

PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

To Friend or Not to Friend: New Developments that Impact Social Media's Place in the Office

*Reprinted from the North Carolina Bar Association's
Employment Law Newsletter, September 2010*



by Elizabeth Johnson

Employers and employees are continuing to grapple with the use of social media in the workplace. On the one hand, social media can be a powerful online marketing tool that provides access to 500 million users (and that number accounts for Facebook users, alone). On the other hand, social media is also a demonstrated leading contributor to security incidents and data leaks. This article presents several recent developments and perhaps overlooked legal constraints that bear on the use of social media in the office.

Vetting Job Applicants

Human resources staff may be in the habit of reviewing applicants' Facebook, MySpace, or LinkedIn pages, or using those sites to recruit new hires. Applicants' posts to social media often reveal "personal characteristics" and "modes of living," which constitute "consumer reports" governed by the federal Fair Credit Reporting Act (FCRA). As a result, assembling reports about applicants based on social media content and regularly disseminating those reports to third parties (including affiliates) can render an organization a "consumer reporting agency." When such reports are used in connection with making employment-related decisions, both the reporting agency and the user of the report can face potential liability if the reporting and decision making was not performed in compliance with the FCRA.

Monitoring and Discovering Employee Use

Monitoring employees' use of the Internet and electronic communications always presents legal risks and compliance is often uncertain, given the maze of case law on the subject. Monitoring employee use of social media has only more recently become the subject of litigation, but some cases have been decided that are beginning to illuminate the boundaries of employer monitoring. In *Pietrylo v. Hillstone Restaurant Group*, (D.N.J. June 16, 2009), a jury entered a verdict against an employer that accessed a private MySpace user group established

by employees for the sole purpose of venting about their employer. This "venting" was allegedly done all on personal time. Management became aware of the user group when a hostess with authorized access to the page showed it to a supervisor at a party. The hostess was subsequently asked to provide her log-in credentials to a second supervisor (she later testified that she complied out of fear for negative job-related repercussions). Two members of the user group were fired and then filed suit, alleging violations of their common law right to privacy, their freedom of speech, the federal Stored Communications Act (SCA), and the New Jersey statute on unlawful access to stored communications. The plaintiffs were successful on the latter two charges, as the jury found that the defendants violated the SCA and the state law equivalent by intentionally accessing the MySpace page (and communications made on it) without authorization.

In *Crispin v. Christian Audigier Inc.* (C.D. Calif. May 26, 2010), a similar result was produced when a federal district court determined that the SCA applies to social media posts, provided that the poster had established privacy settings intended to keep other users from viewing the content without authorization. In this case, the defendant sought access in discovery to any communications made by the plaintiff using MySpace and Facebook if those communications in any way referred to the defendant. Although a magistrate initially sided with the defendant, the district court ultimately reversed, finding that the SCA applied to the communications because the social media site provid-



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601 / P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

ers were electronic communication services. Accordingly, the content in question was electronically stored within the meaning of the SCA and thus could not be accessed without authorization. As a result, messages sent using the sites and content posted but visible only to a restricted set of users (i.e., Facebook friends) were both subject to the SCA and the court disallowed the defendant's discovery request.

These cases do not address other interesting questions, like the protections afforded to arguably non-communicative social media content, such as a user's list of online contacts. And is the analysis affected when a user's online contacts number in the hundreds or even thousands, rendering the communications much less private? In any event, employers will want to follow this line of case law and consider its application to their employee monitoring policies.

Endorsements

Last year, the Federal Trade Commission (FTC) revised its *Guides for the Use of Endorsements and Testimonials in Advertising* to illustrate how those guidelines would apply to endorsements made in the online context. In its *Guides*, the FTC clarified that employees posting online content that endorses or otherwise promotes their employer's products or services must disclose the employment relationship. The rationale is that the employment relationship would be a material factor to the consumer in evaluating the endorsement. As a result, employers should caution their employees against endorsing their products and services using social media unless they also mention their employment.

Although compliance with the *Guides* is voluntary, the FTC has stated that it will treat activities inconsistent with its *Guides* as a violation of the Federal Trade Commission Act. The FTC has already demonstrated its willingness to do so, charging Reverb Communications with a violation of the FTC Act after its employees took to social media sites to promote video games developed by companies Reverb represented. The employees' posts, such as "amazing new game" and "really cool game," did not disclose that the posters were employed by Reverb and thus, in the FTC's view, constituted unfair or deceptive trade practices.

