming HIPAA Audits Will Be ‘Aggressive’......................... 66
- **Avoid The Top 5 Investigated HIPAA-Compliance Issues** ............................................................... 67
- **Watch Out SNFs:** HIPAA Penalties Will ‘Set Records’ .................................................................. 68
- **HIPAA Audits:** Get Ready For Phase 2 Of OCR Audits: Take 7 Steps ........................................... 69
- **Curious? Find Out What Phase 1 OCR Audits Revealed** ................................................................. 72

### Reader Questions

- Can Multiple Small Breach Reports Trigger An Audit? ................................................................. 73

### Business Associate Agreements (BAAs)

- **Update Your ‘Pre-Existing’ BAAs Now** .......................................................................................... 74
- **Breach Risk:** Keep A Close Watch On Your BAs ...................................................................... 75
- **Monitor Your Contracts To Catch Data Breaches** ......................................................................... 76

### Reader Questions

- Do BAs Need To Have HIPAA NPPs? ............................................................................................... 77
- What Are The Dangers Of Not Complying With New BAA Standards? ........................................ 77

### Privacy Rule

- **HIPAA Compliance:** New Guidance: Emergencies Don’t Trump Your HIPAA Requirements .... 78

### Reader Questions

- ‘Consent’ vs. ‘Authorization’ — What’s The Difference? ................................................................. 81
- What To Do When Another Provider Refuses To Release Records ............................................... 81
- Is This An Incidental Use And Disclosure? ..................................................................................... 82
- Does The Privacy Rule Really Allow Disclosures To Family And Friends? .................................. 83
- What’s Wrong With Mailing Postcards To Patients? ................................................................. 83
Case Study: How Much Could You Pay For Your BA’s Mistakes?

*Why you’re increasingly at risk for breach-related private lawsuits.*

Finger-pointing will get you nowhere when you have a HIPAA breach. And one recent case demonstrates how you could end up paying through the nose for your business associate’s (BA’s) HIPAA violation.

**Background:** Led by former patient Shana Springer, Stanford Hospital & Clinics and two of its vendors faced a class action lawsuit for alleged privacy breaches of patients’ protected health information (PHI), violating California’s state privacy laws. The plaintiffs sought $20 million in damages, but the defendants recently settled the case for $4.1 million.

Multi-Specialty Collection Services LLC (MSCS) was Stanford’s BA and was named in the lawsuit, and then another BA contracting with MSCS, Corcino & Associates LLC, was added to the complaint. The lawsuit alleged that Stanford and its BAs were responsible for disclosing the PHI of 20,000 emergency room patients. The BA actually posted an Excel file online containing the PHI.

Because the BAs were at fault for the unpermitted disclosure, they will pay the majority of the settlement — about $3.3 million, reported attorney Elana Zana in a blog posting for the Seattle-based law firm Ogden Murphy Wallace. But Stanford is still stuck paying out a whopping $500,000 toward a “vendor education fund” under the settlement agreement, as well as $250,000 in settlement administrative costs.

**Why ‘No Fault’ Doesn’t Protect Your from Lawsuits**

And keep in mind that this settlement arose strictly from violations of state privacy laws. The state and federal government investigated the incident and determined that Stanford was not at fault for the disclosure, stated Martie Ross, attorney and principal for Pershing Yoakley & Associates (PYA), in an April 4 PYA Healthcare Blog posting. Stanford received no penalties or fines.

**Beware:** “The risks of private lawsuits are real,” Ross warned. Just because HIPAA does not include a private cause of action doesn’t mean that patients cannot sue you under state law.
“Many states, like California, have privacy laws that allow a private individual to sue a party that violates that law,” Ross noted. “Additionally, an individual can bring a common law claim for negligence, alleging a HIPAA breach violates the standard of care.

**Hidden trap:** And now that HIPAA requires you to notify patients of breaches, there are more opportunities for affected patients to pursue private claims, Ross said. Attorneys may not care much about a single patient’s complaint, but breaches usually involve a larger number of patients. And this can lead to a class action lawsuit with a potentially large payout, which is enticing to plaintiffs’ attorneys.

**Crack Down on Your BA’s Actions**

“Looking at the facts as reported, it is hard to find anything Stanford did wrong,” Ross lamented. Stanford had an appropriate BA agreement (BAA) in place, “it had no notice of any prior wrongdoing by MSCS, it encrypted the data sent to MSCS, and it met its obligations with respect to mitigation and breach notification once the posting was discovered.”

Stanford was even unaware of Corcino, which contracted with MSCS, and ultimately was directly responsible for the breach, Ross noted. “So why is Stanford paying out $750,000?”

“Not only is Stanford its brother’s keeper, it is also its brother’s brother’s keeper,” Ross said. Thanks to the HIPAA Omnibus Final Rule, there is now a greater emphasis on BAs’ and subcontractors’ responsibility to protect patient privacy.

**Bottom line:** “The major lesson to glean from this case is that covered entities should better investigate their vendors before transmitting PHI,” Zana stressed. “Meaning not just simply executing a Business Associate Agreement with an indemnification and insurance provision (though advisable), but also reviewing/evaluating their current security policies, staff training, use of subcontractors, and encryption standards.”
Case Study: Follow 3 Steps To Avoid Laptop HIPAA Breaches

*OCR is pushing entities harder to perform risk assessments.*

Two recently announced HIPAA settlements show that the HHS Office for Civil Rights (OCR) is cracking down on unprotected data contained on mobile devices. And if you’re not already encrypting your mobile devices, you’ll likely be next in the OCR’s crosshairs.

**Beware: HHS is Handing Down Tougher CAPs**

**Background:** Stolen unencrypted laptops were to blame for two HIPAA cases, which totaled nearly $2 million in settlements, as well as extensive corrective action plans (CAPs). Concentra Health Services, a subsidiary of Humana, Inc., agreed to a $1.7 million settlement with HHS for alleged HIPAA violations related to a breach notification stemming from a stolen unencrypted laptop.

According to Concentra’s HHS-ordered CAP, the company must:

- Implement a security management process, including a risk analysis and risk management plan;
- Provide written updates to HHS describing encryption requirements for all devices;
- Provide security awareness training for all workforce members;
- Submit an Implementation Report to HHS; and
- Submit Annual Reports to HHS.

QCA Health Plan, a health insurance provider in Arkansas, paid out a smaller settlement of $250,000, also due to a breach involving a stolen unencrypted laptop. The laptop contained the protected health information (PHI) of 148 individuals. Under QCA’s CAP, the insurer must:

- Implement a security management process, including a risk analysis and corresponding risk management plan;
- Provide security awareness training for all workforce members who have access to electronic PHI (ePHI); and
- Submit Annual Reports to HHS.

These two breach cases share many similarities. Among them are three key steps these companies did not take that could have prevented the breaches in the first place — or at least minimized the breach-associated costs and sanctions.

1. **Make Encryption Your Best Friend**

Crucial: The best precaution against a multi-million dollar settlement on your company’s books is widely available encryption software, according to a blog posting by Linn Foster Freedman and Kathryn Sylvia, both Providence, RI-based partners with Nixon Peabody LLP.
Although encryption is not *required* by HIPAA, covered entities (CEs) and business associates (BAs) “should assure that portable devices, including mobile devices and laptops, are encrypted and contain the minimum amount of ePHI necessary for an employee to carry out his or her responsibilities — if it is necessary at all,” Freedman and Sylvia stated.

This high settlement amount indicates that CEs and BAs “who choose not to implement encryption standards must be able to explain themselves,” wrote Elana Zana in an OMW Health Law blog posting for *Ogden Murphy Wallace Attorneys*, a law firm headquartered in Seattle. But there really is no other effective way for most providers to protect data other than encryption.

**Loophole:** “If a laptop or other mobile device is encrypted according to HHS standards, the loss or theft may fall within a legal safe harbor,” Freedman and Sylvia pointed out. “This fact alone should compel healthcare entities to consider using encryption technology.”

### 2. Don’t Make Excuses — Perform a Risk Analysis

One of the big problems in this HIPAA breach case was, in addition to not encrypting the laptops, the entities didn’t perform a risk analysis. You must “do a solid risk analysis,” stresses Jim Sheldon-Dean, founder and director of compliance services for *Lewis Creek Systems, LLC* in Charlotte, VT.

Although unlike Concentra, QCA had no direct fault for failing to encrypt its laptops. Instead, the QCA settlement focused on its lack of sufficient HIPAA security policies and procedures, Zana explained. Specifically, HHS found that QCA failed to conduct a security risk assessment and failed to implement security measures, especially physical safeguards.

### 3. Implement a Risk Management Plan

Implementing a risk management plan is part of both settlement agreements, which should give you a good idea of how important this task really is. The CAP for QCA was different from Concentra’s in that QCA’s focused on workforce training and reporting of workforce noncompliance, rather than on encryption requirements, Zana noted.

**Lesson learned:** “The settlements reinforce the OCR’s continued focus on enforcing failures to adequately protect ePHI on mobile devices,” Freedman and Sylvia observed.

Like most breach cases, the simple solution is to encrypt the data to avoid an actual breach — but these settlements reveal just how extensive your compliance obligations are and how severe the monetary penalties could be when you fail to protect PHI, Zana warned. “The message from HHS is not just the importance of data encryption, but rather its performance and follow-through with security risk analysis and implementation of security policies and procedures.”

Concentra and QCA, like other healthcare organizations who have settled with HHS, will have years of compliance reporting obligations and security management requirements that will likely create significant cost burdens in addition to the monetary settlement,” Zana concluded.

**Link:** To read the HHS press release and access the Resolution Agreements for both HIPAA settlements, go to [www.hhs.gov/news/press/2014pres/04/20140422b.html](http://www.hhs.gov/news/press/2014pres/04/20140422b.html).
Case Study: Learn These Lessons From The Biggest HIPAA Settlement To-Date

Entities agree to pay out a benchmark-setting $4.8 million.

If your company shares a data network and/or has a joint compliance agreement with another healthcare provider, a breach could mean double-trouble — and much bigger fines. Here’s what you can learn from the costly mistakes involved in this recent breach.

Background: Providers New York and Presbyterian Hospital (NYP) and Columbia University (CU) have a joint arrangement in which CU faculty members serve as attending physicians at NYP. The providers also operate a shared data network and firewall, which links to NYP’s patient information systems containing electronic protected health information (ePHI), according to an announcement by the HHS Office for Civil Rights (OCR).

A breach occurred when a CU physician who developed applications for both providers attempted to deactivate a personally owned computer server on the network containing NYP patients’ ePHI. This allowed the ePHI to become accessible on internet search engines.

After receiving a complaint from an individual who found the ePHI of a deceased partner (who was an NYP patient) on the internet, NYP and CU submitted a joint breach report, OCR states. The report revealed the disclosure of 6,800 individuals’ ePHI, including patient status, vital signs, medications, and laboratory results.

Lesson #1: Joint Breach Could Equal Larger Penalties

For the breach, OCR slapped the providers with an astounding $4.8 million in monetary payments — $3.3 million for NYP and $1.5 million for CU. As part of the settlement agreement, both providers have also agreed to substantive corrective action plans (CAPs), according to the OCR announcement.

Significance: “In addition to being the largest HIPAA settlement to date, this is the first settlement involving multiple covered entities,” noted Tampa, FL-based healthcare attorney Elizabeth Hodge in a posting for Akerman LLP’s Health Law Rx Blog.

“This settlement is another reminder of the importance that OCR places on an accurate risk analysis that identifies all places within a system that ePHI resides,” Hodge stated. “To avoid shared settlement payments, covered entities that permit shared access to ePHI should closely read the NYP and Columbia resolution agreements and implement the described action items.”
Lesson #2: Whatever You Do, Don’t Skip the Risk Analysis

According to associate attorney Jefferson Lin in a blog posting for the Seattle-based law firm Ogden Murphy Wallace Attorneys, the CAP for each provider requires both entities to:

- Conduct a comprehensive and thorough risk analysis;
- Develop and implement a risk management plan;
- Review and revise policies and procedures on information-access management, as well as device and media controls;
- Develop an enhanced privacy and security awareness training program;
- Provide progress reports; and Develop a process to evaluate any environmental or operational changes that impact the security of ePHI (CU only)

“This settlement again highlights the necessity for healthcare organizations and business associates to create and implement security policies and procedures, and to engage in a security management process that ensures the security of patient data,” Lin wrote.

Lesson learned: “The message here is to be sure you use good, professional practices in the development and implementation of all systems handling PHI,” stresses Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, VT.


If your company undergoes a HIPAA investigation, will your directors and officers insurance policy cover the costs? Maybe — or maybe not.

Drug-testing company Millennium Laboratories Inc. is facing just such a problem. The laboratory has sued its liability insurer Allied World Assurance Co. (AWAC) for attempting to get out of covering Millennium’s defense costs related to a HIPAA investigation by the U.S. Department of Justice (DOJ) that began in early 2012, Law360 reports.

In May 2014, Millennium and AWAC each filed motions for summary judgment. Millennium argued that AWAC should pay out its $5-million directors’ and officers’ insurance policy to cover the laboratory’s defense costs, Law360 explained. But AWAC stated that certain conditions and exclusions in the policy in the policy bar coverage for the HIPAA investigation, and even if not barred entirely the coverage would be subject to a $100,000 sublimit of liability.

Nevertheless, AWAC has already advanced the $100,000 to Millennium, which is supposed to cover claims for regulatory wrongful acts. But AWAC refuses to pay out the rest of the policy because it alleged that the DOJ investigation doesn’t qualify as a coverage “claim,” and that the coverage is barred because the laboratory had already been on notice of prior actions before the AWAC policy took effect, according to Law360.

Case Study: Don’t Forget About The Privacy And Security Of Your Paper Records

OCR sheds no light on how it calculated the whopping $800,000 penalty

If you’re so caught up in securing all the protected health information (PHI) on your computers, networks and mobile devices that you have started to ignore the paper records in your office, you are making a very costly mistake. As a recent HIPAA breach case demonstrates, the HHS Office for Civil Rights (OCR) isn’t pulling any punches when it comes to paper records.

OCR lowered the boom on community-based healthcare system Parkview Health System, Inc. (serving northeast Indiana and northwest Ohio) following a complaint filed back in June 2010. OCR launched an investigation after receiving the complaint, which was from a retiring physician who alleged that Parkview violated the HIPAA Privacy Rule.

Background: In 2008, Parkview took custody of medical records belonging to approximately 5,000 to 8,000 patients while helping the retiring physician to transition her patients to new providers, according to OCR. Parkview considered purchasing some of the physician’s practice as well.

On June 4, 2009, Parkview employees left 71 cardboard boxes of these medical records unattended in the retiring physician’s driveway when they discovered that she was not at home, OCR states. The medical records were “accessible to unauthorized persons” and “within 20 feet of the public road,” which was “a short distance away from a heavily trafficked public shopping venue.”

What OCR Demands in the CAP

OCR announced on June 23, 2014 that in addition to the $800,000 fine, Parkview agreed to a corrective action plan (CAP). According to attorney Linn Foster Freedman in a June 27 Privacy Alert analysis for the law firm Nixon Peabody LLP, the CAP requires Parkview to:

- Develop, maintain, and revise, as necessary, any written policies and procedures, including addressing non-electronic PHI, and provide them to HHS for approval;
- Distribute the approved policies and procedures to all workforce members who have access to PHI and to new employees within 20 days of starting work;
- Review policies and procedures periodically and promptly update them when operations or regulations change; and
- Develop workforce training and submit it to HHS for approval, and then train all employees, document the training through a dated certification from each workforce member who received training, and train new employees within 20 days of starting work.
Parkview must also notify HHS in writing within 30 days if Parkview determines that a workforce member has violated the policies and procedures, noted associate attorney Jefferson Lin in a June 23 blog posting for the Seattle-based law firm Ogden Murphy Wallace Attorneys. And the settlement agreement requires Parkview to submit to HHS a final report demonstrating compliance with the CAP.

Don’t Ignore Your Security Practices for Paper Records

Sure, this settlement appears to provide the straightforward wisdom: provide proper HIPAA training to all employees and institute proper HIPAA policies and procedures. Or perhaps the simplest lesson is: don’t leave boxes of medical records unattended in someone’s driveway. But experts believe there’s more that you can learn from this case.

Caution: “The settlement is particularly notable because it relates to paper records, which is a departure from OCR’s recent focus on electronic PHI,” pointed out health law attorney Leah Roffman in a June 26 blog posting for the law firm Cooley LLP. And OCR has highlighted that too many complaints stem from improperly discarded or transferred records.

“Organizations should pay careful attention to the transfer and disposal of both electronic and paper patient records,” Lin stressed. And OCR has posted some helpful FAQs regarding HIPAA and the proper disposal of PHI and patient records: www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf. The document answers the following six questions:

What do the HIPAA Privacy and Security Rules require of covered entities (CEs) when they dispose of PHI?

- May a CE dispose of PHI in dumpsters accessible by the public?
- May a CE hire a business associate (BA) to dispose of PHI?
- May a CE reuse or dispose of computers or other electronic media that store electronic PHI?
- How should home health workers or other workforce members of a CE dispose of PHI that they use off of the CE’s premises?
- Does the HIPAA Privacy Rule require CEs to keep patients’ medical records for any period of time?

Beware of Potentially Arbitrary Settlement Amounts

Another interesting aspect of this particular settlement is the seemingly large penalty — inching dangerously close to the $1-million mark. Experts are puzzled at the large settlement amount particularly because the case involved no actual improper access to the PHI.

Watch out: “Although there is no mention that an unauthorized person actually had access to or took any records from the boxes in the driveway, Parkview agreed to pay $800,000 for the violation,” Freedman noted. “There is no guidance on what the settlement amount is based upon or how it was calculated under the HIPAA regulations.”

Bottom line: As more and more breach cases come to light, pay attention to not only the trends in the terms of CAPs, but also the monetary settlement amounts. And hopefully, OCR will become more transparent in how it calculates these penalties.
Enforcement News: How Access Controls And Employee Training Are Key To Preventing Breaches

Plus: Courts, states still unsure how to address data breach lawsuits.

Are the wrong people on your staff accessing protected health information (PHI) that they shouldn’t or that they don’t need to? If so, you could be at risk for an impermissible disclosure blunder.

Rady Children’s Hospital in San Diego announced that it discovered two instances of impermissible disclosure of patient information, both of which arose from Rady employees sending more than 200,000 patients’ PHI to job applicants, reported Elana Zana in a blog posting for the Seattle-based law firm Ogden Murphy Wallace Attorneys. The employees sent spreadsheets containing PHI to job applicants in order to evaluate the applicants’ skill sets.

Zana highlights two HIPAA compliance flaws in particular that arose in this case:

1. Access Controls — The HIPAA Security Rule stresses the importance of both internal and external access controls. You must evaluate who within your organization actually needs access to PHI to perform their job functions. Determining whether access to PHI is appropriate is both a requirement of the HIPAA Security Rule and is a good mitigation tactic to avoid impermissible breaches, such as the one here.

2. Training — Under HIPAA, you are responsible for providing HIPAA Privacy and Security training for all members of your workforce. And the training does not stop with just the initial session; you must provide periodic refresher and update training as well. Providing periodic training updates and reminders, including examples of HIPAA breaches like this one, is very useful in driving home how easily HIPAA breaches can occur, and how expensive they are.

“Avoidance of HIPAA breaches altogether is nearly impossible, but proper access controls and training can help mitigate against breaches such as the one that occurred here,” Zana concluded.

Failure To Allegle Injury Could Nix A Data Breach Lawsuit Against You

If affected patients fail to allege actual injury resulting from a data breach, you might be off the hook for a class action lawsuit — at least, if you’re in Illinois.

Back in July 2013, four unencrypted laptops containing PHI were stolen from Advocate Health and Hospitals Corp. After Advocate notified the affected patients of the breach,
patients filed a class action lawsuit against the organization alleging negligence, violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, invasion of privacy, and intentional infliction of emotional distress, according to a Privacy Alert from the law firm Nixon Peabody LLP.

The Illinois Circuit Court recently ruled against the plaintiffs, deciding to dismiss the case because the plaintiffs were unable to allege or provide evidence that the PHI contained in the laptops was actually accessed, used or sold, Nixon Peabody reported. Further, the court found that the plaintiffs did not satisfy the “injury in fact” requirement to pursue the claims, which meant that they had to allege actual injury.

“This case is in line with the majority of data breach cases, which require plaintiffs to allege actual injury in order to proceed,” stated Linn Foster Freedman, a Providence, RI-based partner with Nixon Peabody, in the Alert. But as more plaintiffs pursue state law claims, “and more courts weigh in on the standing issue, the consistency in this area of law will be in jeopardy.”

**Hacker Incident: Better To Be Safe Than Sorry?**

If you discover that your server has been hacked, but there is no evidence that a hacker actually accessed or used the PHI contained on that server, what should you do?