Special Privacy Considerations for Regulated Organizations

Social media is presenting special problems for organizations that are highly regulated on privacy matters - namely health care providers and financial institutions regulated under HIPAA and the Gramm-Leach-Bliley Act (GLBA), respectively. By virtue of the scope of those regulations, virtually any information about an individual who has received services from those organizations is subject to very restrictive limits on disclosure. As a result, employees of these organizations must be strongly cautioned against making inappropriate disclosures through social media. A remarkable number of such organizations have already experienced breaches as employees, emboldened by social media's veil of seeming anonymity, take to the Internet to vent about patients and customers, ignorant or careless of the legal violations they are committing.

In light of the popularity and pervasiveness of Facebook and other social media sites, every organization needs a clear, documented policy to govern their employees' virtually inevitable use of these sites. In light of the constantly-evolving nature of these applications, and their attendant threats and risks, that policy should be revisited often. Employers and employees need to consider a variety of topics, including those described above. As to each topic, there may be no clear right or wrong approach, but rest assured that one thing is clear: the worst position with regard to social media is to say nothing.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

“Reasonable” Security: The FTC Requires It, But What Is “Reasonable” Security?

by *Kate Paradise*



The Federal Trade Commission (FTC) has taken more than 25 actions alleging that inadequate information security constituted an unfair trade practice in violation of the FTC Act. In these enforcement actions, the FTC has targeted corporations for failure to implement “reasonable and appropriate security measures” and requires in the subsequent consent orders that the organizations implement a comprehensive written information security program and submit to third-party assessments of that program every other year for the duration of the order (usually 20 years).

But what does “reasonable security” really mean? And more important, how do you apply reasonable security measures to your business? Although you can rely to some extent on technology standards and industry best practices, information security law has evolved to a point where case law and FTC enforcement actions are a source of some suggestions.

A recent action against Twitter illustrates that having a defensible password security policy is a crucial security element. The FTC faulted Twitter for permitting “weak” administrative passwords — consisting of only common dictionary words written using all lowercase letters, and containing no numbers or symbols. In addition, Twitter’s system failed to lock out users after multiple unsuccessful login attempts. Lack of reasonable safeguards allowed an automated password-guessing program to gain access to the Twitter system after thousands of login attempts. In a separate breach, a hacker who compromised a Twitter employee’s personal e-mail account was able to guess a Twitter administrative password because two similar passwords were stored in plain text within that employee’s e-mail. The FTC cited storage of passwords in an e-mail account among the “unreasonable” practices Twitter employed.

In another enforcement action, the FTC pursued restaurant chain Dave & Buster’s for failure to provide reasonable and appropriate security for credit and debit card data stored on its networks. Credit card information that was collected at in-store terminals, transferred to in-store servers, and finally transmitted to a third-party credit card processing company was intercepted by hackers because the company failed to detect and prevent unauthorized access to the computer net-

works. The FTC faulted Dave & Buster’s for failing to conduct security investigations, failing to monitor system logs, and for not using readily available security measures to limit access to its computer networks through wireless access points. The FTC specifically noted the lack of data loss prevention software and an intrusion detection system when alleging the unreasonableness of Dave & Buster’s information security program.

These and other FTC cases provide insight into the policies and practices that are necessary to support a “reasonable and appropriate” information security program. Demonstrating that you have implemented such a program is crucial to mitigate the risk of an unfair trade practices charge by the FTC. Our Privacy and Information Security Practice can help you evaluate your information security program to ensure that it addresses your compliance and risk objectives, as well as areas highlighted by past FTC and other government agency enforcement actions.

Kate Paradise may be reached at 919.783.2886 or kparadise@poynerspruill.com.



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Do You Know Who's Got Your Data? It's Time to Pin Down Your Vendors and Make Sure They Toe the Line on Information Security



by Elizabeth Johnson
and Pam Scott

Your organization may be minding its information privacy and security Ps and Qs, but are your vendors? From your payroll provider to your copy service, from your data hosting provider to your records disposal service, dozens of third parties handle personal information on your behalf, and your information security program is only as good as theirs.