The Montana Department of Public Health and Human Services was in just such a situation, and it decided to notify 1.3 million individuals of the hacking incident “out of an abundance of caution.” The notified population included individuals who have received services from the state, current and former Department employees, and contractors that have done business with the state, according to a June 27 Nixon Peabody LLP Privacy Alert.

An independent forensic investigation discovered that the Department’s server had indeed been hacked after personnel noticed “suspicious activity,” Nixon Peabody stated. The Department shut down the server on May 22, 2014 and reportedly took steps to strengthen security.

**Posting Of PHI On Facebook Spurs Lawsuit**

What are you posting on social media? Hopefully not protected health information (PHI).

A Facebook posting of Cincinnati-area woman’s medical records has led to a lawsuit against a hospital, according to a June 4 news article on Cincinnati.com. In the lawsuit, plaintiff Shawntelle Turley claims that employees of the University of Cincinnati Medical Center (UCMC) posted a screenshot of her medical record to a Facebook group. The screenshot showed her name and her diagnosis of syphilis.

The UCMC employees who posted Turley’s medical record purportedly did so at the request of her ex-boyfriend. Turley is seeking more than $25,000 in damages for invasion of privacy, emotional distress, malice, and negligence.
You Could Get A Prison Sentence For HIPAA Violations

A relatively new development is terrorizing healthcare providers — criminal charges stemming from violating HIPAA.


During that time, Hippler worked for an East Texas hospital and allegedly accessed protected health information (PHI) with the intent to use the information for personal gain, announced U.S. Attorney John M. Bales.

The criminal charges came about after HHS Office of Inspector General (OIG) agents conducted an investigation into the purported HIPAA violation. If convicted, Hippler could face up to 10 years in prison.
Case Study: Learn 4 Lessons To Secure Your Backup Tapes

*Delayed breach reporting can get you into even more hot water.*

For HIPAA compliance, it may seem like you’re encrypting everything these days — from emails to laptops and other devices. But if you aren’t also encrypting your data backup tapes, you’re opening up your organization to a potentially serious breach risk. Here’s how one hospital learned this lesson the hard way.

Background: On July 22, 2014 *Women & Infants Hospital of Rhode Island* (WIH) agreed to a consent judgment involving a $150,000 payment to resolve HIPAA breach allegations, according to an announcement by the *Massachusetts Attorney General’s* (AG’s) Office. The judgment resulted from a data breach that WIH reported to the AG’s Office in November 2012.

The data breach exposed patients’ names, dates of birth, Social Security numbers, exam dates, physicians’ names, and ultrasound images. WIH has agreed to pay a $110,000 civil penalty, $25,000 for attorneys’ fees and costs, and a $15,000 payment toward the AG Office’s fund for education and future data security litigation. WIH also agreed to perform a review and audit of its security measures and to take any corrective measures recommended in the review, the AG Office said.

HIPAA expert and director of compliance services for *Lewis Creek Systems LLC* in Charlotte, VT Jim Sheldon-Dean offers the following four lessons that you can learn from this case:

### 1. Encrypt All Your Backup Tapes

In the summer of 2011, WIH shipped backup tapes from two of its Prenatal Diagnostic Centers to a central data center at WIH’s parent company, *Care New England Health System*, according to the AG’s press release. The backup tapes contained the protected health information (PHI) of 12,127 patients from the Centers, which are located in Providence, RI and in New Bedford, Mass.

Then, the parent company was supposed to ship the backup tapes off-site to transfer legacy radiology information to a new picture archiving and communications system. At some point during this shipping process, 19 unencrypted backup tapes went missing.

**Crucial:** One of the most important lessons to glean from this case is that you must encrypt your backup tapes, Sheldon-Dean stresses.
The missing backup tapes may not have posed such a serious HIPAA breach risk if they were encrypted. Unfortunately, WIH failed to encrypt the tapes.

“This case illustrates how important it is to ensure that any protected health information that is transported off site, including backup tapes, are properly protected through encryption or other secure means,” advised attorneys Kathryn Sylvia and Linn Foster Freedman in a blog posting for the law firm Nixon Peabody LLP.

2. Put a Good System in Place to Manage Inventory

**Problem:** WIH had “an inadequate inventory and tracking system,” which contributed to the hospital’s alleged failure to discover that the tapes were missing until nearly one year later, the AG’s Office charged.

**Solution:** “Have a good system for managing your backup tape inventory,” Sheldon-Dean urges.

Under the settlement agreement, WIH agreed to maintain an up-to-date inventory of the locations, custodians and descriptions of unencrypted electronic media and paper patient charts containing PHI.

3. Beware of Transporting Over State Lines

In this case, the missing backup tapes contained PHI from Massachusetts residents, even though the transport originated from locations in both Rhode Island and Massachusetts. Therefore, WIH needed to report the breach to and comply with the breach-notification statute in Massachusetts.

**Pitfall:** “Recognize that you may have issues with other states when you have a breach and your patients are residents of other states,” Sheldon-Dean points out.

4. Don’t Drag Your Feet on Breach Reporting

What made matters even worse for WIH was the fact that the hospital failed to report the breach in a timely manner, Sheldon-Dean notes. Although the breach occurred in the summer of 2011, WIH didn’t discover it until the following spring. Then, the hospital didn’t report the breach until November 2012.

The AG’s Office pointed to “deficient employee training and internal policies” as the cause of WIH’s delay in properly reporting the breach.

**Bottom line:** And here’s Sheldon-Dean’s fourth lesson: “Don’t delay reporting your breaches properly — have a solid process!”
Lawsuits: How Potential Precedent-Setting Court Ruling Is Good News For You

Could this court decision affect breach lawsuits beyond California?

In a major HIPAA-breach lawsuit, an appellate court recently decided that “the mere possession” of protected health information (PHI) was not enough to warrant damages. Here’s why this ruling could set the pace for future court decisions in breach-related lawsuits.

**Background:** A data breach occurred when a computer was stolen from Sutter Health. The computer contained the personal and health information of 4.3 million patients. Specifically, the database stored on the computer held the names, addresses, dates of birth, telephone numbers, email addresses, medical record numbers and names of health insurance plans for 3.3 million patients. And the computer contained dates of service and descriptions of diagnoses for another 1 million individuals.

**Watch Out: State Laws Can Inflate Damage Amounts**

After Sutter Health notified patients of the computer theft, they filed a class action lawsuit under the California Confidentiality of Medical Information Act. The Act allowed for statutory damages of up to $1,000 per individual — that’s a whopping $4.3 billion in damages.

The lower court decided that Sutter Health was liable under the Act, and Sutter Health appealed the ruling. On July 21, 2014 the California appeals court reversed the decision and dismissed the case, holding that Sutter Health could not have violated the Act “because there was no evidence that the thief who stole the computer had actually viewed any of the information,” explained partner attorney Linn Foster Freedman in a blog posting for the law firm Nixon Peabody LLP.

“The plaintiffs failed to state a cause of action under the Confidentiality Act because they failed to allege a breach of confidentiality,” the appellate court ruled. “Therefore, the trial court should have sustained Sutter Health’s demurrer.”

**Stay Up-To-Date with This Lawsuit Trend**

“This is a significant decision that is consistent with many other jurisdictions that the mere loss of information does not form the basis for a claim for monetary damages,” Freedman said.

And the dismissal could set a precedent in California, reported Kathy Robertson, senior staff writer for the Sacramento Business Journal, in a news report. “As data breaches become more common, courts are beginning to look at the actual toll from the incidents and question whether a theft that doesn’t hurt anybody should bring multimillion-dollar damage awards.”
This potential precedent is especially true in light of another appeals court ruling in a University of California Regents case last year, which came to the same conclusion, Robertson noted.

“As the court said, it's called the ‘Confidentiality of Medical Information Act,’ not the ‘Possession of Medical Information Act,’” Dallas-based partner attorney Jeffrey Drummond said in a July 23 Jackson Walker LLP blog posting. “Loss of peace of mind apparently isn't a damage.”

Takeaway: But Drummond suspects that “nothing will be settled here until the California Supreme Court (and possibly the U.S. Supreme Court) rules.”
Theft Risk Is Always Present: Encrypt All Laptops

Even when a stolen laptop ends up in the bottom of a lake, if you didn’t encrypt the device you’re sunk.

Case in point: Two intruders broke into the facilities of South Carolina-based Self Regional Healthcare over the Memorial Day weekend last year and stole an unencrypted laptop containing 39,000 patient records, reported partner attorney Linn Foster Freedman in a blog posting for the law firm Nixon Peabody LLP.

Law enforcement later arrested the intruders, who admitted to the break-in and theft but claimed they never accessed the information on the laptop and dumped the laptop in a nearby lake, Freedman said. Divers were unable to locate the laptop. Because the laptop was unencrypted and not recovered, the hospital elected to notify the affected patients.

“The incident reiterates that removable media like laptops should be encrypted at all times — when they are within a locked premises, as well as when they are removed from the facility — as the risk of theft is always present,” Freedman warned.
Case Study: Watch Out For Sophisticated Malware Breaching Your Systems From Overseas

Pay attention: Massive breach teaches you four crucial lessons.

The latest HIPAA breach is the largest ever, affecting millions of patients across more than half of the United States. And this is the type of breach that strikes fear into the hearts of many healthcare providers — find out why and what you can do right now to avoid the same disaster.

Background: Tennessee-based Community Health Systems, Inc. (CHS) has reported the breach of approximately 4.5 million patients’ personal information, including patient names, addresses, Social Security numbers, telephone numbers and birthdates. The hackers accessed the patient records in the CHS system in April and June 2014. The affected patient population spans 28 states.

Keep in Mind HIPAA’s Wide PHI Definition

“Although the breached records do not contain the details of the patients’ treatment at CHS’ hospitals, the identifying information in the records still meets the HIPAA definition of ‘protected health information’ [PHI],” noted attorney Casey Moriarty in an Aug. 19 Ogden Murphy Wallace Attorneys health law blog posting. “Therefore, CHS will have to follow the HIPAA breach notification requirements.”

The hackers were an “Advanced Persistent Threat” Chinese group that used highly sophisticated malware and technology to attack CHS’ systems, bypassing the security measures in place, reported partner attorney Linn Foster Freedman in a privacy alert posting for the law firm Nixon Peabody LLP. Then, the hacker group copied and transferred the patient data outside CHS.

‘Heartbleed’ Bug Strikes Again?

“The technology is rumored to be the ‘Heartbleed’ bug,” Freedman noted. Federal authorities identified the hacker group as typically seeking valuable intellectual property, such as medical device development data. But in this case, the group accessed non-medical patient data related to physician practice operations.

CHS first reported the breach to the Securities and Exchange Commission (SEC) and has hired the data security firm Mandiant to investigate the breach. CHS is also in the process of notifying the affected patients.
But because the data involved in the incident falls under HIPAA, CHS must also report the breach to the **HHS Office for Civil Rights (OCR)**, pursuant to the Health Information for Technology and Clinical Health Act (HITECH), Freedman stated. And once CHS does so, this breach will become “the largest HIPAA breach reported to the OCR since HITECH was enacted in 2009."

**Follow 4 Expert Tips to Prevent This Type of Breach**

This type of massive, sophisticated data breach may seem impossible to prevent — but you can actually avoid it by taking a few simple steps. Moriarty offered the following tips:

1. **Safeguard & Educate**: This large breach is yet another reminder to safeguard your electronic systems and educate your staff members on security policies and procedures.

2. **Watch Staff Emails**: The type of malware that caused this breach is relatively easy to overlook. A staff member who clicks on a link in an email or responds to an email from hackers who pose as security personnel could result in unknowingly installing the malware.

3. **Use Encryption**: Consider employing encryption technology that meets the HIPAA breach safe-harbor standards to avoid or mitigate this type of breach.

4. **Check with IT**: When staff members are in doubt about a suspicious email, phone call or other communication, instruct them to always check with your information technology (IT) personnel and your HIPAA Privacy Officer before taking any action.

**FBI: How Your IT Personnel Can Thwart This Attack**

The threat of this type of breach is growing exponentially — so much so in fact that the **Federal Bureau of Investigation (FBI)** recently released an alert. The alert states that the FBI has “observed malicious actors targeting healthcare related systems,” possibly to obtain PHI or Personally Identifiable Information (PII).

“These actors have also been seen targeting multiple companies in the healthcare and medical device industry, typically targeting valuable intellectual property, such as medical device and equipment development data,” the FBI warns. “Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware.”

The FBI goes on to detail two main indicators of a possible compromise to your IT systems:

1. **Network-Based Indicator.** Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36.

2. **Host-Based Indicator.** The malware runs as a Windows service “RasWmi (Remote Access Service)” from the malicious .dll C:\Windows\system32\wbem\raswmi.dll. The implant is installed from an executable file *(the file has been observed under a variety of names)* which drops the raswmi.dll file into the same directory and sets it to run as a service.
Ask Yourself 5 Questions To Gauge Your Breach Vulnerabilities

Tip: Look for all opportunities to encrypt PHI in your organization.

Although many industry experts might argue that a healthcare provider is never fully protected from hackers and data thieves, there are so many things that your organization can do to protect against a messy HIPAA breach. Are you doing everything you can to protect against a data breach?

In an article published in The National Law Review, Godfrey & Kahn S.C. attorneys Thomas Shorter, Douglas Poland and Scott Thill provide the following questions that you should ask about your organization in light of the recent Community Health Systems, Inc. breach:

1. **When did we last review and update our HIPAA security measures?** When did you last perform a risk analysis? Does your organization maintain sufficient security logs and malware detection software, and employ other resources to identify external attacks and intrusions on your system?

2. **Have we identified all areas in our organization where we may receive or maintain PHI?** Has your organization implemented a mobile device policy? Has your organization addressed the use of USB drives, CDs and other portable media?

3. **Have we identified all access points to our systems containing PHI?** Has your organization reviewed its networked devices for potential vulnerabilities that may allow an intruder to bypass your security? Are there additional opportunities to encrypt PHI within our organization?

4. **Do we have sufficient cyber or other liability insurance to cover breaches of PHI?** Will your organization’s existing insurance cover the expenses related to a breach and, if not, should you procure such insurance?

5. **Even though we have addressed HIPAA’s requirements, should we do more?** Does your organization have opportunities for additional protection that are feasible?
Enforcement News: How Data Breach Settlement Sets ‘Unfortunate Precedent’

*Plus: How your BAs can get you into a big breach mess.*

Forget a class action lawsuit under HIPAA — some plaintiffs are filing lawsuits (*and winning settlements*) against healthcare providers for data breaches under a variety of other federal and state laws.

After the billing vouchers of more than 13,000 patients went missing from an off-site storage vendor, plaintiffs filed a class action lawsuit against the *University of Miami Health System* (UMHS). The vouchers came from patient records from the health system’s Department of Otolaryngology and included patients’ names, dates of birth, Social Security numbers, physician names, insurance company names, medical record numbers, and procedure and diagnostic codes.

UMHS recently requested that a Florida judge approve a proposed settlement in the class action lawsuit, according to partner attorney *Linn Foster Freedman* in a privacy alert posting for the law firm *Nixon Peabody LLP*. Under the settlement agreement, UMHS would pay $100,000 in individual claims, $90,000 in attorneys’ fees, and $1,500 to the named plaintiff. UMHS would also conduct risk assessments and remediation.

What’s especially curious about this lawsuit is that the plaintiff filed the action under the Fair Credit Reporting Act (FCRA) and Florida state law, alleging that she suffered financial harm because money was withdrawn from her bank account following the breach, Freedman stated. “This is the first time we have seen a settlement by a health system for a data breach under the FCRA, nor do we see how the FCRA can be relevant to the facts of this case.”

Moreover, patients’ financial information does not appear to have been included in the breached data from the billing vouchers.

**Warning:** “This settlement is an unfortunate precedent on two levels — first, it appears to be a settlement under the FCRA, which is a first to our knowledge,” Freedman stated. “And second, it is a settlement of a case where there does not appear to be any relationship between the data breach and the alleged harm and where the attorneys received almost as much as the settlement on the merits.”

**Bottom line:** “Opening these doors in the data breach arena is discouraging,” Freedman concluded.
Breach Risk: Keep A Close Watch On Your BAs

Using third-party vendors is always a concern when it comes to handling protected health information (PHI) and other personal or financial information. So here’s yet another case to inspire you to make sure that your business associates (BAs) are keeping your patients’ data safe and secure.

Hackers accessed the computer systems of Onsite Health Diagnostics, a third-party vendor that Tennessee uses to store information on its state employees, WSMV reported. The hackers stole data on more than 60,000 state workers contained in a data table that included personal information belonging to members who participate in wellness screenings as part of the health plan.

Although the Tennessee Benefits Administration (TBA) claims that the hackers did not access any Social Security numbers, financial information or medical information, they did obtain individuals’ email addresses, phone numbers, addresses, genders and dates of birth.

No identity thefts have occurred so far related to this data breach, but Onsite is offering affected individuals free identity theft protection. TBA blamed the breach on Onsite’s “old computer system,” but said that the vendor now has a new computer system in place with new securities, according to WSMV.

Hackers Attack ‘Obamacare’ Website

If hackers can attack a huge federal government website using relatively low-tech means, how can you be sure that your systems are safe?

On Sept. 4, 2014 the Obama Administration reported that a hacker had breached the Healthcare.gov website, reported the New York Times. Although investigators found no evidence that the hacker had taken or viewed users’ personal data, this breach is nonetheless worrisome for the security of the online federal health exchange.

The Administration claims that the hacking incident was “an intrusion on a test server” that contained no consumer personal information and that the Healthcare.gov website was not even specifically targeted, according to the Times. The test server was connected to the Internet in error, its manufacturer-default password was unchanged, and it was not subject to regular security scans.

Federal employees noticed the breach on Aug. 25, 2014. Hackers downloaded malware onto the test server intended as a broader denial-of-service attack that would shut down other websites.
Don’t Let Terminated Employees Sneak Out With Patients’ PHI

Yet another HIPAA breach reinforces all the crucial reasons why you should encrypt all mobile devices and portable data storage, as well as why you must keep a close watch over what employees — and former employees — take home with them.

A home burglary sparked a breach incident for St. Elizabeth’s Medical Center in Brighton, Mass., after thieves stole a former employee’s laptop and USB thumb drive that both contained 595 patients’ protected health information (PHI), according to an Aug. 29 blog posting for the law firm Nixon Peabody LLP by attorney Kathryn Sylvia. The laptop and thumb drive were not encrypted and contained patients’ dates of birth, medical history, diagnoses, test results and medications.

The patients received treatment at St. Elizabeth’s Center for Breast Care or the hospital’s hematology/oncology department sometime from May 14, 2011 through Jan. 31, 2014. The former employee was a physician at St. Elizabeth’s.

St. Elizabeth’s does not allow storage of unencrypted PHI. Although St. Elizabeth’s has reported the theft to affected patients and officials do not believe that the thieves have misused the PHI, local police are still investigating the incident, Sylvia noted.

Takeaway: “This should be a lesson for health care facilities and hospitals to ensure that, upon termination, all employees return electronic patient data and all hard drives or USB thumb drives are wiped clean to avoid situations like this,” Sylvia stressed.

Why You Could Be Protected From State Law HIPAA-Breach Claims

HIPAA breach lawsuits are still in an uncertain territory when it comes to filing claims under state laws. But many states, like Illinois, are holding fast to the idea that if the plaintiffs cannot prove actual harm from a data breach, they don’t have a leg to stand on.

Case in point: In August 2013, Advocate Health & Hospitals Corporation reported a large data breach after four laptops were stolen from an Advocate medical group administrative building. The laptops contained unencrypted protected health information (PHI) of more than 4 million patients.

Following the breach, two patients filed a class action lawsuit alleging negligence, violation of the Illinois Personal Information Protection Act, violation of the Illinois Consumer Fraud Act, invasion of privacy, and failure to take necessary steps to safeguard patients’ PHI, according to a Sept. 5 Health Law Rx blog posting by healthcare attorney Carolyn Metnick for the law firm Akerman LLP.
But on July 10, the Kane County Circuit Court in Illinois granted Advocate’s motion to dismiss the claims for lack of standing and failure to state a claim, Metnick reported. “The court held that the plaintiffs lacked standing because they could not prove that the information stolen had been accessed or used, and therefore, they could not prove that there had been actual identity theft or harm.”

Although the court conceded that an increased risk of harm existed due to the laptops’ theft and potential accessibility of the unsecured PHI, the thieves would actually need to disclose, sell or otherwise misuse the PHI for the lawsuit claims to be valid.

“This case is an example of the challenges in bringing claims under state law for HIPAA data breaches,” Metnick explained. “Because most, if not all, states require that plaintiffs show actual injury to state a sufficient claim, plaintiffs often must overcome a high hurdle because they cannot show that their PHI was used to commit identity theft or other harm.”

**Caveat:** “Even though state causes of action may be difficult to prove, covered entities and business associates face penalties under HIPAA,” Metnick warned. “Also, although difficult, state causes of action are still a risk.”
Case Study: Don’t Overlook Data Breach Risks From Desktop Thefts

Are you including desktop computers in your security risk assessment?