Identifying these service providers and obligating them by contract to implement necessary security measures is mandatory in many states and thus necessary to comply with law. Forty-six state laws and several federal rules require your organization to notify affected individuals of any breach your providers may cause, making appropriate diligence and contracts necessary to avoid costly data breaches and related risks. The Ponemon Institute's 2009 study of data breach costs indicates that 42 percent of the breach incidents studied were caused by third-party mistakes, and the involvement of those third parties increased the cost of the breaches by 12 percent.

Examples of contractor missteps that have caused recent data breaches include:

- Tossing boxes filled with the personal information of tens of thousands of individuals into open dumpsters and recycling bins.
- Publishing login credentials in a brochure and on the Internet for a secure website that contained hundreds of thousands of individuals' personal information.
- Leaving an unencrypted laptop containing personal information of thousands of individuals in a car, from which it was stolen.
- Losing a shipment of computer backup files and unencrypted CDs containing personal information for tens of thousands of individuals.

In all cases, the organizations that hired these contractors were obligated to give notice of the breaches. These incidents typically result in bad press, government enforcement actions, lawsuits, and lost productivity while the organization responds to the breach. The average cost to respond? Over \$6.5 million.

So how do you comply with information security laws and avoid cleaning up a contractor's costly data breach? The most effective solution is to implement a comprehensive privacy and security compliance program that includes vendor management. The first step to vendor management is to actually identify all the contractors that access your data. The next step is to conduct appropriate diligence on their security programs, which can consist of a questionnaire, a conversation, an onsite review – any level of checking is better than doing nothing.

Arguably the most crucial step in vendor management is executing a strong contract that is agreed to before the first piece of sensitive data reaches the contractor's hands. As above, a number of states require contracts by law when a service provider will have access to or dispose of personal information. Contractual issues to consider include control of subcontractors a service provider may use; compliance with applicable information privacy and security laws; appropriate security measures such as encryption and system activity review; notice and cooperation in situations involving data breaches; the right to audit the contractor's compliance and security program; and appropriate allocation of responsibility and liability in the event of a breach.

Our Privacy and Information Security Practice can help you develop an appropriate vendor management program, streamlining diligence efforts, addressing common contracting issues, and assisting you in negotiations.

Elizabeth Johnson may be reached at 919.783.2971 or ejohnson@poynerspruill.com. Pam Scott may be reached at 919.783.2954 or psscott@poynerspruill.com.



Poyner Spruill ^{LLP}
ATTORNEYS AT LAW



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Are Facebook's Woes a Preview of Things to Come for Amazon?

Reprinted from TechJournal South, July 28, 2010



by Elizabeth Johnson

Most of you are familiar with the controversy over Facebook's revision of its privacy settings, with the default settings generally causing users to share more information about themselves with more people and, in some cases, with everyone on the Internet.

Around the same time, another controversy arose involving Facebook that received less attention: The social media site's sharing of individual user information with advertisers in apparent violation of its privacy policy.

Facebook's Legal Troubles...

Now, to be fair, other social media sites like MySpace are alleged to have engaged in the same behavior and the disclosure was potentially inadvertent. Although there are variations, the disclosure typically proceeds down a similar path. First, a social media user logs into their page and, while there, gets interested in an ad on the page.

The user clicks on the ad. That click automatically results in the social media site (in this case, Facebook) sending to the ad provider a stream of information. In the case of most websites, that stream of information ordinarily does not include anything about the user at an individual level. For example, the stream includes the website URL the user visited at the time he clicked the ad.

But, in the case of social media sites, a user's profile page often includes their username within the URL so, if the user clicks on the ad from his profile page, the stream of information sent to the advertiser will include his username. If the username is the user's actual name, then the advertiser now has his name as well.

In either case, the allegation is that the advertiser can now identify the individual user who clicked on the ad and may go back to his profile page on the social media site and view other information about him. And, in Facebook's case, since the site recently reset default privacy settings to make ever-greater personal information available to a larger audience, that advertiser will find more personal information now than it might have in the past.

Facebook faces lawsuit

As a result of these disclosures, Facebook faces a user's lawsuit claiming breach of contract due to its actions. The theory goes like this: Facebook promised users in its website privacy policy that it would never share their personal information with advertisers unless the user first consented. In spite of that promise, Facebook sent personal information to advertisers without consent in the manner described above.

The plaintiff is claiming that violation of Facebook's privacy policy is a breach of contract. Similar disparities between what a website privacy policy says as compared to what the website provider actually does have formed the basis for similar private actions and also government enforcement, particularly "deceptive trade practice" claims by the FTC.

In the FTC cases, providers often settle the FTC's claims by agreeing to FTC review of all proposed consumer privacy notices, disgorge any moneys earned from the alleged deceptive practices, and retain for the FTC's inspection copies of any invoices, records or communications related to any disclosure of information to a third party. As a result, violating your own privacy notice, even inadvertently, can be an expensive proposition.



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601 / P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Another case: Amazon vs. North Carolina

Now let's consider these developments in the context of another recent privacy-related case: Amazon's dispute with the state of North Carolina over the state's requested release of customer records. Presumably, the state would like to know the individual identities of Amazon's customers in North Carolina so that the state can review whether those shoppers paid sales tax in connection with their purchase of goods.

The controversy over whether such purchases are subject to state sales tax has a fairly long and contentious history, with Amazon closing its North Carolina affiliates in June 2009 to bolster its argument that it has no obligation to charge North Carolina sales taxes.

In the current case, Amazon is fighting the state's request for customer records, in part by claiming that there are privacy concerns with releasing customer information to the state. While some may judge this assertion by Amazon as nothing more than a smokescreen to fight what is really its staunch aversion to charging state sales tax, this view is too cursory.

As discussed above, a website operator can face real liability when its disclosures of information are contrary to the promises it makes to users in its website privacy policy. So what does Amazon's privacy policy say to users about whether it will disclose information to the government? The most relevant promise seems to be, "We release account and other personal information when we believe release is appropriate to comply with the law"

Court order ramifications

If Amazon had simply handed over the information because North Carolina asked nicely, it would be a little difficult to say that it had lived up to the promises in its privacy policy (and, yes, these statements often are enforced as promises in legal disputes) because the disclosure would arguably not have been "appropriate to comply with the law."

But what if Amazon, as it is doing here, fights the request in court but, despite its arguments against disclosure, is ordered by the court to hand over the information? In that case the disclosure is more clearly necessary to comply with law and, among other things, provides Amazon with a clearer defense to any customer-filed complaint alleging it violated its privacy policy by disclosing the information.

What are the chances of an Amazon customer filing a privacy-related claim against it in connection with disclosures of information to state government? Hard to say, but it usually depends on how annoyed the customer is by the objectionable disclosure and what level of harm he actually suffered.

In Facebook's case, its user filed a lawsuit over a seemingly inadvertent disclosure of demographic information to advertisers that would, at worst, result in the user receiving unwanted ads.

Amazon's Quandry

If that behavior is enough to prompt a lawsuit, imagine the ire of Amazon customers who find themselves outted by the company to state tax auditors who will, as a result of that disclosure, potentially demand that those customers pay past due sales taxes and subsequent penalties.

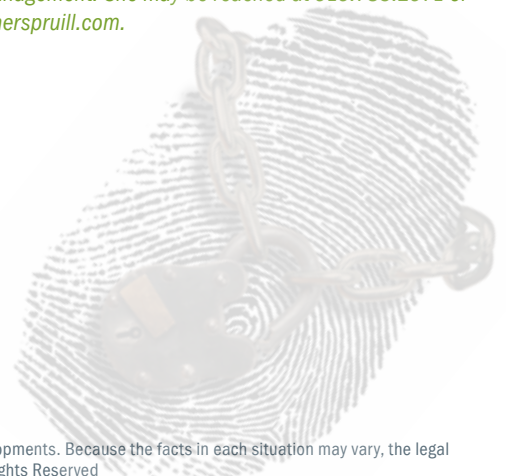
Now consider the scale of Amazon's quandry. If North Carolina succeeds in its request, can other states be far behind, particularly now that state coffers are running on empty?

So what's the lesson here for any organization with a website? Be careful with your website privacy policy. In most cases, websites are required to post one in order to comply with law. So, when producing yours, you need to carefully consider your current uses and disclosures of information collected via the site and, ideally, anticipate future uses and disclosures.