No healthcare provider is immune from theft. And although you hear a lot lately about laptop thefts leading to HIPAA breaches, desktop computers are at risk as well. Are you taking the right precautions to protect all your computers?

**Background:** The theft of an unencrypted desktop computer during a break-in at a Temple University Physicians medical office in Philadelphia, PA resulted in the breach of 3,780 patients’ protected health information (PHI). The theft occurred sometime between July 18 and July 21, 2014, according to Temple’s breach notification to the HHS Office for Civil Rights (OCR).

The desktop computer was in the surgery department and contained files with PHI including names, ages, billing codes and referring physicians’ names, reports the Philadelphia Inquirer. Temple claimed that the files did not contain financial information nor Social Security numbers.

**Take the Right Steps in Breach Response**

Correctly, Temple immediately reported the theft to local police, HHS, and the affected patients. So far, Temple is providing free identity theft-monitoring services to all affected patients for the next 12 months.

Temple also plans to beef up its employee training, improve physical security, and boost technical security measures on desktop computers, according to the healthcare system. Unfortunately, the desktop was not encrypted.

**What You Can Learn from This Breach**

“Time and again data breaches are caused by the loss or theft of a laptop computer, but it is less common that a desktop is stolen that compromises health information,” said partner attorney Linn Foster Freedman in a blog posting for the law firm Nixon Peabody LLP.

**Lesson learned:** You should include desktop computers in your security risk assessments, “as the risk of theft of desktop computers is real, which is apparent from this incident,” Freedman warned. “It is a reminder that all computers are a security risk for an organization and proper security measures for all media — removable or otherwise — is essential.”
Enforcement News: Can PHI Really End Up On Google? Yes, This Happened

Yet another data breach serves as a warning to mind your business associates (BAs) and third-party vendors.

Case in point: Huntsville, AL-based Diatherix Laboratories recently notified more than 7,000 of its U.S. clients that their protected health information (PHI) was unsecured for nearly three years, according to a Sept. 24 blog posting by Dallas-based Entrust. Although the breach first occurred back in September 2011, Diatherix didn’t discover it until July 2014.

Specifically, the PHI included patients’ lab test results, which became publicly accessible through Google when Diatherix’s billing contractor, Diamond Computing Company, accidentally allowed the PHI to become accessible on the Internet. In addition to test results, patients’ exposed records also included patient addresses, Social Security numbers, diagnoses, and more, Entrust reported.

How New State Data-Breach Laws Could Cause HIPAA Compliance Confusion

A new state law in Florida that became effective on July 1 has continued the trend of stricter data breach state laws. And Florida is the newest state to enact a breach statute that conflicts in key ways with the federal HIPAA law.

The new Florida law, the Florida Information Protection Act (FIPA) replaces the state’s breach notification requirements and expands Florida’s reach and enforcement, said Maryland-based partner attorney Emily Wein in a recent analysis for Ober Kaler Attorneys at Law. FIPA is yet another law that reinforces a trend of states enacting their own data breach and notification laws that expand beyond the scope of the federal requirements under HIPAA.

Under FIPA, in the event of a breach, covered entities (CEs) must provide affected individuals with a notice that meets the statute’s requirements within 30 days after the breach determination or reason to believe a breach occurred, Wein explained. But this requirement conflicts with federal HIPAA requirements — under HIPAA, providers have 60 days to provide notice.

Trap: “The question raised is whether HIPAA [CEs] in Florida continue to have the 60-day timeframe or 30-day timeframe,” Wein pointed out. “Answering that question requires a determination of whether HIPAA’s longer notice period would be preempted by FIPA’s more stringent 30-day timeframe.”

FIPA differs from HIPAA in a few other important ways. For example, FIPA requires CEs and their third parties to institute reasonable security measures but falls short of providing detail on what that means. HIPAA, on the other hand, has more specific security requirements, which Florida providers must still follow.
Also, FIPA requires some compliance by a CE’s third-party agent, but the statute does not actually make that third party individually liable under FIPA like business associates are under HIPAA, Wein stated. And FIPA’s penalties for not providing proper notice are assessed per breach, not per affected individual, but the statute doesn’t say whether state regulators will also take into account the specific facts of each situation in assessing total penalties like HIPAA does.

To read the new Florida statute (Fl. Stat. § 501.171), go to www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html. Or go to www.leg.state.fl.us/statutes/index.cfm and type “501.171” into the search box.

**Why Certain HIPAA Breach-Related Lawsuits Are Failing**

More state courts are requiring actual proof that patients’ information was used for identity theft following a data breach before awarding punitive damages. This time, an Alabama court chimes in.

In February, Alabama-based **Flowers Hospital** determined that one of its employees stole patient records containing patient names, addresses, Social Security numbers, and health insurance information, according to a blog posting by the law firm **Nixon Peabody LLP**. The employee was charged with trafficking in stolen identities, and then five affected patients filed a class action lawsuit against Flowers.

Flowers filed a motion to dismiss the complaint, arguing that the patients “didn’t have standing to sue based merely on an increased likelihood of identity theft in the future,” Nixon Peabody related. In response, the judge ordered the patients to file a Second Amended Complaint to show evidence that a third party used their Social Security numbers to file false tax returns as they alleged.

**Bottom line:** “Clearly, if the plaintiffs can show that their identities were actually stolen and used to file false tax returns as a direct result of the breach at Flowers Hospital, the Motion to Dismiss will be jeopardized,” Nixon Peabody concluded.
Case Study: Understand HIPAA’s Evolving Impact On Med Mal Lawsuits

*Decision point: Courts look to preemption provisions in the HIPAA regs.*

Patients in Florida can’t “have their cake and eat it too” when it comes to HIPAA privacy protections and medical malpractice lawsuits. So says the U.S. Court of Appeals for the Eleventh Circuit.

**Background:** Plaintiff-appellee Glen Murphy received medical treatment from defendant-appellant Dr. Adolfo Dulay. When Murphy was unsatisfied with Dr. Dulay’s care, he thought about suing the doctor for medical negligence.

**How Med Mal Lawsuit Rules Challenge HIPAA Privacy**

A Florida medical malpractice pre-lawsuit authorization law requires the plaintiff patient to authorize the release of their protected health information (PHI) before suing a medical provider for negligence, explained attorneys Thomas Range and Elizabeth Hodge in an analysis for the law firm Akerman LLP.

The Florida law requires that the presuit notice of intent to initiate a medical malpractice action must also include the authorization for both sides to access the plaintiff’s PHI as it relates to the case.

“This authorization will allow a defendant, or his or her attorney, to interview a plaintiff’s treating providers regarding the plaintiff’s alleged injury without the presence of the plaintiff or the plaintiff’s attorney,” Range and Hodge explained. If the presuit notice doesn’t include the authorization, the presuit notice is void.

But Murphy alleged that the state law conflicted with HIPAA’s privacy requirements and that the provision was coercive, according to a blog posting by partner attorney Linn Foster Freedman of the law firm Nixon Peabody LLP. The lower court sided with Murphy, agreeing that requiring plaintiffs to sign the authorization before being able to proceed with a malpractice case doesn’t give the plaintiff meaningful choices about who can access his PHI.

When Dr. Dulay appealed the decision, the Eleventh Circuit overturned the decision, finding that the Florida law is consistent with HIPAA disclosure requirements, Freedman reported.

**Impact:** Medical malpractice defendants will now have the same access as plaintiffs to treating providers, “but it remains to be seen whether treating providers will agree to ex parte interviews with defense lawyers,” Range and Hodge said.
Look to Preemption for the Answer

“HIPAA specifically states that state law that is more stringent in protecting an individual’s [PHI] preempts HIPAA, and covered entities and business associates are required to follow the more stringent law,” Freedman explained.

The appellate court found that the Florida law was clearly less stringent than HIPAA. The written authorization form required by Florida statute “is fully compliant with the HIPAA statute and its regulations, and the state and federal law are not in conflict,” the court wrote.

**Takeaway:** Courts have upheld similar laws in Tennessee and Texas, Freedman noted. And as long as a state law doesn’t conflict with, and is less stringent than, the federal HIPAA statute, courts will continue to uphold these types of laws in medical malpractice cases.
Enforcement News: How You Can Overcome HIPAA Lawsuits Based On ‘Speculative’ Claims

Plus: Breach impact grows by leaps and bounds over time for Cedars-Sinai.

More and more courts are dismissing lawsuits involving HIPAA breaches when the plaintiffs cannot prove that their personal information was actually used. Here’s yet another case with a similar outcome.

In 2012, Alere Home Monitoring Inc. suffered a data breach when a password-protected laptop was stolen from an employee’s vehicle, according to a blog posting by partner attorney Linn Foster Freedman of the law firm Nixon Peabody LLP. The laptop contained 116,000 patients’ names, addresses, birthdates, Social Security numbers and diagnosis codes.

Following the breach, patients filed a putative class action lawsuit against Alere, alleging negligence and unjust enrichment, as well as violations of the Fair Credit Reporting Act (FCRA), the Unfair Competition Law and the California Medical Information Act, Freedman reported. Alere asked the California court to dismiss the claims.

The court agreed with Alere, dismissing the claims because the plaintiffs couldn’t prove that Alere is a credit reporting agency under the FCRA and that the information release constituted a loss of property. Alere claimed that the only damages alleged were for risk of identity theft and wrongful use of medical information, and invasion of privacy — all of which were “speculative” claims, Freedman noted.

Bottom line: “This decision is consistent with many other similar cases, so it appears that this area of the law is becoming more and more well-settled,” Freedman said.

Breach Aftermath: Time Is Not Always On Your Side

As the months tick by after a HIPAA breach, you might think that you’re getting more and more breathing room from a bad situation. But that’s not always the case — the passage of time can actually reveal that a breach was in fact much bigger than you first thought.

Case in point: When Cedars-Sinai Medical Center reported a data breach of patient records this past summer, the count of affected individuals was at least 500 patients. But after recently consulting a data forensics firm, the hospital has increased the number of affected patients to a whopping 33,136, according to an article in the Los Angeles Times.

The breach occurred when burglars stole a laptop from a Cedars-Sinai employee’s home. Although the laptop was password-protected, it didn’t have additional encryption software to
further protect the patient data contained on the laptop. The laptop was never recovered and law enforcement hasn’t made any arrests in connection with the burglary.

**Don’t Let Your Patients’ PHI Blow In The Wind**

If you needed another reason to ensure that your business associates are HIPAA-compliant in the face of a breach incident, here’s one for you.

On Oct. 23, 2014 potentially thousands of medical records flew out of the back of a truck in southwest Omaha, NE, according to *KETV Omaha*. The truck, owned by Lincoln, NE-based Medi-Waste Disposal, was carrying paper medical records to a disposal and storage site. The back door of the truck wasn’t latched and the papers flew out the back as the truck traveled down the road.

Good Samaritans and volunteers attempted to retrieve the records as the papers blew around the roadside, and Medi-Waste believes they recovered all documents, *KETV* reported. Medi-Waste has promised to establish new checks and balances to secure documents better in the future.
Case Study: Don’t Cut Any Corners In Your Security Rule Compliance Practices

*The road to a data breach is riddled with (fixable) security potholes.*

Taking a lax approach to your security policies and procedures — especially your risk assessments — will only lead to disaster. And if you’re running outdated software and not applying appropriate patches, you’re practically guaranteeing that you’ll suffer a harmful data breach of your patients’ electronic protected health information (ePHI).

**Case in point:** Following a breach of 2,743 individuals’ ePHI, Anchorage Community Mental Health Services (ACMHS) has reached a HIPAA settlement with the HHS Office for Civil Rights (OCR), according to an OCR announcement. ACMHS is a five-facility behavioral healthcare organization based in Anchorage, Alaska.

ACHMS will pay out $150,000 and adopt a corrective action plan to fix deficiencies in its HIPAA compliance program. Also under the Resolution Agreement, ACHMS must report to OCR on the state of its compliance for the next two years.

OCR attributed the breach to ACMHS’ failure to implement good security processes and regularly update their IT resources with available patches, as well as the fact that it was running outdated, unsupported software. Here’s what you can learn from this breach.

**Don’t Take a ‘One-Size-Fits-All’ Approach**

**Problem #1:** OCR’s investigation revealed that ACMHS adopted sample Security Rule policies in 2005, but didn’t follow them.

“Simply having in place template Security Rule policies and procedures is insufficient to satisfy the requirements of the HIPAA Security Rule and to ultimately secure ePHI,” warned Seattle-based associate attorney Elana Zana in a blog posting for Ogden Murphy Wallace Attorneys. You need to tailor security policies to the actual information security infrastructure you have in place at your organization.

“The ACMHS settlement underscores that Security Rule compliance cannot be accomplished with a one-size-fits-all, ‘check the box’ approach,” noted Boston-based associate attorney Kate Stewart in an analysis for the law firm Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

Remember: The Security Rule allows flexibility when choosing which tools to use to protect ePHI, but requires you to actually evaluate your infrastructure to make these decisions, Zana stressed.
Make Security Risk Assessment Your Best Friend

Problem #2: ACMHS failed to identify and address basic risks by conducting a thorough risk assessment, and did not implement security measures to reduce risks and vulnerabilities to its ePHI, OCR charged.

You must evaluate your security policies and procedures, and conduct a security risk assessment on your actual system, at least annually, Zana advised. The process of drafting the security policies and procedures, as well as conducting the security risk assessment, will help you to identify vulnerabilities, evaluate security options, and ultimately safeguard your ePHI.

“OCR has repeatedly emphasized the importance of conducting risk assessments and continuing to update and revise risk assessments based on new threats,” Stewart noted. This was a key takeaway from the Joint OCR/NIST HIPAA Security Conference held in September, and was highlighted by OCR’s release of a Security Risk Assessment Tool earlier this year (www.healthit.gov/providers-professionals/security-risk-assessment).

Patch, Repair & Update

Problem #3: ACMHS failed to “ensure that firewalls were in place with threat identification monitoring of inbound and outbound traffic, and that information technology resources were both supported and regularly updated with available patches,” OCR stated.

“Like Community Health Systems, which reported a breach of 4.5 million patient records due to Chinese hackers targeting a 'heartbleed' vulnerability, ACMHS is finding out the hard way the importance of software patching and updating,” Zana said. “Staying up to date on security patches and software updates is not an easy task, but an important one considering that hackers are exploiting these vulnerabilities.”

“Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis,” OCR Director Jocelyn Samuels said in the announcement. “This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks.”

Link: You can read ACMHS’ Resolution Agreement at www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/amchs-capsettlement.pdf.
Learn 7 Big Lessons From HIPAA Breaches

Tip: Don’t forget about physical safeguards for your paper records.

Data breaches and exposure of protected health information seems to be happening on nearly a daily basis all over the United States. But what should you be learning from these breaches?

Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT, offers the following key lessons and quick tips for compliance:

1. Data Encryption — Encrypt data at rest on any desktop or portable device/media storing electronic PHI (ePHI).

2. Safeguards — Have clear and well-documented administrative and physical safeguards on the storage devices and removable media that handle ePHI.

3. Security Awareness — Raise the security awareness of workforce members and managers to promote good data stewardship. Make sure your staffers are well trained on what to do and what not to do.

4. Double-Check Before Sending — Make sure you have the right fax number, email address or postal address before sending PHI. Check your fax numbers on a regular basis, at least once per year, to ensure that the fax number you’re using is correct. If you don’t verify the fax number, who knows where that fax will end up?

5. Paper Records — Do not neglect physical safeguards for areas where paper records are stored or used.

6. Alternative Storage — Reduce risk through network or enterprise storage as an alternative to local devices.

7. Internal Audit — Monitor and audit your systems so you know what’s going on.
Enforcement News: When HIPAA Trumps State Law Privacy Claims

Plus: Identity theft hackers could open you up to an investigation by the IRS and FBI.

Like many other providers, you've been able to rest easy knowing that a specific section in the HIPAA regulations prohibits a private right of action to sue for a HIPAA violation. But some state courts are allowing plaintiffs to use state law claims to circumvent this federal HIPAA prohibition. Has your state jumped on the bandwagon?

Emily Byrne sought treatment at the Avery Center for Obstetrics and Gynecology, P.C., which provided her with its Notice of Privacy Practices (NPP). Avery's NPP included a description of protected health information (PHI) that the provider could disclose without her authorization in certain circumstances, reported partner attorney Linn Foster Freedman in an analysis for the law firm Nixon Peabody LLP.

Byrne specifically instructed Avery not to disclose her PHI to Andrew Mandoza, a man with whom she had a relationship. In response to a subpoena from Mandoza in a paternity action, Avery mailed a copy of Byrne's medical file to the court. Avery failed to notify Byrne of the subpoena and didn't file a motion to quash.

Mandoza reviewed Byrne's medical record, and then Byrne moved to seal her medical file. Byrne claimed that she suffered harassment and extortion due to Mandoza's review of her medical records, Freeman said. Byrne filed a lawsuit against Avery for breach of contract (the NPP), negligence, and violations of a Connecticut statute and HIPAA.

The lower court ruled that HIPAA preempted negligence claims under Connecticut state law and that the state law claim was not more stringent than HIPAA. The court stated that HIPAA "preempts any action dealing with confidentiality/privacy of medical information" and that it is "well settled … that HIPAA does not create a private right of action, requiring claims of violations instead to be raised through the department's (OCR) administrative channels.

Not so fast: Byrne appealed the decision to the Connecticut Supreme Court, arguing that although there is no private right of action under HIPAA, she was not asserting a claim for a HIPAA violation — instead, she was asserting common law negligence actions with HIPAA guiding the standard of care, Freeman explained.

The Connecticut Supreme Court agreed with Byrne, noting that it was not deciding whether the state's common law allows a plaintiff relief against a healthcare provider for breaching its confidentiality duty by responding to a subpoena, Freeman said. But assuming that the law does allow this, the court decided that HIPAA does not preempt the action and that federal regulations may inform the applicable standard of care in certain circumstances.
The court decided that neither HIPAA nor its implementing regulations intend to preempt state law court actions stemming from the unauthorized release of a plaintiff’s medical records, Freedman noted. “As a result of this holding, Connecticut joined Missouri, West Virginia and North Carolina in chipping away the private right of action preclusion in HIPAA.”

Watch out: “We will continue to see plaintiffs attempt to argue that state law negligence and privacy claims are not preempted by HIPAA in order to bring claims for data breaches and other HIPAA violations,” Freedman warned. “Covered entities and business associates, particularly in the states of Connecticut, Missouri, West Virginia and North Carolina, should take note.”

Beware Of Identity Theft Rings Stealing Your Patient Data
They might not be looking for medical information, but identity theft criminal rings are aggressively seeking your patients’ personal information.

On Nov. 3, 2014 Miami-based Jessie Trice Community Health Center, Inc. (JTCHC) announced that an identity theft criminal operation stole its patients’ personal information. Law enforcement authorities alerted JTCHC of the data breach. The Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) are investigating the breach.

Although the ring did not obtain or compromise any medical records, the theft included 7,888 patients’ names, birth dates, and Social Security numbers. JTCHC notified all the affected patients of the data breach and is working with a data-breach response vendor to help their patients.

JTCHC is also “working vigorously and diligently assessing how to mitigate future risks to all patients and has implemented new procedures and protocols to protect patient information so that this type of theft cannot reoccur,” President and CEO Annie Neasman said in the announcement.

Could ‘Shotgun Pleading’ Protect You From Data Breach Lawsuit?
A “shoddy pleading” could force plaintiffs to redefine their claims against you in a data breach lawsuit, but it won’t necessarily win a bid to dismiss the case altogether.

Alabama-based hospital chain Community Health Systems Inc. (CHSI) and its subsidiaries filed several motions to dismiss claims arising from a massive data breach that affected 4.5 million patients. CHSI claimed that the plaintiffs’ complaints in the lawsuit are classic “shotgun pleadings” and are jumbled, inconsistent, confusing and incoherent, reported Law360.

Patients filed the class action lawsuit against CHSI and its subsidiaries following a data breach earlier this year that allegedly exposed their medical records. In the motions to dismiss, CHSI also argued that it doesn’t directly conduct business in Alabama and has a remote role that is too tenuous to trigger personal jurisdiction, according to Law360.
The defendants also argued that only two of the 21 plaintiffs in the case have alleged that they suffered economic loss due to the data breach, Law360 stated. The judge ordered the plaintiffs to respond to the request for a more definite statement of their claims by Dec. 15, 2014, but the court did not yet set a briefing schedule on the motions to dismiss.

**Precedent Set: Yes, You Are Liable For Employees’ HIPAA Violations**

The *Indiana Court of Appeals* upheld a $1.4-million verdict against *Walgreen* pharmacy chain, potentially setting a national precedent as the first published court decision where a healthcare provider has been held liable for HIPAA violations committed by its employees.

On Nov. 14, 2014 the appeals court affirmed the large jury verdict against Walgreen, reported *The Indiana Lawyer*. The case involved a Walgreen pharmacist, *Audra Withers*, who allegedly disclosed Abigail Hinchy’s prescription history to the customer’s ex-boyfriend *Davion Peterson*. At the time, Withers was involved in a relationship with Peterson.