All should be disclosed clearly but at an appropriately general level so that users are informed of your practices but you maintain reasonable flexibility.

It's very helpful to be apprised of current case law in this area so that you understand the types of statements that proved problematic for other organizations. And, of course, know which laws apply to your provision of privacy policies to consumers and make sure all the legally-mandated contents are included.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Your Website Privacy Notice: A Publicly Available, Legally Enforceable Promise – Understand the Risk of Overpromising and Underdelivering

by *Kevin Ceglowski*



The Federal Trade Commission (FTC) has taken a number of enforcement actions alleging that seemingly innocuous statements in privacy notices were “deceptive.” In particular, companies that post privacy notices online where the FTC can easily access and analyze them have been subject to enforcement actions when those notices are deemed deficient. If your organization posts a privacy notice online (as it is likely required by law to do), you should be aware of the risks and take steps to prevent FTC scrutiny.

One recent enforcement action against Twitter highlighted a statement in the privacy notice saying, “Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access.” The FTC alleged that statement was deceptive. Many websites say something similar. So what was the problem here?

The problem was that Twitter failed to implement a “reasonable” security program to back up its seemingly innocuous privacy promise, suffered a breach that made headlines, and thus attracted the FTC’s attention. In keeping with the agency’s past enforcement actions, it went straight to the website to see what kind of privacy promises the company made to users. The FTC took issue with Twitter’s failure to keep its system secure when contrasted with the company’s public statement of concern for users’ privacy and charged it with a violation of the FTC Act.

Past FTC enforcement has tended to focus on overly broad and unrealistic promises (e.g., “We will never disclose your personal information to a third party without your consent.”). Such promises, while well-meaning, are impossible to enforce in the current landscape where multiple third parties, ranging from authorized service providers to unauthorized hackers, might access data.

Other problems besides government enforcement actions can also be created by broad privacy promises. A series of bankruptcy cases has created precedent that customer lists may not be sold if that disclosure would be contrary to statements made in consumer privacy notices.

Reading this, you may be tempted to simply take down your website’s privacy notice. Don’t. There are several laws that may require you to provide a privacy notice, and even if the law does not require online posting (some do), posting online remains an easy and inexpensive way to disseminate the notice. A nonexclusive list of laws that may require a privacy notice includes the Children’s Online Privacy Protection Act, the California Online Privacy Protection Act, the Gramm-Leach-Bliley Act, HIPAA, the Fair Credit Reporting Act, state laws governing SSNs, and a slew of international laws. The variety of potentially applicable laws creates a myriad of requirements that can be difficult to navigate and reconcile. Couple that with case law and the pattern of FTC enforcement, and you’ve got a quagmire of legal compliance and risk issues that, if not properly addressed, end up publicly posted on your website, easily available for a regulator’s review.

The attorneys of Poyner Spruill’s Privacy and Information Security Practice can navigate the relevant legal requirements for you to help your organization ensure that its privacy notices meet your compliance objectives without creating unnecessary risks.

Kevin Ceglowski may be reached at 919.783.2853 or kceglowski@poynerspruill.com.



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

Bad Behavior = Bad Press Employee Behaviors That Spell Trouble for Your Information Security Compliance Program



by Elizabeth Johnson

In the world of privacy and information security compliance, your employees can either be your greatest source of risk or your first line of defense. How so? A well-trained employee can be the difference between a significant data breach and a near miss. Recent headlines reveal how employees' inadvertent mistakes led to these widely publicized information security breaches:

- Properly trained, your employees will not inappropriately download and take home with them files that include the Social Security numbers of millions, only to have their laptops stolen. Actual headline: "VA Loses Data on 26 Million Veterans: Employee Claims Laptop With Sensitive Data Was Stolen."
- Properly trained, your employees will not use peer-to-peer file-sharing programs on their work computers, potentially exposing files they did not intend to share. Actual headline: "Widespread Data Breaches Uncovered by FTC Probe: FTC Warns of Improper Release of Sensitive Consumer Data on P2P File-Sharing Networks. (More than 100 organizations were affected.)"
- Properly trained, your employees will not print identification numbers on external mailings that inadvertently expose the recipients' Social Security numbers. Actual headline: "Citi Apologizes for Envelope Gaffe (It affected 600,000 customers)."
- Properly trained, your employees can help ensure that malware does not infiltrate and expose personal information by avoiding suspicious emails and attachments. Actual headline: "U of C Warns Patients After Computer Virus Hits Medical Records."

These headlines reveal a small sampling of the types of incidents that can result in a legal obligation to notify affected individuals of a security breach. These incidents also result in bad press, unwanted attention from regulators, lawsuits, and lost productivity as your organization responds to the breach. Tens of thousands of these incidents have been reported since 2005, when California became the first state to require breach notifications for affected individuals. Forty-five other

states, the District of Columbia, Puerto Rico, and the Virgin Islands have since enacted similar requirements, often requiring notice not only to affected individuals but also to state attorneys general or other regulators.

The Federal Trade Commission and state agencies have been very active in taking enforcement actions based on such incidents, alleging that the inadequate security evidenced by the breach notice letters constitutes an unfair trade practice in violation of federal or state unfair and deceptive trade practices statutes. A common result in FTC cases is a consent order that requires implementation of a comprehensive, fully documented information security program with a third-party audit of that program every other year for 20 years.

So what to do? Unfortunately, there is no easy answer. The best and most effective response is to maintain a comprehensive information security program and fully implement it. It's not enough to have written policies and procedure -- training, including refreshers and reminders, is a critical aspect of an effective information security program.

You can also be on the lookout for the following characters, all well-meaning, and all of whom regularly and unknowingly create risk for their employers. A comprehensive security program with meaningful training will address these behaviors.



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601 / P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

TELECOMMUTERS AND OVERACHIEVERS. These are the employees who take work home, either because they work from home or because they can't get enough of it in the office. Without discouraging either behavior, consider how you can provide them with secure methods to remotely access personal information if necessary to perform their duties. They should not be downloading it to their personal computer, toting it around on portable devices (laptops, thumb drives, CDs, etc.) or in hard copy, or emailing it to their personal email account in order to access it online from home.

THE FACEBOOK JUNKIE. By now, most people realize that social networks are rife with malware, scammers, and hackers. These are sufficient reasons to be cautious in your personal use of social networks (which is done in the office more frequently than might be ideal). But what about legitimate professional use of social networks? If your employees take to the Web, of their own volition or yours, to promote your organization, the FTC has stated that they must disclose their connection to your organization. The rationale is that the employment relationship, if not apparent in the context of a chat room, blog, or social network, may constitute a material fact that would affect a consumer's evaluation of the promotional comment your employee has offered. In addition, organizations are increasingly using social networking as a tool to evaluate potential hires, current employees, and even consumers applying for credit. Depending on the situation, this activity could raise issues under the Fair Credit Reporting Act, the Stored Communications Act, or state privacy tort statutes.

THE MARKETING WHIZ. The best marketers are often the most creative and risk-tolerant. Making your marketing team aware of the overlapping and sometimes inconsistent requirements imposed on direct marketing will help them design a campaign that takes into account your downstream legal obligations. After all, who wants to spend thousands on a campaign to collect mobile phone numbers, only to discover that follow-up text messaging is not an option because the proper consents were not obtained at the time of collection?

THE PROCUREMENT SPECIALIST. It might be low-cost, quick, and efficient in the short term, but relying on a purchase order to govern your relationship with vendors is not appropriate when they handle personal information on your behalf. Your business is responsible for the privacy and security practices of its service providers, including any security breaches caused by them. When these vendors have access to mass quantities of information (e.g., payroll processors, data hosting services, records storage providers, tech support, employee benefits providers,

shredding services, etc.), the risk increases exponentially. A recent study by the Ponemon Institute reveals that 44% of information security breaches are caused by vendors, and the average cost of these breaches was 23% higher. As a result, it's prudent to do some diligence before you hire a provider that will handle personal information. Specific contractual provisions are also a must; a mere representation of compliance with the law will not necessarily address concerns related to confidentiality, secure disposal of information, security breaches, or appropriate security measures. In addition, some federal regulations and certain states require specific contract language, depending on your operations and the nature of the information you provide to vendors.