The appeals court agreed with the trial court’s verdict, which found Walgreen liable for negligent supervision and retention, as well as invasion of privacy. The fact that Walgreen appealed (and lost) means that courts across the United States can rely upon the verdict in holding employers accountable for their employees’ HIPAA violations.
Case Study: Watch Out: Data Breach Litigation Is Getting More Creative

*Missouri court doesn’t care about proving actual damages suffered.*

Attorneys filing class action lawsuits against healthcare entities that have allegedly violated HIPAA don’t seem to be bothered by the fact that no private right of action exists under HIPAA — and apparently, state-level courts aren’t bothered either. This case should serve as a reminder that you’re not always protected from lawsuits based on HIPAA preempting less stringent state laws.

Kansas City, MO-based *Midwest Women’s Healthcare Specialists* (MWHS) recently entered into a settlement agreement and release to settle a class action lawsuit alleging a HIPAA data breach. MWHS agreed to pay out a settlement fund totaling $400,000 for class members, which included an incentive award for the named plaintiffs, attorneys’ fees, and credit monitoring for the affected individuals.

**Don’t Dispose of Records This Way (Obviously)**

**Background:** Back in May 2014, MWHS came under fire for a data breach. Hospital workers dumped MWHS patients’ paper records into an open-topped dumpster on a rather unfortuunately windy day. Many of the paper records blew away in the wind.

The medical records contained patients’ names, addresses, telephone numbers, birth dates, Social Security numbers, insurance information, treatment instructions, doctor’s names, medical procedures, and treatment dates, according to Kansas City’s *KSHB*. A man driving by stopped and gathered about 70 patient records. When the hospital workers walked away instead of collecting the scattered records, the man brought the papers to *KSHB Action News*.

Patient records had blown into a field about one-quarter of a mile away from the medical center. Potentially hundreds of medical records blew out of the dumpster, but the settlement states that the breach affected more than 1,500 patients.

“You would think that it would be common sense not to dump stuff in the dumpster that contained protected health information,” said healthcare attorney *Mary Beth Gettins of Gettins’ Law LLC* in a recent blog posting. “If not for common sense, you would think the fear of facing the chance of paying large sums of money would be a deterrent.”

**Remember:** “Proper disposal of health information is serious,” Gettins stressed. “Under the HIPAA Rule, entities must have policies and procedures for the proper disposal of records and items containing PHI.”
When Proving Actual Damages Suffered Might Not Matter

On behalf of a putative class, two named plaintiffs filed a Petition for Damages and Class Action against MWHS, alleging breach of fiduciary duty under Missouri common law to keep the plaintiffs’ medical information confidential. The complaint argued that the fiduciary duty of privacy that Missouri law imposes “is explicated under the procedures set forth” in the HIPAA Privacy Rule “which requires a covered entity, healthcare provider, to apply appropriate administrative, technical, and physical safeguards to protect the privacy of patient medical records.”

As a result of the improper disclosure of medical information, the plaintiffs alleged that the class members suffered damages, “although the specific alleged damages were not outlined in the complaint,” noted attorney Linn Foster Freedman in a Dec. 19 blog posting for the law firm Nixon Peabody LLP.

Beware of ‘Creative Lawyering’

“This case illustrates the creative lawyering that can follow a data breach,” Freedman cautioned. “It is a mystery how HIPAA ‘explicates’ a fiduciary duty of privacy ‘imposed by Missouri law.’ No Missouri law is cited in the complaint, so what Missouri law is applicable is unexplained.”

Lesson learned: “There is no private right of action under HIPAA, and HIPAA preempts state law that is not more restrictive,” Freedman pointed out. “The precedent of the argument is concerning, but is a clear sign that litigation around data breaches will continue to grow and get more creative.”
Enforcement News: No ‘Present Injury,’ No Grounds For Lawsuit, State Court Says

Plus: Encryption policy does nothing if you don’t actually follow it.

If you’re a healthcare provider in Michigan, you can rest easy knowing that a state appeals court has ruled that unless a plaintiff can prove a “present, actual injury” in a data breach case, awarding damages will be highly unlikely.

On Dec. 18, 2014 the Michigan Court of Appeals shot down a lower court’s ruling that sided with the patients, reported Bloomberg’s Bureau of National Affairs. The appellate court reversed and remanded the lower court’s opinion, ruling that the lower court should have granted summary judgment to Detroit-based Henry Ford Health System (HFHS) in a class action lawsuit.

Background: HFHS contracted with Perry Johnson and Associates Inc. (PJA) for transcription services, according to Bloomberg. PJA’s subcontractor made an error that caused patient records to become available on the Internet.

The online-accessible information included patient names, medical record numbers, and physician notes on patient visits. The named plaintiff in the class action lawsuit claimed her information posted online included diagnoses of alopecia and a sexually transmitted disease.

The lawsuit alleged negligence, breach of contract, and invasion of privacy, Bloomberg reported. The lower court denied HFHS’s and PJA’s summary judgment motions. HFHS and PJA appealed the decision.

Because the plaintiff’s only claim of losses stemmed from costs she incurred for identity theft protection services, the appeals court disagreed with the lower court’s ruling. The appeals court decided that the plaintiff failed to prove that the credit monitoring costs “relate to a present, actual injury.” Further, the plaintiff provided no evidence that anyone actually viewed her PHI on the Internet or used her information for an improper purpose.

Identity theft protection services that the named plaintiff initiated “are not cognizable damages in the absence of present injury,” the appeals court said. Many other courts have also decided that plaintiffs in data breach lawsuits cannot recover credit monitoring services as damages following a data breach where there is no evidence of actual identity theft.

Encrypt Your Mobile Devices — Or Face A Hefty Judgment

Yet another unencrypted laptop has sparked a data breach — and this time, the oversight and other compliance demands outweighed the monetary penalty.
In a Dec. 19, 2014 consent judgment, the Boston Children’s Hospital (BCH) agreed to pay out $40,000 as a result of an alleged data breach that affected more than 2,000 patients, according to an announcement by the Massachusetts Attorney General’s (AG’s) office.

An unencrypted BCH-issued laptop was stolen from a physician while he was at a May 2012 conference in Buenos Aires, the AG reported. The laptop contained the PHI of 2,159 patients, including names, birth dates, diagnoses, procedures, and surgery dates. More than 1,700 of those patients were children under the age of 18.

Despite BCH’s written policies to the contrary, the laptop had no encryption software installed on it prior to the incident. As a result, BCH faced a lawsuit filed under HIPAA and the Massachusetts Consumer Protection Act.

Suffolk Superior Court entered a consent judgment, alleging that BCH failed to protect the PHI of these 2,159 patients, the AG said. The consent judgment ordered BCH to pay a $30,000 civil penalty and $10,000 to a fund for educational programs regarding protecting personal information and PHI.

BCH also must take steps to prevent future security violations and comply with state and federal data security laws and regulations, including tracking, encrypting and physically securing all portable devices, as well as train its workforce on proper handling of PHI. And BCH will continue a review and audit of its security measures, according to the AG.

Another Boston hospital faced an even bigger payout of $100,000, also for failing to protect patients’ PHI when an unencrypted laptop was stolen from a physician’s unlocked office. On Nov. 21, 2014 the Massachusetts AG’s office announced that a court has ordered Beth Israel Deaconess Medical Center (BIDMC) to pay a $70,000 civil penalty, $15,000 in attorneys’ fees, and $15,000 to the AG’s educational fund.

The stolen laptop was the physician’s personal device, but the hospital knew about and authorized its use for hospital-related business. The laptop contained the PHI and personal information of nearly 4,000 patients and employees.

BIDMC’s policy required employees to encrypt and physically secure laptops containing PHI and personal information, but staff were not following these policies, the AG charged. Also, BIDMC did not notify the affected individuals about the data breach until nearly four months after the fact.

In addition to the monetary penalties, BIDMC is facing similar oversight and compliance requirements as BCH.
Hospital Claims HIPAA Violation To Fight Back Against Whistleblowers

If your organization is facing a whistleblower action for violating the False Claims Act, can you accuse the whistleblower employees of violating HIPAA in the course of making their case against you? This hospital thinks so.

Mount Sinai Hospital employees Joseph Gaston and Xiomary Ortiz filed a whistleblower action against the New York City-based hospital, alleging Medicaid fraud, according to a Dec. 22 analysis by Indianapolis-based attorney Norman Tabler, Jr. of the law firm Faegre Baker Daniels LLP.

Gaston and Ortiz claimed that Mount Sinai used “doctor swapping” practices in which one doctor provided services but the hospital billed the services under another doctor’s name, Tabler said. They also accused the hospital of upcoding, billing for services never provided, and billing multiple times for a single service item.

Mount Sinai not only denied the whistleblowers’ allegations, but it also filed a motion against Gaston and Ortiz claiming that they violated patients’ privacy protections under HIPAA by exploiting confidential patient information in order to make the whistleblower case against the hospital.

In other words, Mount Sinai’s position is not that Gaston and Ortiz “exploited inside information about the hospital; it’s that they violated the privacy of patients by accessing their confidential medical records to make their whistleblower case,” Tabler explained.

Keep A Close Watch On Your Contractors To Catch Data Breaches

If you don’t know what your business associates are really doing when you’re not looking, you could have a leak of protected health information (PHI) for weeks or even months before you even realize it.

Dignity Health Mercy Oncology Center’s transcription contractor accidentally made public a link to some physician notes stored on a private server during a routine update, Redding Searchlight reported on Dec. 22, 2014. Dignity reported that about 620 patients’ PHI was accessible online for several weeks.

On Dec. 13, a physician reviewing patient records discovered the link accessible via Google. The records included the patients’ names, birth dates, diagnoses, medications, therapies, and treatment plans. The records did not contain any financial information or Social Security numbers.

Mercy removed the link immediately and is working with Google to scrub any other links or archived versions of the web page, Redding reported. Mercy also no longer works with the transcription company. The healthcare provider claims that there are no signs of any unauthorized access to the PHI.
Reader Questions

Will Your General Liability Policy Cover Security Breaches?

**Question:** Our insurance agent who deals with our practice’s general liability policy told me that the policy won’t cover expenses related to a security breach. He says that we need to purchase a separate policy. Is this now the norm?

**Answer:** If you’re still relying on a corporate general liability insurance policy, you’re not alone. But the language in those policies was drafted before so much information became digital and proven vulnerable to hackers around the globe, pointed out Tallahassee, FL-based associate attorney Sheryl D. Rosen with Akerman LLP in a posting in the firm’s Health Law Rx Blog.

“Now, increasingly, general liability policies are excluding breaches, carving out those benefits into separate cybersecurity policies,” Rosen explained. “Such policies typically cover privacy notification expenses, administrative penalties, crisis management, and other costs” that result from a breach.

So don’t mistakenly think that your general liability policy still covers breaches, even if it did so in the past. You should review your practice’s coverage and make sure that if your firewalls fail, your liability insurance won’t, Rosen advised.

No Breaches—Do You Still Need To Submit An Annual Report?

**Question:** Do we still submit a report for the HHS annual breach reporting even if we don’t have any breaches during the year?

**Answer:** “No, if you haven’t had any breaches to report, there is no particular report that you need to make,” answers Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, VT. You would submit a report only if you do have a breach.

“But do keep in mind that all of the breaches that you have, even the small ones, do need to be reported,” Sheldon-Dean warns. You must report the bigger breaches within 60 days and the smaller ones by March 1 every year.
Does Breach Of Single Person’s PHI Require Notification?

Question: What must we do in terms of breach notification if we mail a statement to the wrong patient? The statement doesn’t have much information on it, other than the fact that there was an office visit, maybe the date of the visit and that the patient went to the visit. Would we have to go through the whole breach notification process?

Answer: “This is a typical situation,” Sheldon-Dean notes. “The kind of breach that happens most often is a piece of paper that winds up in the wrong envelope and goes to the wrong address.”

And the statement doesn’t even necessarily need to have very much information on it, “but if it does have somebody’s name and something about an office visit in any way, then that really is the kind of information you need to report as a breach,” Sheldon-Dean says.

But this is a relatively straightforward process because the breach involves just one individual’s information. You have to notify only that one individual, but you do need to send the patient the official notification, Sheldon-Dean stresses. And the breach will be one that you should submit in your annual accounting to the U.S. Department of Health and Human Services (HHS) before 60 days after the end of each year.
Check Out These Free Compliance Tools

If you’re thinking about redecorating your facility with some HIPAA-focused adornments, the website HealthIT.gov offers a treasure trove of posters, factsheets, brochures, and much more.

All the downloadable materials are free and include banners and badges for your website, as well as educational presentations. The downloadable materials focus on privacy and security issues relating to mobile devices. To view the materials, go to www.healthit.gov/providers-professionals/downloadable-materials.

Example: To give you a sense of what the materials have to offer, here are the tips from HealthIT.gov’s postcard, “10 Tips to Protect and Secure Health Information When Using a Mobile Device:"

1. Use a password or other user authentication.
2. Install and enable encryption.
3. Install and activate remote wiping or remote disabling.
4. Do not install or use file sharing applications.
5. Install and enable a firewall.
6. Install security software and keep it up to date.
7. Research mobile applications before downloading.
8. Always keep your device in your possession.
9. Use adequate security to send or receive health information over public Wi-Fi networks.
10. Delete all stored health information before discarding the mobile device.
Enforcement News: Make Photography And Recordings Part Of Your HIPAA Policies

Recent class-action lawsuits have highlighted the extremely expensive consequences of healthcare professionals who photograph or videotape patients inappropriately. If your organization photographs or records patients in the course of providing care, make sure your HIPAA policies contain strong parameters for this.

**Johns Hopkins Hospital** recently agreed to a $190-million settlement with more than 8,000 patients of gynecologist **Dr. Nikita Levy**, following allegations that Levy secretly photographed and videotaped their bodies in the exam room, according to a July 24 blog posting by Florida-based attorneys **Julie Gallagher** and **Leslie Schultz-Kin** for the law firm **Akerman LLP**.

Although the patients’ faces were not visible in the images, “and it could not be established with certainty which patients were recorded or how many, thousands of patients were traumatized, according to lawyers,” Gallagher and Schultz-Kin wrote. The patients included both women and girls.

And this is not the only lawsuit involving a physician photographing a patient inappropriately — Gallagher and Schultz-Kin point out that several other cases, including some involving posting the photos to social media websites, have cropped up in the past few years.

**Beware:** “In this era of social media where the use of smartphones and tablets make sharing data so easy, these cases raise fresh concerns about a hospital’s ability to protect patients’ privacy,” Gallagher and Schultz-Kin warned. “Accordingly, it is imperative that hospitals implement comprehensive policies regarding patient photography, video imaging and audio recording.”

**Best practice:** Gallagher and Schultz-Kin advised that such policies should:

- Define allowable purposes and circumstances for obtaining film, digital photographs, video images or recording patients using a camera or other device;
- Set forth standards for the creation, use, disclosure and retention of the images;
- Ensure that patient/legal representative consent is given in writing or by verbal consent documented through an appropriate authorization form; and
- Identify prohibited activities and behaviors relating to photography, video or audio recordings of patients, including personal use, entertainment purposes, posting on social media or in public areas, malicious use, or using such images in a way that is disruptive to patient care or the work environment. Make staff failing to comply with such policies subject to disciplinary action.
HIPAA Compliance: How Your HIPAA Obligations Regarding Same-Sex Marriage Have Changed

OCR augments the definitions of spouse, marriage, and family member.

The U.S. Supreme Court ruled last year that federal law cannot disregard same-sex marriage. Since the ruling, the federal government has been mum on how this would affect HIPAA, but new guidance has finally come through.

On Sept. 17, 2014 the HHS Office for Civil Rights (OCR) released guidance to help covered entities (CEs) understand how the United States v. Windsor Supreme Court decision may affect certain HIPAA Privacy Rule requirements. In the Windsor case, the Supreme Court ruled that the Defense of Marriage Act (DOMA), which provided that federal law would recognize only opposite-sex marriages, is unconstitutional.

Note: And on Oct. 6, the Supreme Court made yet another ruling, letting stand appeals court rulings allowing same-sex marriage in five states: Indiana, Oklahoma, Utah, Virginia, and Wisconsin. The ruling may be a sign that a nationwide right to same-sex marriage is on the horizon.

Know the New Meaning of 3 Key Terms

“The guidance clarifies that same-sex spouses have the same HIPAA rights as other family members, no matter where services are provided,” explains Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT. The guidance further specifies “that spouses include both same-sex and opposite-sex individuals who are legally married, whether or not they live or receive services in a jurisdiction that recognizes their marriage.”

The Windsor decision has effectively changed the meaning of three key terms contained in the HIPAA regulations: spouse, marriage, and family member. Here’s how you need to consider these terms in light of Windsor:

- **Spouse:** The term “spouse” includes individuals who are in a legally valid same-sex marriage sanctioned by a state, territory, or foreign jurisdiction (as long as a U.S. jurisdiction would also recognize the marriage in a foreign jurisdiction).

- **Marriage:** The term “marriage” includes both same-sex and opposite-sex marriages.

- **Family Member:** The term “family member” includes dependents of those marriages.
How ‘Family Member’ Definition Impacts Your Practices

One of the areas of the HIPAA rules where you’ll see the revised definition of family member is in §164.510(b) Standard: Uses and disclosures for involvement in the individual’s care and notification purposes. Under certain circumstances, covered entities (CEs) may share an individual’s protected health information (PHI) with a family member.

New: “Legally married same-sex spouses, regardless of where they live, are family members for the purposes of applying this provision,” the guidance states.

For health plans, the revised definition of family member affects §164.502(a)(5)(i) Use and disclosure of genetic information for underwriting purposes. “This provision prohibits health plans, other than issuers of long-term care policies, from using or disclosing genetic information for underwriting purposes,” OCR explains.

Requirement: Plans cannot use information from genetic tests of an individual’s family members, or family members’ diseases or disorders, in making underwriting decisions about that individual. “This includes the genetic tests of a same-sex spouse of the individual, or the manifestation of a disease or disorder in the same-sex spouse,” the guidance says.

Look ahead: The guidance released on Sept. 17, 2014 won't be the only advice on the subject. OCR has promised to issue additional clarifications, through guidance or rulemaking, on same-sex spouses as personal representatives under the Privacy Rule.
Can You Let NPP Rules Slide In This Situation?

**Question:** We sometimes need to collect preoperative information about a new patient over the phone prior to the day of surgery. Usually, we haven’t seen this patient in our office before. Does HIPAA prohibit doing this if the patient has not received or acknowledged our Notice of Privacy Practices (NPP)?

**Answer:** No, the HIPAA Privacy Rule does not prohibit this practice when a healthcare provider’s initial contact with a patient is simply to schedule an appointment or procedure, or to collect information prior to an appointment or procedure, answers the HHS Office for Civil Rights (OCR).

**What to do:** The Privacy Rule allows you to have this phone communication, even if you’re gathering health information from the patient, without attempting to offer that patient your NPP. You can satisfy the Privacy Rule’s requirements for providing the NPP and obtaining the patient’s acknowledgement of receipt when the patient arrives at your facility for his appointment or procedure, OCR instructs.

Is A ‘Consent Form’ A Good Idea For Email Communications?

**Question:** Should we develop some sort of consent form for patients to sign if they indicate that they prefer to communicate with us via email?

**Answer:** “I definitely think that it’s a good idea to have a consent form — that’s a good term for it,” answers Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT. This type of consent form isn’t strictly a HIPAA authorization because the patient isn’t authorizing the release of protected health information (PHI) for a specific purpose.

But you could have a consent form that basically indicates that the patient has discussed email communications with you and that you’ve explained that there are risks of their PHI being exposed and they consent or prefer to communicate via email, Sheldon-Dean says.

Of course, patients always have the right to require email communications using a secure method, “in which case you need to provide them with an encrypted attachment or a secure portal, or some other means if you’ve got any information in some encrypted way,” Sheldon-Dean advises.
Is Signing NPP Acknowledgement Enough For Communication Permission?

**Question:** We have one of those text and email appointment-reminder systems in place. And in our Notice of Privacy Practices (NPP), it does say that is how we communicate reminders to our patients. Do we still need to get their individual approval to communicate that way? Or since they’ve signed our acknowledgement of NPP receipt, are we okay?

**Answer:** In the past, your NPP always had to include something saying that you might use the patient’s health information for contacting him for appointment reminders and other similar things, notes Jim Sheldon-Dean, HIPAA expert and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT. But now the requirement to include that particular item in the NPP no longer exists.

So you don’t necessarily have to say this in your NPP, Sheldon-Dean says. “At the same time, now people are using systems like your texting and email system for communicating.” This is the kind of issue “where I haven’t seen particular guidance from Health and Human Services that says that this is okay without having had to ask for permission,” he adds.

**Best bet:** “So I would suggest that it’s a good idea for you to secure that permission” as a sort of extra safeguard against a HIPAA problem, Sheldon-Dean offers. Start working on a process for obtaining permission as you contact patients. Before the next time you contact patients, ask them if it’s okay to contact them by email and have that discussion.

“I think you need to start working that in because I haven’t seen a specific guidance that would say it’s okay to have those kinds of communications without having gotten permission,” Sheldon-Dean cautions. Just signing your NPP doesn’t necessarily give you permission to go forward with using a text and email system for communicating with patients — the NPP just lets patients know what your practices are.
Enforcement News: Check Out The New Risk Assessment Tool For iPad & Windows

Do you need help conducting your security risk assessment? The HHS Office of the National Coordinator for Health Information Technology (ONC) and HHS Office for Civil Rights (OCR) have just the tool for you.

On March 28, 2014 the ONC and OCR announced their joint release of a new security risk assessment tool, designed for small to medium sized providers. The downloadable tool is available for use on Windows 7 or an iPad and helps practices conduct and document a risk assessment. The application even produces a report that you can provide to auditors.

“In many ways, the tool is an evolution of the NIST HIPAA Security Rule Toolkit released in 2011,” notes Jim Sheldon-Dean, founder and director of compliance for Lewis Creek Systems, LLC in Charlotte, VT. “It doesn’t make the work any easier, but it makes organizing the information and producing reports a little easier if you’re new to Risk Analysis.”

Beware: But Sheldon-Dean also cautions that if you use the tool well, it could help — but use it poorly, and “it could provide a false sense of security.”

Link: You can access the tool, user guide, and related videos at www.healthit.gov/providers-professionals/security-risk-assessment.
Risk Assessment: Understand The 6 Major Risk Categories For Your Risk Assessment

And check out 10 other risk areas that you shouldn’t overlook.

According to Susan Ulrey, an internal audit and compliance practice leader for two CPA consulting firms who has conducted more than 100 risk assessments, you should understand the following six key risk categories:

1. Strategic: The risk that your organization will not meet its business objectives due to poorly defined business strategies, poorly communicated strategies, or the inability to execute these strategies due to inadequate organizational structure, infrastructure or alignment.

2. Operational: The risk that operational processes are not achieving the objectives they were designed for to support the business model. This risk addresses inefficient operations, poor alignment of processes with objectives and strategies, failure to protect assets, etc.

3. Financial: The risk that financial reporting is inaccurate, incomplete, or untimely due to a variety of factors including the pace of change, the amount of uncertainty, the presence of a large error, or the pressure on management to meet certain expectations.

4. Compliance: The risk that your organization is not in compliance with the legal and regulatory requirements associated with mandated federal and state regulations, statutes, and standards.

5. Technology: The risk that IT systems/applications are unavailable and/or there is a lack of integrity with the data and information to support decision making. This risk also considers the level of use, sophistication, complexity, robustness, ease of use and speed, and accuracy of system recovery/replacement.

6. Human Capital: This risk addresses the type of behaviors that management encourages, the methods used to reward employees, and the approach to consistently enforce policies and procedures. This risk also includes the selection, screening, and training of employees, as well as the reason and frequency of turnover.

Evaluate Other Key Risk Areas, Too

Although the above categories are the major risk areas, Ulrey identifies the following other risk categories to consider:
Financial impact/assets at risk;
External compliance and regulatory issues;
Significant organizational change;
Complexity;
Reputational;
Information sensitivity/confidentiality;
Health and safety;
Senior management/Board of Trustees concerns;
Internal controls/prior audit results; and
Time since last audit.
Tool: Use This Cheat-Sheet To Mitigate Your Security Risks

Don’t forget about organizational requirements like business associate contracts.

Security Rule compliance may seem overwhelming at times, especially if you’re flying solo on the whole process. Here are some safeguards and examples of processes that you can put into place to address the potential security risks to your organization, courtesy of the HHS Office for Civil Rights (OCR) and the Centers for Medicare & Medicaid Services (CMS):

<table>
<thead>
<tr>
<th>Compliance Topic</th>
<th>Areas to Consider</th>
<th>Examples of Potential Security Measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Safeguards</td>
<td>• Your facility and other places where patient data is accessed</td>
<td>• Building alarm systems</td>
</tr>
<tr>
<td></td>
<td>• Computer equipment</td>
<td>• Locked offices</td>
</tr>
<tr>
<td></td>
<td>• Portable devices</td>
<td>• Screens shielded from secondary viewers</td>
</tr>
<tr>
<td>Administrative Safeguards</td>
<td>• Designated security officer</td>
<td>• Staff training</td>
</tr>
<tr>
<td></td>
<td>• Workforce training and oversight</td>
<td>• Monthly review of user activities</td>
</tr>
<tr>
<td></td>
<td>• Controlling information access</td>
<td>• Policy enforcement</td>
</tr>
<tr>
<td></td>
<td>• Periodic security reassessment</td>
<td></td>
</tr>
<tr>
<td>Technical Safeguards</td>
<td>• Controls on access to EHR</td>
<td>• Secure passwords</td>
</tr>
<tr>
<td></td>
<td>• Use of audit logs to monitor users and other EHR activities</td>
<td>• Backing-up data</td>
</tr>
<tr>
<td></td>
<td>• Measures that keep electronic patient data from improper changes</td>
<td>• Virus checks</td>
</tr>
<tr>
<td></td>
<td>• Secure, authorized electronic exchanges of patient information</td>
<td>• Data encryption</td>
</tr>
<tr>
<td>Policies &amp; Procedures</td>
<td>• Written policies and procedures to assure HIPAA security compliance</td>
<td>• Written protocols on authorizing users</td>
</tr>
<tr>
<td></td>
<td>• Documentation of security measures</td>
<td>• Record retention</td>
</tr>
<tr>
<td>Organizational Requirements</td>
<td>• Business associate agreements</td>
<td>• Plan for identifying and managing vendors who access, create or store PHI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Agreement review and updates</td>
</tr>
</tbody>
</table>
Reader Questions

What’s The Biggest HIPAA Issue For EHR Implementation?

**Question:** What is the biggest issue you’ve seen with HIPAA and the electronic health record (EHR) implementation process?

**Answer:** “One of the problems that I’ve seen has to do with the security, the implementation that’s been done for the system itself,” Sheldon-Dean says. “I’ve seen that the vendor comes in to do a lot of the implementation.”

After the vendor leaves, make sure you review the security of all the EHR software, Sheldon-Dean advises. And make sure the vendor doesn’t leave the software open, “because I have run into situations where the vendors have left behind a relatively insecure installation.” Also ensure that the vendor configures the EHR correctly.

Another issue is remote access to the EHR. Make sure you have good controls for remote access and think about how you can secure all devices, Sheldon-Dean recommends. “Will there be any health information winding up on those devices or not, and then how can you secure those [devices] if you do wind up with health information on them?”

Although having the EHR available remotely to healthcare providers is often very useful, “just make sure you do that carefully,” Sheldon-Dean warns. “Have some good policies and procedures, and of course training for the individuals.”

Which Comes First: Compliance Or Strategic Risk?

**Question:** Should our internal audit focus on compliance or strategic risks?

**Answer:** “It depends,” answers Susan Ulrey, an internal audit and compliance practice leader for two CPA consulting firms who has conducted more than 100 risk assessments.

“I think that [an] internal audit should focus on compliance,” Ulrey says. “Compliance is a very, very critical part of what we do. We are highly regulated. We have privacy and security issues that we need to be responsible for.”

You can’t get away from compliance — but to add value to your organization, you really need to look at those strategic imperatives, Ulrey notes. You really need to do both; it’s not an either/or situation.

Understand that being compliance-focused is not a negative thing at all, but you still must strike the right balance within your organization of compliance and strategic risk, Ulrey points out.
How Can You Make Continuous Monitoring Feasible?

**Question:** What is the best way to develop a more continuous monitoring approach to our internal audit and risk assessment practices?

**Answer:** “Best practices say that looking at risk once a year just isn’t going to cut it,” answers Susan Ulrey, an internal audit and compliance practice leader for two CPA consulting firms.

Ulrey offers the following ways to decide what level of frequency makes the most sense regarding conducting a risk assessment:

1. **Take baby steps** when figuring out the frequency of conducting internal audits and risk assessments. Determine what makes sense so that you’re not burdening the management team and yourself. Taking baby steps is often the right way because you probably don’t have the resources to hire someone full-time who just monitors risks, Ulrey says.

2. **Break it down** into more bite-size pieces. For instance, is there something that you can do every six months or every quarter that isn’t too laborious from a time perspective? This could be as simple as conducting a focus group or sending out a questionnaire to identify risks, Ulrey notes. Or you could conduct some data mining around some key metrics within your organization.

3. **Assign staffers as liaisons** to different business units in your organization. For instance, you might assign someone in the internal audit/risk assessment to be the liaison who works with IT, or with billing, or with health and safety, Ulrey suggests.

The liaison could attend the other department’s staff meetings to stay current on what’s going on, Ulrey says. You can create a “two-way street,” exchanging information back and forth between the risk assessment team and the other departments in your organization.

What Are Some Tips To Elicit More Support For Risk Management?

**Question:** How can I get support from management for my risk management program?

**Answer:** This is a very common question. Bob Chaput, MA, CISSP, HCISPP, CRISC, CIPP/US, provided the following suggestions in a recent blog posting for Clearwater Compliance LLC:

1. **Get a friend on the executive team.** If you don’t already have an ally in the boardroom, align yourself with someone on the executive team. Try to secure a friend in the “C-suite” who understands risk management, such as your organization’s legal counsel, CFO, Medical Officer, or COO, Chaput suggested.

2. **Don’t harp on “compliance.”** When you’re talking with management about risk, talk about “patient safety” and “quality of care” instead of “compliance,” Chaput recommended. “Talk about how the confidentiality, integrity and availability of health information is critical to patient safety and quality of care.”
3. Set up a risk management oversight council or committee. According to Chaput, the council or committee should be responsible for:

- Providing strategic direction relative to risk philosophy;
- Establishing the authority, responsibility and accountability of the risk management program;
- Setting the organization’s risk appetite;
- Understanding the level of risk in the organization and the impact of the consequences;
- Approving initiatives to reduce or mitigate that risk;
- Ensuring adequate resources to achieve initiatives;
- Providing high-level support for initiatives;
- Being aware of compliance issues and remediation; and
- Ensuring that risks are managed appropriately.

4. Establish a risk management working group. According to Chaput, this should be a cross-functional group that’s responsible for:

- Implementing an effective coordinated risk management program, ensuring documented policies and procedures, training the workforce, determining sanctions for violations, establishing incident reporting procedures, and managing Business Associates.
- Mitigating gaps or weaknesses uncovered during compliance assessments and/or risk analyses.
- Keeping the oversight council informed on results and mitigation activities, as well as regulatory changes, trends in incidents and/or breaches, results of compliance audits, workforce training, and progress on remediation plans.

5. Align your recommendations with business strategy. Ensure your recommendations will improve the protection of health information but won’t disrupt operations unnecessarily, Chaput recommended. “Focus your compliance and security recommendations on ensuring customer trust and creating a competitive advantage.”
EHRs: Good News: You Could Get Some Breathing Room For EHR Compliance

But don’t also expect an escape from reimbursement cuts for noncompliance.

If you’re one of the many providers unable to fully demonstrate meaningful use for Stage 1 and Stage 2 by the original deadline, you may now have some extra time to do so.

On May 23, 2014, the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) issued a proposed rule to modify the meaningful use Stage 1 and Stage 2 timeline for the Electronic Health Records (EHR) Incentive Programs, among other things.

Enjoy a Stage 2 Deadline Extension

The proposed rule extends the deadline for providers to meet the Stage 2 criteria for making meaningful use of EHRs, explained Orlando, FL-based partner Robert Slavkin in a posting for Akerman LLP’s Health Law Rx Blog. “Under Stage 2, providers not only transmit patient records electronically when making referrals, but they also must be capable of sending charts to a physician with a different EHR system.”

Stage 2 also requires providers to ensure that patients use EHRs by requiring that at least 5 percent of patients send a message to their physicians using a portal within the EHR system and that 5 percent access their health information online, Slavkin noted.

Why? Many providers have been unable to timely acquire, adopt, or fully implement the 2014 Edition certified EHR technology (CEHRT), which CMS requires for successfully demonstrating meaningful use for Stage 1 and Stage 2 in 2014, according to analysis from the law firm Ropes & Gray, LLP.

Choose from 3 Compliance Options

“As such, CMS proposes allowing eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) that have not been able to fully implement 2014 Edition CEHRT for the 2014 reporting year to use the 2011 Edition CEHRT, or a combination of the 2011 and 2014 Edition CEHRT, for the meaningful use reporting periods in 2014,” Ropes & Gray reported.
If you use the 2011 Edition only, you must meet the meaningful use objectives and measures for Stage 1 that were applicable for the 2013 payment year, regardless of your current stage of meaningful use, Ropes & Gray explained. If you’re using a combination of the 2011 and 2014 Editions, you could choose to meet the 2013 Stage 1 or the 2014 Stage 1 objectives and measures. Or if you are scheduled to begin Stage 2 in 2014, you could choose to meet the Stage 2 objectives and measures.

If you choose the third option — using the 2014 Edition CEHRT only — you could attest to the 2014 Stage 1 objectives and measures for the 2014 meaningful use reporting period, even if you’re unable to fully implement all the functions of your 2014 Edition required for Stage 2.

But to take advantage of the delays, you must attest that you were unable to upgrade or fully implement to the 2014 Edition CEHRT because of issues related to availability, wrote attorney Elana Zana in a May 21 blog posting for the Seattle-based law firm Ogden Murphy Wallace Attorneys.

The proposed rule also makes a formal announcement of CMS’ previously announced plans to extend Stage 2 through 2016 and begin Stage 3 in 2017, after provider complaints about the original deadlines, Slavkin said. But even with this extension, beginning in 2015 you will still need to report to CMS using the new technology.

**Watch Out: Delay Won’t Forgive Noncompliance**

**Warning:** Despite the reprieve on Stage 2, you’re still facing penalties for noncompliance. “Beginning in 2015, lack of EHR compliance means penalties for providers in the form of reduced reimbursements,” Slavkin warned. “For the first year, Medicare reimbursements will be reduced by 1 percent for providers that don’t meet EHR standards. That penalty jumps to 2 percent the following year and 3 percent every year afterward.”

**Bottom line:** “While this extension of time to allow compliance with Stage 2 is welcome news, implementation and compliance are still a priority that must stay on all providers’ radar screens,” Slavkin stressed.

**Look for CQM Reporting Changes, Too**

In addition to the timeline delays, the proposed rule also relaxes the requirements related to reporting on clinical quality measures (CQM) in 2014, Zana reported. “Specifically, the method of CQM submission to CMS will depend on the edition of CEHRT deployed by the provider (States will still have discretion for submission requirements).”

But if you’re using a combination of the 2011 and 2014 Edition CEHRTs to report on either the 2014 Stage 1 CQMs or Stage 2 measures, or if you’re using the 2014 Edition, you should report CQMs as originally indicated in the Stage 2 final rule (submitting electronically), Zana instructed.

Not Ready? Get A Meaningful Use ‘Hardship Exception’

If you’re fretting over the looming meaningful use payment adjustments set for 2015, here’s some good news: You might qualify for a hardship exception.

If you meet certain criteria, you could apply for and receive a hardship exception to avoid the meaningful use payment adjustments. According to a June 12 blog posting by Elana Zana for the Seattle-based law firm Ogden Murphy Wallace Attorneys, eligible professionals (EPs) may apply for a hardship exception based on the following reasons:

- **Infrastructure** — You are in an area without sufficient internet access, or you face insurmountable barriers to obtaining infrastructure, such as lack of broadband.
- **New EPs** — You are a newly practicing EP who has not had enough time to become a meaningful user. In this case, you can apply for a two-year limited exception to the payment adjustments.
- **Unforeseen Circumstances** — Examples may include a natural disaster or other unforeseeable barrier.
- **Patient Interaction** — You have a lack of face-to-face or telemedicine interaction with patients, or a lack of follow-up need with patients.
- **Practice at Multiple Locations** — You lack control over the availability of certified electronic health record technology (CEHRT) for more than 50 percent of patient encounters.
- **EHR Vendor Issues** — Your EHR vendor was unable to obtain 2014 certification or you were unable to implement meaningful use due to the 2014 EHR certification delays.

If any of these circumstances apply to you, you can apply for a hardship exception by submitting the 2015 Hardship Exception Application to the Centers for Medicare & Medicaid Services (CMS) (www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HardshipException_EP_Application.pdf).

And CMS will automatically grant a hardship exception to certain EPs, Zana stated. If you meet the following criteria, you will receive a hardship exception based on your status with CMS — without having to submit an application:

- New providers in their first year;
- EPs who are hospital-based (spending more than 90 percent of your covered professional services in an inpatient or emergency department);
- EPs with certain PECOS specialties, such as anesthesiology, pathology, diagnostic radiology, nuclear medicine, and interventional radiology.
EHRs: Meaningful Use: Get Your 2014 CEHRT Now

Good news: You’re getting another year for Stage 3 compliance.

If you’re not already using 2014 certified electronic health record technology (CEHRT), you’d better hurry up — a new final rule requires that you do so for your meaningful use (MU) reporting in 2015.

On Sept. 4, 2014, the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) published a final rule on the EHR Incentive Programs. The final rule makes no significant changes to the proposed rule from May 23.

How Your MU Requirements Changed

The final rule largely aims to help physicians, hospitals and critical-access hospitals (CAHs) implement and use CEHRT products, according to the American Academy of Family Physicians (AAFP). Specifically, the final rule:

- Allows physicians and other eligible providers to use 2011 CEHRT, or a combination of 2011 and 2014 CEHRT, to complete the 90-day reporting period in 2014;
- Mandates that all eligible healthcare professionals, hospitals and CAHs must use 2014 CEHRT for MU reporting in 2015;
- Extends Stage 2 through 2016 for some providers; and
- Sets the Stage 3 timeline to begin in 2017 for physicians and other eligible providers who became EHR meaningful users in 2011 or 2012.

Caveat: “The rule applies largely to physicians who were scheduled to attest to MU State 2 for the first time in 2014 and had trouble implementing a 2014 edition certified EHR technology (CEHRT),” AAFP notes. “In addition, physicians who were to attest to MU Stage 1 could possibly attest to the 2013 edition of Stage 1; those who were to attest to Stage 2 can attest to the 2013 or 2014 version of Stage 1.”

Choose from 3 Options

In other words: If you’ve been unable to roll out 2014 edition CEHRT because your EHR vendor didn’t develop the products in a timely fashion, you’ll have more flexibility in complying with MU requirements, explains the law firm Ropes & Gray LLP. In this situation, the final rule offers three options:

1. Using 2011 Edition CEHRT Only: Eligible professionals (EPs), eligible hospitals (EHs) and CAHs using only 2011 edition CEHRT during the 2014 reporting period must meet MU objectives and measures for Stage 1 that were applicable during the 2013 payment year, regardless of the current MU stage.
2. Using a Combination of 2011 and 2014 Edition CEHRT: If you’re using a combination of 2011 edition and 2014 edition CEHRT during the 2014 reporting period, you can choose to meet the 2013 Stage 1 or 2014 Stage 1 objectives and measures. Or, if you are scheduled to begin Stage 2 in 2014, you could choose to meet the Stage 2 objectives and measures.

3. Using the 2014 Edition CEHRT Only: If you’re scheduled to begin Stage 2 for the 2014 EHR reporting period but are unable to fully implement all the functions of your 2014 edition CEHRT required for Stage 2, you can attest to the 2014 Stage 1 objectives and measures for the 2014 reporting period.

Important: “The above options are only available to providers that attest they are ‘not able to fully implement’ 2014 edition CEHRT as a result of ‘delays in 2014 edition CEHRT availability,’” Ropes & Gray stresses.

Will Rule’s Timing Cost You Next Year?
AAFP laments the timing of the final rule, arguing that CMS and ONC should have finalized the rule months ago. “For physicians who were to do meaningful use Stage 2 reporting in 2014, that’s important, because on Jan. 1, 2015, physicians will have to begin reporting for a full year at Stage 2.”

And Russell Branzell, president and CEO of the College of Healthcare Information Management Executives (CHIME) is also unhappy with this timing. “CHIME is deeply disappointed in the decision made by CMS and ONC to require 365 days of EHR reporting in 2015,” he wrote in a recent statement.

“This single provision has severely muted the positive impacts of this final rule,” Branzell charged. “Further, it has all but ensured that industry struggles will continue well beyond 2014.” Most hospitals will not be able to meet Stage 2 requirements beginning on Oct. 1, 2014, which means that the penalties hospitals avoided in 2014 will come in 2015, “and millions of dollars will be lost due to misguided government timelines,” he warned.

Bright Spot: Enjoy a Stage 3 Delay
The final rule also solidifies the proposed delay to the Stage 3 deadline. Instead of Jan. 1, 2016, you will have until Jan. 1, 2017 for the first cohort of adopters to implement Stage 3 MU requirements, according to Ropes & Gray.

“The delay is intended to give CMS and ONC the opportunity to focus on the successful implementation of Stage 2 requirements, including those of enhanced patient engagement, interoperability and health information exchange, as well as to utilize Stage 2 participation data to inform policy decisions regarding Stage 3,” Ropes & Gray notes.

Try Decision-Point Maps To Help Justify Not Meeting MU Deadlines

The **Centers for Medicare & Medicaid Services** (CMS) and the **Office of the National Coordinator** (ONC) granted certain flexibility to hospitals and eligible professionals (EPs) in meeting Stage 2 Meaningful Use (MU) measures in 2014. But EPs and hospitals must thoroughly explain the reasons behind their failure.

**Problem:** Although this flexibility is a boon for many struggling providers, CMS’ and ONC’s guidance has left many providers scratching their heads, wondering who is allowed to claim the exception.

“Any EPs or hospitals that attest for a different stage than what they were scheduled for must be prepared to defend this decision in an audit, understanding that each case will be evaluated individually,” warned **Ogden Murphy Wallace Attorneys** (OMW) associate attorney **Elana Zana** in a Sept. 30 announcement. “This defense should therefore be very well documented.”

**Solution:** In partnership with **ECG Management Consultants**, OMW developed maps of decision points and examples of acceptable and unacceptable justifications for not meeting your scheduled MU stage in 2014. One decision-point map focuses on provider options if this is your first or second year and the second map outlines options if this is your third or fourth year — whether you’re dealing with the 2014 Stage 1 or Stage 2 objectives and measures.

**Link:** To access the decision-point maps, go to [http://omwhealthlaw.com/meaningfuluseattestationin2014/](http://omwhealthlaw.com/meaningfuluseattestationin2014/).
Why EPs Are Failing MU Audits

If you’re wondering how providers are doing with their meaningful use (MU) compliance, you might be surprised at the results so far from the new MU audits.

Centers for Medicare & Medicaid Services (CMS) audit results of MU compliance are beginning to emerge, and so far eligible hospitals (EHs) are faring much better than eligible professionals (EPs). Only 4.7 percent of EHs failed the audits, while EPs had far higher rates of failure, stated associate attorney Elana Zana in a blog posting for the law firm Ogden Murphy Wallace Attorneys.

Approximately 21.5 percent of EPs subjected to prepayment audits did not meet MU standards. According to CMS, there were two reasons for this failure:

1. Failure to use a certified EHR; and
2. Failure to meet MU objectives and associated measures.

And most of those EPs who failed the audits (92.9 percent) did not meet the appropriate objectives and associated measures, while only 7.1 percent of those audited failed to use a certified EHR when attesting, according to analysis by Steve Spearman, founder and chief security consultant for Health Security Solutions in Central, SC.

As for post-payment audits, approximately 24 percent of EPs failed to meet MU standards, for the same two reasons as the prepayment failure, Spearman reported. Most of the EPs who failed their post-payment audits (98.9 percent) did not meet the MU objectives and associated measures.

Cost: And for those EPs who failed the MU audits, providers will need to return their incentive payments to CMS — the average returned incentive payment was $16,862.81, Spearman noted. Of course, providers who fail the MU post-payment audits can appeal the audit outcome, and won’t need to return incentive payments if the appeal is successful.

But Spearman warned that for EPs “counting on incentive payments to cover EHR start-up costs and associated business expenses, returning thousands of dollars could be devastating.” And both pre- and post-payment audits are occurring on a regular basis, indicating that the question of an EP or EH being audited is not “if” but “when.”

Pay attention: Because MU incentives can play such a vital role in organization finances, it is important to make every effort to satisfy all MU objectives and associated measures, Spearman stressed.

“More audits are coming, and making sure that you have double-checked your numbers before attesting and performed your security risk analysis, including an implementation plan and completion dates, is necessary,” Zana concluded.
No Electronic Records Causes Sperm Bank Mix-Up

A woman who underwent artificial insemination with sperm from the wrong donor has filed a lawsuit against the sperm bank — and her claims could impact facilities’ recordkeeping and privacy practices.

On Sept. 29, 2014, the woman filed a lawsuit against Chicago-based Midwest Sperm Bank, LLC, charging claims of wrongful birth and breach of warranty, reported Britt Killian in a blog posting for the law firm Nixon Peabody LLP. The sperm bank sent sperm from the wrong donor to the fertility clinic where the woman underwent artificial insemination.

“The media attention surrounding this case largely focused on race-related issues because the plaintiff’s articulated losses resulted from receiving sperm from an African American donor rather than the white donor she had selected, with little attention given to the impact this case could have on the operation and oversight of sperm banks in the future,” Killian said.

The mix-up occurred because the sperm bank did not keep electronic records, but instead kept hand-written records, the plaintiff alleged. The sperm bank sent the wrong vial to the fertility clinic after one employee wrote the donor’s identity as “380” and another employee noted it as “330.”

“The court’s ruling will likely address the necessity of electronic recordkeeping, privacy protection, and the developing area of law surrounding the professional standards applicable to sperm banks,” Killian noted. The Circuit Court of Cook County, Illinois is deciding the case.

Precedent Set: Yes, You Are Liable For Employees’ HIPAA Violations

The Indiana Court of Appeals upheld a $1.4-million verdict against Walgreen pharmacy chain, potentially setting a national precedent as the first published court decision where a healthcare provider has been held liable for HIPAA violations committed by its employees.

On Nov. 14, 2014, the appeals court affirmed the large jury verdict against Walgreen, reported The Indiana Lawyer. The case involved a Walgreen pharmacist, Audra Withers, who allegedly disclosed Abigail Hinchy’s prescription history to the customer’s ex-boyfriend Davion Peterson. At the time, Withers was involved in a relationship with Peterson.

The appeals court agreed with the trial court’s verdict, which found Walgreen liable for negligent supervision and retention, as well as invasion of privacy. The fact that Walgreen appealed (and lost) means that courts across the United States can rely upon the verdict in holding employers accountable for their employees’ HIPAA violations.
Enforcement News: Watch Out: Upcoming HIPAA Audits Will Be ‘Aggressive’

Keep your eyes peeled this autumn for a notification and data request from the HHS Office for Civil Rights (OCR). If you receive these communications, your practice is one of the selected entities that will face a more vigorous HIPAA audit.

OCR plans to audit 350 covered entities (CEs) and 50 business associates (BAs) during the first round of audits. For those who receive the notification and data request in Fall 2014, “the lucky recipients will be the first participants in the OCR’s effort to adopt a more aggressive approach to investigating compliance with HIPAA standards for privacy, security and breach notification,” wrote Tampa, FL-based Akerman LLP associate attorney A. Crosby Crane in a posting for the firm’s Health Law Rx Blog.

Why? The more aggressive approach stems from the December 2013 HHS Office of Inspector General (OIG) report that slammed the OCR for falling behind on HIPAA enforcement, Crane said. OCR has been making headway in implementing a permanent audit program, instead of relying on complaints as a way to assess compliance.

And the looming permanent audit program “could translate into open season” on CEs and BAs, Crane warned. That’s because OCR is no longer favoring voluntary compliance or corrective actions as opposed to monetary settlements as it has in the past. “Many privacy and security experts believe large settlements will become increasingly common as a result of the OCR’s increased enforcement efforts,” he cautioned.

Protect yourself: You can get a leg up on preparing your practice for the upcoming HIPAA audits by taking a close look at your risk assessment. Crane recommended using the security risk assessment tool that HHS released in March (www.healthit.gov/providers-professionals/security-risk-assessment).

Although using the tool won’t guarantee that you’ll survive an audit unscathed, “its use very likely will be a factor in how the government views a provider’s overall compliance efforts,” Crane explained. “Just how much of a factor remains to be seen, but a prudent HIPAA compliance program would be well served to use the tools provided by HHS.”
Avoid The Top 5 Investigated HIPAA-Compliance Issues

With all of the breaches, enforcement actions and audits swirling around the HIPAA stratosphere, you’d better prepare yourself with some basic information. For example, do you know what types of covered entities (CEs) are most likely to face corrective action?

As of March 31, 2014, the HHS Office for Civil Rights (OCR) has compiled and analyzed enforcement data to reveal the most common compliance issues investigated and the most common types of CEs who’ve faced corrective action. According to OCR, the most common compliance issues investigated are (in order of frequency):

1. Impermissible uses and disclosures of protected health information (PHI);
2. Lack of safeguards of PHI;
3. Lack of patient access to their PHI;
4. Uses or disclosures of more than the minimum necessary PHI; and
5. Lack of administrative safeguards of electronic PHI (ePHI).

And the most common types of providers required to take corrective action for voluntary compliance are (in order of frequency):

1. Private practices;
2. General hospitals;
3. Outpatient facilities;
4. Health plans (group health plans and health insurance issuers); and
5. Pharmacies.

Resource: To stay abreast of these HIPAA enforcement statistics, visit OCR’s Enforcement Highlights webpage at www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.
Watch Out SNFs: HIPAA Penalties Will ‘Set Records’

Now that the HIPAA audits are back in full swing, you need to be on your guard. And according to government officials, skilled nursing facilities (SNFs) are especially at risk for record-breaking HIPAA penalties.

The U.S. Department of Health and Human Services’ chief regional civil rights counsel Jerome Meites warned that HIPAA penalties during the next 12 months should “set records,” reported Christopher Froeb in a Nixon Peabody LLP blog posting. Meites made these comments during an American Bar Association conference in Chicago on June 12 and 13, 2014.

Meites urged SNFs and other providers to perform comprehensive risk analyses, particularly now that HIPAA audits have recommenced after the temporary suspension in 2012.

“SNF operators should take note of this increased enforcement and, if necessary, perform internal audits to confirm policies are in place regarding HIPAA compliance,” Froeb advised.
HIPAA Audits: Get Ready For Phase 2 Of OCR Audits: Take 7 Steps

Beware: These new audits could lead to civil money penalties.

Now that the Phase 1 audits have finished, the HHS Office for Civil Rights (OCR) is poised and ready to begin the second round of HIPAA audits. Are you prepared for OCR to knock on your door for a Phase 2 audit?

What to Expect in Phase 2

Unlike the Phase 1 pilot audits that OCR conducted in 2011 and 2012 which focused on covered entities (CEs) only, the Phase 2 audits will involve both CEs and business associates (BAs), according to McDermott Will & Emery (MWE) attorneys in an article published in The National Law Review.

“Unlike the Phase 1 audits, OCR will conduct the Phase 2 audits as desk reviews with an updated audit protocol and not on-site at the audited organization,” MWE noted. And OCR will post the Phase 2 audit protocol on its website so you can use it for your internal compliance assessment.

OCR itself will conduct the Phase 2 audits and will focus on more high-risk areas, explained partner attorneys Adam Greene and Rebecca Williams in a recent advisory from the law firm Davis Wright Tremaine LLP. OCR may also potentially integrate the audits into its formal enforcement program.

This means that if “an audit reveals a serious compliance concern, OCR may initiate a compliance review of the audited organization that could lead to civil money penalties,” MWE warned.

Pay Close Attention to These Compliance Areas

And in the Phase 2 audits, OCR will target HIPAA standards with the highest numbers of noncompliance in the Phase 1 audits. According to MWE, these standards include:

- Risk analysis and risk management;
- Content and timeliness of breach notifications;
- Notice of privacy practices (NPP);
- Individual access;
- Privacy standards’ reasonable safeguards requirement;
- Training to policies and procedures;
- Device and media controls; and
- Transmission security.
HIPAA compliance experts offer the following steps that you should take to prepare for Phase 2 of the OCR audits:

1. **Double-Check Your Risk Analysis**
   
   Make sure that your organization has recently completed a comprehensive assessment of potential security risks and vulnerabilities, MWE advised. Also, “confirm that all action items identified in the risk assessment have been completed or are on a reasonable timeline to completion.”

   **What’s more:** Your risk analysis should actually identify and categorize risks as low, medium or high, “rather than merely documenting that controls are in place or documenting the gaps in compliance with the Security Rule,” Greene and Williams urged.

2. **Update Your Policies And Procedures**
   
   Auditors will also scrutinize your policies — particularly your breach notification, risk analysis and risk management policies, as well as your NPP and patient access policies, Greene and Williams noted.

   Make sure your organization has implemented a breach notification policy that accurately reflects the content and deadline requirements under the breach notification standards, MWE stated. And check to ensure that your NPP is compliant and not only a website privacy notice.

   Additionally, review your organization’s HIPAA security policies to identify any actions that you have not yet completed as required, MWE recommended. Review your physical security plans, disaster recovery plan, emergency access procedures, etc.

3. **Locate Your Documentation for Quick Access**
   
   Because auditors will ask for a plethora of information and documentation — and you’ll have only two weeks to respond to OCR’s audit data request — you should keep certain other papers handy. For instance, know how to readily collect documentation of patients’ receipt of NPP acknowledgements and, where there is no patient acknowledgment, documentation supporting the reason why you did not obtain an acknowledgement, Greene and Williams said.

   **Smart idea:** Greene and Williams also recommended that you should keep certain supplemental documentation readily available and clearly labeled. This documentation should include breach investigations and risk assessments, risk analyses, and risk management plans, as well as responses to patient requests.

4. **Keep a Current List of BAs**
   
   Yet another piece of information that auditors will want is a list of your business associates (BAs), so ensure that you have a complete inventory of your organization’s BAs for purposes of the Phase 2 audit data requests, MWE said.
**Best strategy:** You should maintain a current list of BAs with relevant contact information, Greene and Williams agreed. “An internal audit of accounts payable may help identify BAs and is a methodology that was used by OCR’s contractors in Phase 1 audits.”

5. **Check Your ‘Addressable Implementation Standards’**

**Don’t overlook:** If your organization “has not implemented any of the security standards’ addressable implementation standards for any of its information systems, confirm that the organization has documented: (i) why any such addressable implementation standard was not reasonable and appropriate; and (ii) all alternative security measures that were implemented,” MWE recommended.

6. **Inventory All Your Information System Assets**

Confirm that your organization maintains an inventory of information system assets, including mobile devices (even in a bring-your-own-device environment), MWE said. Also make sure that all systems and software that transmit electronic PHI (ePHI) employ encryption technology or that you have documentation in your risk analysis supporting the decision not to employ encryption.

7. **Review Your Security Plan**

Ensure that your organization “has adopted a facility security plan for each physical location that stores or otherwise has access to PHI, in addition to a security policy that requires a physical security plan,” MWE advised. Your organization must have “reasonable and appropriate safeguards in place for PHI that exists in any form, including paper and verbal PHI.”
Curious? Find Out What Phase 1 OCR Audits Revealed

*Security-standard compliance items are a weak spot for providers.*

If you’re wondering how covered entities (CEs) fared during the first round of audits by the HHS Office for Civil Rights (OCR), you might be surprised at the answer. And you should pay close attention to these findings, because they will impact the compliance areas that OCR will focus on in the Phase 2 audits.

According to McDermott Will & Emery (MWE) attorneys in a July 29 article published in The National Law Review, the Phase 1 OCR audits of 115 CEs produced the following aggregate results:

Only 11 percent of audited CEs had no findings or observations;

Despite representing just 53 percent of audited CEs, health care providers were responsible for 65 percent of the total findings and observations;

The smallest audited CEs struggled with compliance under all three of the HIPAA standards;

More than 60 percent of the findings or observations were security-standard violations, and 58 of 59 audited health care provider CEs had at least one security-standard finding or observation, even though the security standards represented only 28 percent of the total audit items;

OCR attributed more than 39 percent of the findings and observations related to the privacy standards to a lack of awareness of the applicable privacy-standard requirement; and

Only 10 percent of the findings and observations related to a lack of compliance with the breach-notification standards.
Reader Questions

Can Multiple Small Breach Reports Trigger An Audit?

**Question:** If our clinic reports every small HIPAA breach throughout the year instead of waiting until the end of the year, will this trigger an audit?

**Answer:** Whether you report each small breach as they occur or report them all at once at the end of the year, this should not make much of a difference in terms of triggering an audit, answers Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT.

For small breaches, you only need to report them to the **U.S. Department of Health & Human Services** (HHS) within 60 days of the end of the year, instead of as they happen like for larger breaches, Sheldon-Dean explains. But certainly some people wonder whether reporting small breaches to HHS in a single batch at the end of the year (along with all the other small breaches from providers) is “less noticeable” than sending the breach notifications throughout the year.

**Red flag:** What HHS is really looking for — and what may trigger an audit — is whether your practice has similar small breaches that could indicate a systemic problem, Sheldon-Dean warns. HHS will “take a look at all the potential issues and then make decisions as to whether they need to do any kind of compliance investigation.”

❖
Update Your ‘Pre-Existing’ BAAs Now

*Focus on 3 BAA terms that can increase your liability.*

While you’re pondering your business associate’s (BA’s) ability to comply with HIPAA and state privacy laws, keep in mind that you need to amend your pre-existing BAAs by September. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, you must update and revise your BAAs to ensure they’re in compliance with the HIPAA Omnibus Final Rule.

The HITECH Act mandates that you negotiate and implement amendments to all pre-existing BAAs — those entered into prior to Jan. 25, 2013, said attorney **Casey Moriarty** in a blog posting for the Seattle-based law firm **Ogden Murphy Wallace**.

But you should “also be mindful of the important terms in BAAs that can lead to increased liability,” Moriarty noted. Specifically, pay attention to these three terms:

- **Indemnification**: Although not required under the HITECH Act, you should push for strong indemnification language that requires the BA to indemnify your organization for its breach of PHI and HIPAA violations, Moriarty said. “Acceptable indemnification language for each party depends on the nature of the PHI involved in the transaction and the amount of PHI that is transmitted between the parties.”

- **Limitation of Liability**: Many BAs push for BAA language that limits their liability to certain amounts. But accepting a BA’s “limitation of liability” terms can pose significant risks if the BA violates HIPAA after the BAA is signed, Moriarty warned.

- **Breach Notification Time Period**: The HITECH Act requires BAs to notify CE’s of a breach within 60 days of discovery. But to protect your relationships with patients affected by a breach, your proposed BAAs should require the BA to provide notification within 10 days or less, Moriarty recommended. A BA’s “acceptance to a shorter notification period can put tremendous pressure on it to investigate and disclose accurate information after a breach occurs.”

**Lesson learned**: Although you must complete the BAA amendments by the Sept. 23 deadline, you still need to take the time to think critically about the language in your BAAs prior to signing them, Moriarty stressed.
Breach Risk: Keep A Close Watch On Your BAs

Using third-party vendors is always a concern when it comes to handling protected health information (PHI) and other personal or financial information. So here’s yet another case to inspire you to make sure that your business associates (BAs) are keeping your patients’ data safe and secure.

Hackers accessed the computer systems of Onsite Health Diagnostics, a third-party vendor that Tennessee uses to store information on its state employees, WSMV reported on Aug. 26. The hackers stole data on more than 60,000 state workers contained in a data table that included personal information belonging to members who participate in wellness screenings as part of the health plan.

Although the Tennessee Benefits Administration (TBA) claims that the hackers did not access any Social Security numbers, financial information or medical information, they did obtain individuals’ email addresses, phone numbers, addresses, genders and dates of birth.

No identity thefts have occurred so far related to this data breach, but Onsite is offering affected individuals free identity theft protection. TBA blamed the breach on Onsite’s “old computer system,” but said that the vendor now has a new computer system in place with new securities, according to WSMV.
Monitor Your Contracts To Catch Data Breaches

If you don’t know what your business associates are really doing when you’re not looking, you could have a leak of protected health information (PHI) for weeks or even months before you even realize it.

Dignity Health Mercy Oncology Center’s transcription contractor accidentally made public a link to some physician notes stored on a private server during a routine update, Redding Searchlight reported on Dec. 22, 2014. Dignity reported that about 620 patients’ PHI was accessible online for several weeks.

On Dec. 13, a physician reviewing patient records discovered the link accessible via Google. The records included the patients’ names, birth dates, diagnoses, medications, therapies, and treatment plans. The records did not contain any financial information or Social Security numbers.

Mercy removed the link immediately and is working with Google to scrub any other links or archived versions of the web page, Redding reported. Mercy also no longer works with the transcription company. The healthcare provider claims that there are no signs of any unauthorized access to the PHI.
Reader Questions

Do BAs Need To Have HIPAA NPPs?

**Question:** Does a business associate (BA) need to have a HIPAA Notice of Privacy Practices (NPP)?

**Answer:** BAs don’t necessarily need to have a HIPAA NPP, answers Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, VT. But BAs may be responsible for participating in and maintaining an NPP if they are providing those kinds of front line services for their covered entity (CE).

**Meaning:** If the CE hires the BA to manage the front desk and/or sign up new patients or gather contact information, the BA may be responsible for managing that NPP and distributing the NPP to the patients, Sheldon-Dean says. But BAs wouldn’t have an NPP of their own for their own operations.

What Are The Dangers Of Not Complying With New BAA Standards?

**Question:** Despite the Sept. 22 deadline, we have not yet updated our business associate agreement (BAA) contracts. What happens now?

**Answer:** “Technically, a healthcare practice faces statutory penalties for any improperly used or leaked PHI,” answered attorney David Schoolcraft of Ogden Murphy Wallace Attorneys in an interview with DocuSign. “For example, if a healthcare provider contracts with a medical billing vendor without an updated BAA, they face stiff penalties should there be any improper use of PHI.”

“Updating your BAAs is a risk management strategy, and it allows you to add additional protection clauses, such as stipulations about the use of data and operations in the cloud,” Schoolcraft stated. “With the proliferation of cloud vendors and third parties working with healthcare providers, the new BAAs provide a mechanism to not only require the safeguarding of PHI and the reporting of a breach, but the sharing of responsibility when a breach does occur.”

If you don’t update your BAAs, you won’t have the opportunity to ensure that you have sufficient indemnification and insurance provisions in place, Schoolcraft continued. And without such provisions, you cannot necessarily expect reimbursement and defense from the business associate in the event of a breach.
HIPAA Compliance: New Guidance: Emergencies Don’t Trump Your HIPAA Requirements

Know what information you can share with disaster relief organizations.

Do you know your patients’ HIPAA privacy rights in emergency situations? How about your obligations to public health reporting? Here’s what you need to know so an emergency situation doesn’t become a HIPAA breach disaster.

Citing the recent Ebola virus outbreak, the HHS Office for Civil Rights (OCR) has released guidance on HIPAA compliance in emergency and public health situations. The guidance explains the ways in which covered entities (CEs) may share protected health information (PHI) under the HIPAA Privacy Rule in emergency situations.

Know Your State’s Requirements

“Federal laws and regulations permit, and many state laws require, the disclosure of patient information without a patient’s consent or authorization for certain public health activities,” pointed out partner attorney Laurie Cohen in a blog posting for the law firm Nixon Peabody LLP.

According to the OCR guidance, the HIPAA Privacy Rule allows CEs to disclose necessary PHI without individual authorization:

- **To a public health authority**, such as the Centers for Disease Control and Prevention (CDC) or a state or local health department authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability.
- **At the direction of a public health authority, to a foreign government agency** that is acting in collaboration with the public health authority.
- **To persons at risk** of contracting or spreading a disease or condition if other law, such as state law, authorizes the CE to notify such persons as necessary to prevent or control the spread of the disease, or otherwise to carry out public health interventions or investigations.

Stick to the ‘Minimum Necessary’

But when you’re disclosing PHI to a public health authority, keep in mind that the disclosure is subject to HIPAA’s “minimum necessary” standard, Cohen reminded.
The standard provides that the CE will limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

According to HIPAA, when making disclosure to public health officials, a CE “may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary … if the public official represents that the information requested is the minimum necessary.”

Example: A CE may rely on representations from the CDC that the PHI requested by the CDC about all patients exposed to or suspected or confirmed to have Ebola is the minimum necessary for the public health purpose, OCR says.

Remember: Also, don’t forget to include the disclosure in the accounting of disclosures of patients’ PHI — this HIPAA requirement includes disclosures for public health purposes, Cohen stated.

Public Health Reports: Safeguard Patients’ Privacy Rights

Although HIPAA permits disclosures of PHI without patient authorization for public health activities, you “cannot disregard a patient’s right to privacy in those cases where a patient’s information has been the subject of a public health report,” Cohen warned.

“Put another way, the public disclosure of a patient’s information, including the identity of a patient, by a covered entity is not permissible even in cases where a public health report has been made and a public health official subsequently releases information about the patient as part of its public health surveillance, investigation or intervention,” Cohen explained. If you were to release a patient’s information, you would need to have a valid authorization signed by the patient or the patient’s authorized representative.

Consider Other Disclosures & Imminent Danger

The HIPAA Privacy Rule also allows you to “share patient information with anyone necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public,” OCR notes. But even in “imminent danger” situations, you must still comply with applicable laws, such as state statutes, regulations or case law, and your own standards of ethical conduct.

When it comes to sharing a patient’s PHI with family members, friends and others involved in the individual’s care, you should try to get verbal permission or otherwise reasonably infer that the patient does not object, when possible in an emergency situation, OCR instructs. If the patient is incapacitated or not available, you can share PHI if your professional judgment is that doing so is in the patient’s best interest.

What’s more: You can also share PHI with disaster relief organizations like the American Red Cross for the purpose of coordinating notification of family member or other individuals
involved in the patient's care, of the patient's location, general condition or death, OCR notes. “It is unnecessary to obtain a patient's permission to share the information in this situation if doing so would interfere with the organization's ability to respond to the emergency.”

**Understand the ‘Limited Waiver’**

Finally, the HHS Secretary may provide a “limited waiver” of certain HIPAA Privacy Rule provisions under the Project Bioshield Act of 2004 and Section 1135(b)(7) of the Social Security Act. This waiver can occur when the U.S. President declares an emergency or disaster and the HHS Secretary declares a public health emergency.

In this case, the HHS Secretary may waive sanctions and penalties against a covered hospital that doesn’t comply with the following Privacy Rule provisions:

- The requirement to obtain a patient’s agreement to speak with family members or friends involved in the patient’s care.
- The requirement to honor a request to opt out of the facility directory.
- The requirement to distribute a Notice of Privacy Practices (NPP).
- The patient’s right to request privacy restrictions.
- The patient’s right to request confidential communications.

**Caveats:** According to OCR, if the Secretary issues this waiver, it applies only:

1. In the emergency area and for the emergency period identified in the public health emergency declaration; 2. To hospitals that have instituted a disaster protocol; and 3. For up to 72 hours from the time the hospital implements its disaster protocol, or until the Presidential or Secretarial declaration terminates (even if 72 hours has not elapsed).

**Bottom line:** Despite certain special allowances in emergency situations and public health considerations, you should never think that you can set aside HIPAA Privacy Rule protections during an emergency.

‘Consent’ vs. ‘Authorization’ — What’s The Difference?

**Question:** Under the HIPAA Privacy Rule, what is the difference between “consent” and “authorization?”

**Answer:** The term “consent” relates to disclosing protected health information (PHI) for treatment, payment, and healthcare operations (TPO) purposes. The Privacy Rule allows (but does not require) you to voluntarily obtain patient consent for such disclosures, and allows complete discretion to design a process that best suits a provider’s needs.

On the other hand, patient “authorization” relates to PHI disclosures not otherwise allowed under the Privacy Rule, according to the HHS Office for Civil Rights (OCR). You must have a signed patient authorization that gives you permission to use PHI for specified purposes, generally other than TPO purposes. You would also need an authorization to disclose a patient’s PHI to a third party.

OCR lists the following specific elements that you must include in an authorization:

- A description of the PHI that you’ll use or disclose;
- The person authorized to make the use or disclosure;
- The person to whom you may make the disclosure;
- An expiration date; and
- The purpose for using or disclosing the PHI (in some cases).

What To Do When Another Provider Refuses To Release Records

**Question:** We’re treating a new patient and need to obtain the patient’s prior treatment records. The patient has requested that our office receive the records, per his access request. But the other provider notified our office that it will not grant the disclosure request and won’t send the records. What should we do?

**Answer:** “This is a difficult problem to solve, because the new provider has little leverage over the prior provider(s),” stated Bruce Borkosky, Psy.D. in a whitepaper for Malvern-Group Incorporated.

**Best bet:** First, find out whether the prior provider would be more comfortable sending the records to the patient directly, instead of to your office, Borkosky advised. If so, the patient can then forward the records to you, the new provider.

Although this is likely the best, easiest and lowest-impact solution to the problem, you do have a few other options:

1. **Have a discussion.** Although the provider’s reasons for denying the disclosure may or may not be rational, the provider might be open to reason, Borkosky said. “Consider discuss-
ing the state laws and rules, as well as HIPAA regulations that require providers to release records to other providers for treatment.”

“Consider mentioning state disciplinary cases, if your state has ever sanctioned someone for failing to release records for treatment,” Borkosky suggested. Also consider discussing the U.S. Department of Health and Human Services (HHS) case examples and resolution agreements published on its website (www.hhs.gov/ocr/privacy/hipaa/enforcement/examples).

“If the provider is employed by an agency or in a group practice, a short telephone call (or even a fax) to the agency’s attorney or business manager can make a huge difference,” Borkosky noted. “The attorney is likely to have a clearer understanding of the HIPAA Privacy Rule and the potential for liability for failing to comply with it.

2. File a disciplinary complaint. You could file a disciplinary complaint under the provider’s licensing agency, but it can be time-consuming to complete the paperwork, Borkosky noted. This can also require many months for resolution, be expensive for taxpayers, create ill will among fellow providers, and be a sledge-hammer-solution when a needle would do.

Additionally, filing a disciplinary complaint “may ultimately result in no findings if the licensing agency views it as a minor offense,” Borkosky said. “Similarly, a HIPAA complaint can take years to resolve and may result in nothing more than a ‘letter of education.’”

3. Ask your attorney to draft a letter. You might consider asking your attorney to draft a letter on the patient’s behalf, Borkosky stated. But this can also be expensive and time-consuming. “Although it may impress or intimidate some providers, others might recognize that such a letter carries no force of law,” he added. ✤

Is This An Incidental Use And Disclosure?

**Question:** This summer our practice has two interns from the local community college who are helping with front desk duties. The way our small office is set up, these interns are often within earshot when we are discussing patient billing and care issues. The problem is that the interns are not technically authorized to handle patient information. Does this situation fall under the Privacy Rule’s provisions allowing incidental uses and disclosures?

**Answer:** Yes, because the HIPAA Privacy Rule’s provisions apply universally to incidental uses and disclosures permitted under the Privacy Rule, according to the HHS Office for Civil Rights (OCR). These provisions don’t just apply to incidental uses and disclosures resulting from treatment communications or only to communications among healthcare providers and authorized medical staff.

**Key:** You do, however, need to make “reasonable efforts to avoid being overheard and reasonably limit the information shared” so that the incidental use or disclosure resulting from such conversations would be permissible under the Privacy Rule, OCR reminds. Consider
the following examples that would fall under the incidental uses and disclosures provisions under the Privacy Rule:

- A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.
- A health plan employee discussing a patient’s health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

**Does The Privacy Rule Really Allow Disclosures To Family And Friends?**

**Question:** We often have patients’ family members calling our hospital to ask how their loved one is doing. What are we really allowed to disclose under the HIPAA Privacy Rule?

**Answer:** What you can or cannot disclose to a patient’s family member depends on whether the person calling has a role in taking care of the patient, according to the American Medical Association (AMA). Also, you need to take into account whether the physician believes, in his/her professional judgment, that releasing the patient’s information to the family member is in the patient’s best interest and relates to the family member’s involvement in the patient’s care.

“The Privacy Rule allows a physician to share a patient’s information with the patient’s family member or friend so long as the information is limited to information directly relevant to that person’s involvement in the patient’s care,” the AMA says. “The physician should not share more information than the person needs to assist with the patient’s care.”

**Example:** A physician may tell a family member or friend living with the patient that he needs plenty of rest and lots of fluids, or that the patient needs to take a prescribed medication twice daily with food.

But don’t share a patient’s information with his family or friends if he has asked you not to or if the physician believes that a disclosure would be inappropriate, the AMA cautions.

**What’s Wrong With Mailing Postcards To Patients?**

**Question:** Our provider group would like to send out postcards to our patients. The postcards would contain a link to an online quality-of-care survey. Should we worry about any HIPAA implications?

**Answer:** Yes, there are HIPAA privacy risks involved in mailing out postcards to your patients. Even though the postcards might contain only the patients’ names and addresses, along with the link to the online survey, you’re still exposing their protected health information (PHI) — and risking a HIPAA privacy breach.
In fact, a recent case illustrates this point:

The **Colorado Department of Health Care Policy & Financing** unintentionally disclosed the PHI of about 15,000 individuals receiving behavioral health services through Medicaid or the Department of Human Services’ Office of Behavioral Health, according to an Oct. 10, 2014 Department announcement. The disclosure occurred when the Department mailed survey postcards to these individuals.

**Problem:** The postcards were not mailed in envelopes and therefore could be read by someone other than the addressee, the Department said. Although the postcards did not contain individuals’ Social Security numbers or any other information used for identity theft, they did include the addressee’s address and first and last name, as well as the Department’s logo and a request to provide feedback regarding the addressee’s behavioral healthcare services.

Disclosing that the addressee receives behavioral healthcare services is a violation of HIPAA. The Department notified affected individuals of the breach after receiving a complaint on Sept. 9, 2014. ✴
What The FBI Has To Say About PHI Security

How valuable is your patients’ PHI? Can you quantify each patient’s record in a dollar amount? Well, the FBI’s Cyber Division apparently can.

On April 8, 2014, the agency issued a Private Industry Notification entitled, “Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain.” The Notification generally classifies the state of information security in healthcare, according to Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek System, LLC in Charlotte, VT.

So what did the FBI conclude? First, healthcare entities are implementing security measures insufficiently, breaches are widespread, and the rapid increase in electronic health record (EHR) implementation is leaving the healthcare industry vulnerable, Sheldon-Dean reported.

Another interesting tidbit from the FBI was that the agency believes PHI is far more valuable than financial data — PHI is worth $50 per record, while financial information is valued at just $1 per record. You can read the Notification at www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
Compliance: Learn 3 Big Lessons From The HITECH Annual Reports

How to avoid the top 4 causes of HIPAA breaches

The HHS Office for Civil Rights (OCR) recently released some surprising data in two in-depth reports on HIPAA compliance and breaches. Luckily, the reports also contained a few gems of advice to healthcare providers that will help you prevent a HIPAA catastrophe.

On June 11, OCR issued two reports to Congress mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act: “Breaches of Unsecured Protected Health Information” and “HIPAA Privacy, Security, and Breach Notification Rule Compliance.” The reports cover calendar years 2011 and 2012.

What the Reports Had to Say

The breach notification report provides an overview of the breach notification requirements, while the report on the HIPAA rules summarizes complaints that HHS has received of alleged violations of HITECH and the HIPAA Privacy and Security Rules, according to OCR.

During 2011 and 2012, the reports state that HHS entered into seven resolution agreements/corrective action plans totaling more than $8 million in settlements, reported Milwaukee, WI-based attorney Meghan O’Connor in a June 12 blog posting for the law firm von Briesen & Roper, S.C. These settlements resulted from breaches reported to HHS, which spurred investigations. OCR received 236 reports in 2011 and 222 reports in 2012 of breaches involving 500 or more individuals.

“The compliance report reviews HHS compliance and enforcement activities, as well as complaints received by HHS with respect to the HIPAA Privacy, Security, and Breach Notification Rules,” O’Connor said. From 2003 to 2012, OCR investigated 27,466 complaints and resolved 18,559 of these cases by requiring corrective actions and/or providing technical assistance.

Avoid the Top 4 Causes of HIPAA Breaches

O’Connor pointed out that, according to the breach report, the primary reported causes of larger breaches included:

- Theft;
- Unauthorized access, use, or disclosure;
- Improper disposal; and
- Hacking/IT incident.
“Based on the types of breach reports submitted, HHS advises that entities subject to HIPAA should ensure completing of risk evaluations, secure portable electronic devices, provide for proper disposal of PHI, implement physical access controls, and provide trainings to members of the workforce,” stated a June 20 blog posting by health law attorney Leah Roffman for the law firm Cooley LLP. “These are important steps to take to limit the likelihood of a breach.”

And although these reports may seem simply like jumbles of depressing statistics, you can actually learn quite a bit from them. Here are three key lessons you can glean from these reports:

1. **Ratchet Up Your Theft-Prevention Efforts**

Theft didn’t merely rank number one on the list of breach causes, it blew all other causes out of the water. Theft accounted for half of the breaches in both years (50 percent in 2011 and 53 percent in 2012), according to Roffman.

“The statistics in both reports clearly show that the most breaches still come from ‘older’ sources of PHI, such as paper records, desktop computers, and network servers,” noted attorneys Stephanie Willis and Dianne Bourque in an analysis for the law firm Mintz Levin Cohn Ferris Glovsky and Popeo PC, which was published in The National Law Review.

“In addition to updating and monitoring security protocols for older PHI sources, covered entities should address security problems with newer storage media,” according to Willis and Bourque.

And specifically, the breach report also shows a large increase in the number of breaches involving laptops, said Willis and Bourque. “Because theft was the primary cause of breaches in 2009 to 2012, ensuring that laptops and other portable devices are secured in accordance with standards acceptable under HIPAA will become even more important as organizations adopt more ‘bring your own device’ policies to ensure the mobility and convenience of health care delivery.”

2. **Keep a Close Eye on Your BAs**

Although BAs accounted for only 26 percent of the breaches in the reporting period, these breaches affected 59.3 percent of the total individuals affected by all the breaches reported. And the large number of affected individuals in breaches involving BAs likely reflects the reality that BAs may house PHI for multiple CEs, Willis and Bourque pointed out.

**Action point:** “Based on these statistics, health care organizations must impose standards for using BAs and subcontractors,” Willis and Bourque urged. You must also ensure that your BAs and subcontractors understand their obligations under the HIPAA Privacy and Security Rules.
3. Beware of the Cumulative Effects of Small Breaches

Although small breaches — those involving fewer than 500 individuals — may seem like a far cry from mega breaches affecting millions of people, they can still seriously hurt your organization.

**Reason:** “The problem with small breaches for organizations is that they can occur more frequently than large ones,” warned Willis and Bourque. “The occurrence of repeated small breaches can be indicative of a systemic compliance problem, and may suggest to a regulator that the organization has not taken steps to identify and remedy the problem.”

That’s why it’s crucial for your organization to determine its breach risk profile, and identify and correct any compliance gaps, Willis and Bourque stressed. “All covered entities should ensure that they account for the likelihood of small breaches as much as they do for large breaches when doing their security risk assessments.” (For help with your risk assessment, check out the HHS Office of the National Coordinator’s Security Risk Assessment Tool for small and medium-sized health care providers at www.healthit.gov/security-risk-assessment.)

**Links:** To access the breach notifications report, go to www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html. The report on the HIPAA rules is available at www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.
Data Security: Weigh The Benefits vs. The Risks Of Storing Data In The Cloud

How a signed BAA doesn’t ensure HIPAA compliance.

Cloud services are incredibly helpful for many healthcare providers — and for some providers, cloud storage is practically essential to operations. But is using the cloud safe? How can you protect against a data breach while using cloud services?

**Upside:** “The features of Dropbox and other [cloud storage] providers like Dropbox (Box and OneDrive) include ease of use, convenience and ‘anywhere access’ capabilities,” stated John G. Roman, Jr., CISSP, director of Nixon Peabody LLP’s Electronic Discovery and Information Technology Operations team, in a blog posting for the law firm. “The good news is that most cloud-based providers have tightened their data security in the wake of recent breaches.”

But according to Roman, the question remains: “Do the benefits of using the cloud outweigh the risks associated with data potentially being compromised?”

**Dispel This BA Compliance Myth**

First, understand that just because an entity signs a business associate agreement (BAA) doesn’t make that entity automatically HIPAA-compliant, warned Nixon Peabody partner attorney Linn Foster Freedman in a blog posting for the law firm. “The entity must actually have policies, procedures and safeguards in place that comply with the Security Rule.”

“That means dozens of policies and procedures specifically designed to protect the PHI it receives from a covered entity,” Freedman explained. “In my experience, many business associates have no idea that they are required to have these policies and procedures in place and have not implemented them.”

**Beware:** No certifying agency or government body will give any entity a “HIPAA compliant” stamp of approval, Freedman continued. The only way you could really know whether you’re HIPAA compliant is if you make it through an HHS Office for Civil Rights (OCR) investigation unscathed.

**Consider 7 Factors to Weigh the Pros & Cons**

Regardless of the risks involved in working with third parties, nearly all providers need to. So if you’re thinking about using a cloud system, experts offer the following thoughts on weighing both the risks and benefits of using a cloud service vendor:
1. **Require the vendor to sign a BAA.** Although merely signing the BAA won’t ensure that the cloud vendor actually complies with HIPAA, you still need to have any third party with access to PHI sign a BAA.

And be sure to verify whether the cloud vendor provides appropriate breach monitoring. You must “understand and evaluate the cloud vendor’s breach response plan,” according to an article by attorneys James Wieland and Joshua Freemire for Ober Kaler Attorneys at Law.

2. **Don’t use free cloud storage versions.** Free cloud storage, like any other free version of an application, “typically lack[s] the full features and functions of paid versions,” Roman warned. And those features and functions include security safeguards.

Also, consider the vendor’s individual industry background, Wieland and Freemire advised. “Not all vendors are created equal in this respect,” and you want a vendor with experience in dealing with regulated information, ideally PHI. These vendors are more likely than less-experienced ones to understand HIPAA security requirements and to have HIPAA-appropriate mechanisms in place.

3. **Ensure all data is encrypted.** Make sure that the vendor encrypts data both “in motion” and “at rest.” You need to be certain “that as you are uploading and downloading data, as well as while being stored within the cloud provider’s data centers, data is being encrypted using the highest level of data encryption,” Roman stressed.

Additionally, make sure that the vendor truly segregates your data (especially your PHI) from the data of the vendor’s other clients, Wieland and Freemire advised. “One of the characteristics of the public cloud — multi-tenancy — makes cloud providers a target of choice for hackers, since the data is Internet accessible and data of a number of targets is available through one source, due to what is referred to as physical and electronic proximity of the data of a number of clients of the vendor in one system.”

4. **Password-protect your documents.** Also, you can add an extra security step by password-protecting your documents, which will provide an additional safeguard, Roman suggested.

5. **Create an automatic deletion policy.** Depending on how you need to utilize the cloud services, you could consider using the cloud for only temporary storage of data. This will minimize the data’s exposure.

“If the primary reason for using the cloud is to upload and download documents to share … create and enforce an automatic deletion policy that will delete any data stored in the cloud after a specified period of time,” Roman suggested.
6. **Implement a private cloud.** “In most cases, the safest place to store data is behind your company’s firewall, in your data center,” Roman said. “There are several private cloud data storage options that can be implemented within your data center that work identically to a Dropbox or Box offering.”

The private cloud presents a more secure environment, Wieland and Freemire agreed. “Bear in mind, however, that vendors of private cloud systems may reserve the right to shift data to a public cloud environment if overall demands on the vendor’s system require such a step.” So make sure you explicitly ask the private cloud vendor about this.

7. **Know where your data will be stored.** Most importantly, make sure that the cloud vendor will not transmit or store your data outside the United States, where the federal government has no jurisdiction to help if you have a problem with the vendor, Roman stated.

**Dig Deeper Into Vendors’ HIPAA Compliance**

If you decide to move forward with using cloud storage, you must choose your vendor wisely. “We are seeing an increase in data breaches caused by vendors, so be cautious when choosing a vendor,” Freedman cautioned.

But how can you assess a vendor’s compliance with HIPAA? Freedman provided the following tips:

- Make sure the vendor will sign a BAA and will indemnify you fully for any and all data breaches that the vendor causes (not just up to the amount of the contract).
- Ask the vendor to see its HIPAA Compliance Program. “If they look at you sideways, that is a clue that they are clueless,” Freedman pointed out.
- For a high-risk vendor, ask to see an executive summary of its security risk assessment.
- Have the vendor complete a security audit questionnaire.

**Do Your Homework Before Jumping In**

“Providers interested in cloud computing will have to learn a fair amount about a new technology without forgetting what they already know about HIPAA compliance and information security, Wieland and Freemire contended.

**Bottom line:** “Cloud computing has much to offer, and, with a careful assessment of risk and benefits (as well as a careful review of contractual and policy language) providers can take advantage of new technologies to increase data speeds, increase mobile data access, and decrease hosting and storage costs,” according to Wieland and Freemire.
Get Ready For More HIPAA Security Scrutiny From OIG In 2015

The HHS Office of Inspector General (OIG) has released its annual Work Plan for fiscal year (FY) 2015, and HIPAA security is on its “hit list.”

The OIG’s Work Plan lists items like analyzing the IT security of community health centers and reviewing controls over networked medical devices at hospitals. The OIG wants to determine whether the Centers for Medicare & Medicaid Services’ (CMS) oversight of hospitals’ security controls over networked medical devices is sufficient to effectively safeguard electronic protected health information (ePHI).

“Computerized medical devices, such as dialysis machines, radiology systems, and medication dispensing systems that are integrated with electronic medical records (EMRs) and the larger health network, pose a growing threat to the security and privacy of personal health information,” the OIG states in its Work Plan. “Such medical devices use hardware, software, and networks to monitor a patient’s medical status and transmit and receive related data using wired or wireless communications.”

Beware Of Identity Theft Rings Stealing Your Patient Data

They might not be looking for medical information, but identity theft criminal rings are aggressively seeking your patients’ personal information.

On Nov. 3, 2014, Miami-based Jessie Trice Community Health Center, Inc. (JTCHC) announced that an identity theft criminal operation stole its patients’ personal information. Law enforcement authorities alerted JTCHC of the data breach. The Federal Bureau of Investigation (FBI) and Internal Revenue Service (IRS) are investigating the breach.

Although the ring did not obtain or compromise any medical records, the theft included 7,888 patients’ names, birth dates, and Social Security numbers. JTCHC notified all the affected patients of the data breach and is working with a data-breach response vendor to help their patients.

JTCHC is also “working vigorously and diligently assessing how to mitigate future risks to all patients and has implemented new procedures and protocols to protect patient information so that this type of theft cannot reoccur,” President and CEO Annie Neasman said in the announcement.
HIPAA Compliance: Weigh The Pros & Cons Of Communicating With Patients Via Texting

*Check out these ‘HIPAA compatible’ text messaging Apps.*

Text messaging is a common communication method for most Americans these days, but text communications that include protected health information (PHI) can pose a whole host of risks to privacy. Don’t risk a HIPAA breach with your text messages — here are the decision points you need to consider before using texts to communicate with patients and what you can do to mitigate the risks.

**Is Texting Right for Your Patients?**

“With the proliferation of mobile technologies and a steady shift toward smartphone interactions as a predominant mode of communications for many consumers, you may be considering texting as a more effective and efficient way to communicate among providers and/or with patients,” attorney Michelle Caswell, JD said in a blog posting for Clearwater Compliance LLC.

Texting is a fast way to communicate short messages to patients, such as updates and schedule changes, according to Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT.

And in some cases, texting may be more appropriate than sending an email or making a phone call, Sheldon-Dean points out. For example, texting can be more discreet and private than a phone conversation that someone could overhear. Texting is sometimes quicker than a phone call for short messages and can provide accurate information not dependent on voice.

In the past, many healthcare professionals would use pagers, but now texting has become a better option, Sheldon-Dean says. Many paging operations are moving to texting now, and texting is more interactive than paging.

**2 Big Issues with Texting**

The biggest, overall HIPAA-related issues with text messaging are privacy and documentation. Consider these issues carefully before deciding to use texting in your patient communications.

1. **Privacy:** Patients may not appreciate the risk of privacy loss through texting, Sheldon-Dean warns. Also, texting is a new technology and people will not understand it fully for quite some time.
“HIPAA does require you to do your best to meet patient preferences for communication methods,” Sheldon-Dean reminds. You must use a Risk Analysis to evaluate and explain the risks to patients, Sheldon-Dean advises.

2. Documentation: “Regular texting doesn’t provide a paper trail of conversations and contacts,” Sheldon-Dean says. If a communication is part of patient care, you must document it properly, and that requires more than regular texting. A secure, traceable texting technology is important when you’re texting medical record information.

If PHI is included in texts between you and your patient, “the messages may be subject to HIPAA in more ways than just security,” Caswell agreed. You may need to save texts for a legally required time period, allowing the patient to access and amend the text messages. And if you choose to delete the texts for security purposes, you may be violating HIPAA’s retention requirements.

Weigh the Risks of Texting Carefully

Many things can go wrong when it comes to text messaging with patients or other providers. For example, you might end up providing information to the wrong person due to poor authentication and access controls, Sheldon-Dean warns. This situation would lead to a “small” breach and a healthcare threat.

Or you could accidentally provide incorrect information about a patient, “perhaps by faulty authentication or a poorly performing App, causing a healthcare threat,” Sheldon-Dean cautions. And if you use an unsecured text messaging App, data may remain and be accessible on systems.

Another problem: What if the patient loses his device, exposing his data? This is the patient’s problem, but what if the device loss potentially exposes additional data or provides faulty data? What if you or one of your employees loses control of a device, potentially exposing extensive data? This is a big problem. And an even bigger problem is if the device loss potentially provides access to your systems.

Follow 5 Tips to Create Effective Texting Policies & Procedures

If after weighing the pros and cons your practice decides to communicate with patients via text, you should implement policies and procedures that establish safeguards and reduce liability exposure, Caswell said. Caswell offers the following tips for creating solid policies and procedures:

1. Include only non-urgent information. If you’re texting with a patient, include only non-urgent information like appointment reminders or prescription refills. If you have a secure patient portal, you could use text messaging simply to alert the patient to a message in the portal.

2. Don’t communicate identifiable information. Avoid texting any information that is specific and identifiable to the patient, such as patient ID numbers, treatment details or names of conditions.
3. **Double-check the number.** Always ensure that the number you’re using to contact the patient is the appropriate number to send texts.

4. **Include treatment texts in the medical record.** If texts are related to patient treatment, you must include the contents of the texts in the patient’s medical record.

5. **Put a mobile device management plan in place.** Your mobile device management plan should include:
   - Encryption of mobile devices;
   - Password protection;
   - Guidelines on whether employees can use their own devices or if they must use only company-owned devices;
   - Monitoring/audit of all text messages; and
   - Use of applications that will allow the phone to verify a device prior to sending (similar to credit card companies that allow you to verify your phone prior to sending data).
Try A Secure Texting Solution: 15 Available Apps

Some texting Apps even provide a signed BAA for your convenience.

If you decide to communicate via text messaging with patients, or with other providers, your best bet to fend off a data breach is to ensure that the messaging application is as secure as possible.

Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT, suggests the following texting Apps for more secure communications:

- **Cortext by Imprivata**: This texting solution comes in several versions and the free App provides a secure channel. You can also get upgrades to the App that will provide documentation, reporting, etc. Go to www.imprivata.com/products-solutions/secure-communications/secure-texting-practices.
- **TigerText**: This is a free App that provides a secure channel. Go to www.tigertext.com/messaging-for-healthcare.
- **DocHalo**: Check out this secure App at www.dochalo.com/index.html.

The TeleMental Health Institute also offers the following list of companies that provide secure texting with “HIPAA compatibility,” and some of which also provide a signed business associate agreement (BAA):

- **Cureatr** https://cureatr.com/
- **DocsInk** www.docsink.com/docsink_hipaa_compliant_texting.html
- **HipaaChat** www.hipaachat.com/security/
- **Hippomsg** http://hippomsg.com/features/
- **Medigram** https://medigram.com/
- **miSecure Messages** http://www2.misecuremessages.com/how-it-works/security
- **On Page** http://onpage.com/home/industriesserved/healthcare/
- **Spok Mobile** www.spok.com/solutions/mobile_communications/hipaa-compliant_texting
- **Startel Secure Messaging** www.startel.com/solutions/unified-communications/startel-messaging-service
- **ZIPIT** http://zipitconfirm.com/
Implement These Measures To Avoid An Attack On Your Windows Systems

Following the recent hacker attack on Sony, the U.S. Computer Emergency Readiness Team (US-CERT) issued an alert on “targeted destructive malware” for Windows systems. The alert informs you of what you can do to help prevent an attack like the one on Sony.

Specifically, the Dec. 25, 2014 alert describes a Server Message Block (SMB) Worm Tool, which cyber threat actors are using to conduct cyber exploitation activities. Hackers used the SMB Worm Tool against Sony. The SMB Worm Tool is equipped with a Listening Implant, Lightweight Backdoor, Proxy Tool, Destructive Hard Drive Tool, and Destructive Target Cleaning Tool.

“Due to the highly destructive functionality of this malware, an organization infected could experience operational impacts including loss of intellectual property and disruption of critical systems,” US-CERT stated. For healthcare organizations, this malware could also cause exposure of protected health information (PHI).

The alert also contains steps that your organization can take to prevent infection and protect computer networks.

“Healthcare institutions would be well advised to review the bulletin and implement measures accordingly,” warns Jim Sheldon-Dean, founder and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT. “Make sure your technical security folks know about this!”

**Link:** You can access the US-CERT alert (TA14-353A) at [https://www.us-cert.gov/ncas/alerts/TA14-353A](https://www.us-cert.gov/ncas/alerts/TA14-353A).
Reader Questions

Is Faxed Information Considered ePHI?

**Question:** If we fax a document containing a patient’s medical information from one place to the other and it goes to the wrong location, is that considered electronic protected health information (ePHI)?

**Answer:** If the document is simply going through a straight fax machine to another, that’s not considered ePHI, answers Jim Sheldon-Dean, founder and director of compliance for Lewis Creek Systems, LLC in Charlotte, VT.

Still, this situation is considered a breach, although it basically winds up being a Privacy Rule violation, Sheldon-Dean says. And so in this case, you had information that went to the wrong location, which means you had an improper disclosure.

This is the kind of situation that you would need to report to the individual and to the U.S. Department of Health and Human Services (HHS) as a small breach that affects just one individual, Sheldon-Dean instructs.

But if the document originated from a computer to a fax server and was faxed to the wrong location, this is considered ePHI, Sheldon-Dean warns. When you have a computer-generated document going into a fax server, you must treat that as electronic information under the Privacy and Security Rules.

How Often Must You Change Your Passwords?

**Question:** We are having a little disagreement in our office. How often should we change our computer and electronic health record (EHR) application passwords? Some of us say every month, while others are saying only every four to six months.

**Answer:** The short answer is that you should change your passwords quarterly. Users should change their passwords regularly and should be prevented from reusing at least their last two or three passwords, instructs the HHS Office of the National Coordinator for Health Information Technology (ONC).

You should ensure that your systems are configured so that passwords must be changed on a regular basis, ONC stresses. “By requiring passwords to change quarterly, you help prevent passwords from being discovered and used illicitly.”

Also, remember to ensure that staff members create strong passwords. According to ONC, strong passwords are at least eight characters long, and include a combination of upper and lower case letters, at least one number, and at least one special character like a punctuation mark.
What Kind Of Risk Does Using Private Email Accounts Pose?

**Question:** Our provider group has a secure system for encrypting all outgoing emails from our internal email system. But the physicians are sending protected health information (PHI) from the internal email to their home email (HotMail, Gmail, etc.). Is this putting our company at risk?

**Answer:** Yes, this is definitely a risky behavior, answers Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, VT. “What happens is those messages wind up on the HotMail or Gmail servers and can wind up being preserved and not really very well protected.

**Pitfall:** And depending on exactly how you’re using HotMail or Gmail, these email providers may even have as part of their terms of service a stipulation that they have a right to look at whatever information that passes through your account, Sheldon-Dean warns. You must try to get the physicians to not use their own personal email accounts, because those email services are not secure.

**What’s more:** Some organizations even report usage of personal unencrypted email accounts as an official breach, Sheldon-Dean adds. “It’s up to your attorneys to decide whether that’s something you need to report as a breach or not — just the fact that [the physicians] have been using those email accounts. So you’re certainly in a dangerous situation right now, and you need to consider it very carefully.”

Can Patients Waive Encryption For B2B Communications?

**Question:** I understand that a patient can request that we send to them unencrypted emails, but what about “business-to-business” (B2B) communications? Can a patient authorize our practice to email back and forth with another provider or entity without encrypting the communications?

**Answer:** No, the patient cannot say it’s fine for those B2B communications to happen via plain emails, states Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, VT. “That would amount to patients giving up their rights under HIPAA to have that information protected.”

Patients are allowed to ask for plain email communications when it’s with themselves, because that’s exerting their rights for how they would like you to communicate with them, Sheldon-Dean explains. But “as far as business communications are concerned, those should be encrypted communications. You shouldn’t be using plain email for transmitting PHI between business entities.”
Can You Reuse A Mobile Device Containing ePHI?

**Question:** Can we reuse or dispose of a mobile device that has stored health information on it?

**Answer:** Yes, but first you must remove the electronic protected health information (ePHI) stored on the mobile device, according to the HHS Office of the National Coordinator for Health Information Technology's (ONC). Or, you need to destroy the mobile device itself before disposing of it.

You must destroy all PHI in electronic form to make the information unusable, unreadable, or indecipherable to unauthorized persons, ONC stresses. Proper destruction methods may include, but are not limited to:

- Clearing (using software or hardware products to overwrite media with non-sensitive data);
- Purging (degaussing or exposing the media to a strong magnetic field to disrupt the recorded magnetic domains); and
- Destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

For more specific guidance on how to destroy ePHI contained on a mobile device, read "HHS Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals" at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html. Also check out guidance on the proper disposal of ePHI at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf.

What Are The HIPAA-Compliance Needs For Text Messages?

**Question:** If we wanted to start sending text message notifications to patients just regarding that a statement is now available for viewing, how would that play into the HIPAA rule? What do we need to do in terms of compliance if we’re not really providing patients with any information other than the fact that a statement is available for viewing?

**Answer:** “That’s a perfect example of the kind of information that you should be allowed to communicate via text message,” says Jim Sheldon-Dean, founder and director of compliance services at Lewis Creek Systems, LLC in Charlotte, VT. But this situation does indicate that you have a patient-provider relationship with the individual, which is considered protected health information (PHI) under HIPAA.

**What to do:** You should ask the patient’s permission to have that text-message communication, Sheldon-Dean advises. You need to ask the patient whether he is okay with text communications, advising him that the text messaging is not secure so the message itself could be exposed. “But obviously, it’s a very minimal kind of risk,” he notes.
And generally, patients will most likely agree to receiving these types of text messages. “I don’t think you even necessarily have to have a copy of a written signature, so long as you have a documented conversation for something that simple and straightforward,” Sheldon-Dean recommends. “I think that would be a reasonable thing to do.”

**Can You Email Blank Forms To Patients With A Simple ‘Okay?’**

**Question:** I work in a pain management clinic, and we want to start sending patients their information by email. Specifically, we want to send an eight-page registration form. Currently, when we send the registration forms, we just ask for the patient’s email address. Should we just ask the patients whether it’s okay to send them these forms via email and document it somewhere on our files that we’ve gotten a verbal okay to email them?

**Answer:** “Yes, I think that would be a reasonable thing to do,” answers Jim Sheldon-Dean, HIPAA expert and director of compliance services for Lewis Creek Systems LLC in Charlotte, VT.

In this case, you’re just sending patients the forms, which are blank, “so you’re really not revealing too much in that case,” Sheldon-Dean notes. There’s minimal risk involved.

If you just ask the patients for their permission to email and document that they’ve agreed to that, then you can go ahead with the emails and you have that documentation, Sheldon-Dean says. “That seems like a reasonable use.”

**Are There Security Rule Considerations For Telemedicine?**

**Question:** One of our practice’s nurse practitioners provides occasional telemedicine services via videoconferencing. Does the Security Rule apply to these sessions?

**Answer:** The HIPAA Security Rule does not cover telemedicine treatment sessions provided by videoconferencing, according to the American Speech-Language-Hearing Association (ASHA).

The Security Rule states that “because ‘paper-to-paper’ faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail were not in electronic form before the transmission, those activities are not covered by this rule.”

**Caveat:** But if you record the session and save a copy, the saved version would be subject to Security Rule provisions, ASHA says.

“Regardless, the treatment session and all related information and documentation are subject to the Privacy Rule provisions,” ASHA notes. “To ensure the patient’s privacy during treatment sessions, clinicians should consider the use of private networks or encrypted videoconferencing software.”

© 2015 codinginstitute.com
**Is Sending An Unencrypted Email An Automatic Breach?**

**Question:** If we use unencrypted email to send a message with a patient’s protected health information (PHI) to another doctor’s office, is that a reportable breach?

**Answer:** Unfortunately, there’s no clear-cut decisive answer to this, says Jim Sheldon-Dean, founder and director of compliance for **Lewis Creek Systems LLC** in Charlotte, VT. “I see plenty of reports of breaches that are taking place that involve this kind of communication.”

Many lawyers will say that the proper way to interpret a situation where you’ve sent an unencrypted email containing PHI is as a breach, Sheldon-Dean notes. And beyond the unencrypted email itself, you need to understand that these messages wind up on email servers and can remain there for quite some time after you send or read the messages.

**Bottom line:** “In that case, the information winds up being maintained and isn’t necessarily being secured,” Sheldon-Dean warns. “So you want to avoid … using those kinds of services as much as possible unless you use a secure version. Otherwise, you’re leaving yourself open to a violation.”
Get All the Information You Need In 2015 with 2015 Physician Bundle

CPT®, ICD-9 and HCPCS – With 2015 Physician Bundle
Comprising Three Power-Packed Coding Books.

Our comprehensive three-in-one 2015 book bundle covers:

• **2015 AMA CPT® Professional**
  A trusted resource that will help you correctly interpret and report medical procedures and services in 2015 by providing you with up-to-date CPT® codes, descriptions, guidelines and easy-to-understand illustrations.

• **2015 HCPCS Level II Expert**
  This comprehensive reference guide will help you select the correct HCPCS Level II code for accurately reporting medical supplies to Medicare.

• **2015 ICD-10-CM Code Set**
  This book will get you the complete diagnostic code set used in physician offices and outpatient facilities. You can quickly look up the latest official government version of ICD-10-CM code set (with color-coded symbols, alerts, and illustrations).

Visit www.codinginstitute.com/2015-physician-book-bundle-1.html to learn more or call at (866)-228-9252 to know more about 2015 Physician Bundle
2222 Sedwick Drive, Durham, NC 27713
Phone: 1-800-508-2582
E-mail: service@codinginstitute.com

$149.00