THE PACK RAT. This employee keeps all her files and correspondence, including email, forever. In addition to increasing your company's costs for storing hard copy and electronic records, this behavior increases costs related to discovery in the event of a legal dispute. Accumulating records containing personal information also increases risk of a security breach and, if one occurs, increases the potential magnitude, since a greater number of people may be affected. An effective and fully implemented records management program will minimize this risk. That program should feature, at minimum, an overarching policy, training for your employees, a legal hold overlay to implement litigation-related preservation requirements, a schedule with retention periods that comport to any legal obligations to maintain certain records, and a disposal policy that complies with state laws mandating destruction procedures for certain records.

In order to effectively implement a comprehensive security program, you need to make sure these and other risks are addressed. You then need to ensure that your program has been communicated to employees, preferably via both written policies and procedures and training.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.



PRIVACY LAW ALERT

from the Privacy & Information Security Group of Poyner Spruill LLP

“Avon calling...” (or is it)? A few reasons to get prepared for social engineering

the new art of parting your organization from its critical information.



by **Elizabeth Johnson**

When summer hits full swing, you can always count on the tried and true activities that are the hallmarks of these warmer months. School is out, families are embarking on vacation, beachgoers are frying in the sun, and thousands of hackers are preparing to converge on Vegas for arguably the world’s largest hacker conference, DEF CON, during which they often wreak a little havoc on the private sector in the name of fun and raising awareness of security flaws.

Is getting hacked not on your list of typical summer fun? Well, to see how you can avoid it, let’s consider just one of this year’s DEF CON events, billed as a “capture the flag” contest. This contest is a bit lower-tech than you might expect. Rather than hunching over a laptop, cracking a sophisticated computer code to gain access to information systems, this year’s participants need only pick up a phone and engage in “social engineering.” In short, the contestants will be showing off their social engineering prowess by calling the target organization and using all their powers of deception and coercion to extract (within 20 minutes) as many “flags” as possible from the unlucky person who answered the phone. The flags are specific items of information, selected in advance by contest organizers. Who is the target? The unfortunate targets have been selected from among contestant suggestions and so could be any organization except (as DEF CON wisely suggests) government agencies or defense contractors. For more on the rules and particulars, visit the contest site.

The first place winner receives a specially branded 16GB iPad and bragging rights. The only “loser” of this contest is the target company, which, in the best case, has a little egg on its face or, in the worst case, suffers bad press and a potential information security breach.

So what to do? Well, you might consider not answering your office phone from July 30-August 1 when DEF CON takes place. You also could cross your fingers and rely on the presumably very low probability that your organization was chosen as a target. But odds are, sooner or later, someone with malicious intent will target your organization, and they may not have the same “fun” motives as DEF CON, which actually does aim to avoid serious damage and legal violations in its contests. My advice is to use eye-catching events like this as an example to management of why appropriate privacy and information

security training is not only appropriate but critically necessary to protect your organization from “attacks” that are now virtually inevitable. A hacker conference may not be the most practical example, but it is one among an amazing diversity of malicious activities that are striking organizations with increasing frequency. Being proactive to raise awareness is quite possibly the most effective defense against these attacks.

This particular DEF CON contest gives you an opportunity to consider and address your organization’s preparedness to deal with one type of attack: “social engineering,” loosely defined as “the act of manipulating people into performing actions or divulging confidential information ...typically appl[ying] trickery or deception for the purpose of information gathering, fraud, or computer system access.” This type of attack can come in many forms, such as phishing emails (like those emails that appear to be from a legitimate sender but contain malware or a link to a malicious website), spoofing calls (in which caller ID readouts are “tricked” into presenting the ID of legitimate callers, like your own IT department) or just plain old deception that can be conducted by phone, email, text or instant messages; via online chats or social networking; and even in person. Helping your employees to understand the methods and sources of these attempts to gain access to personal or corporate information and systems will help you better-secure your organization, addressing the “human error factor” that your technology controls are incapable of entirely blocking

Elizabeth Johnson’s practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

p.s.
Poyner Spruill^{LLP}

ATTORNEYS AT LAW

p.s.

POYNER SPRUILL publishes this newsletter to provide general information about significant legal developments. Because the facts in each situation may vary, the legal precedents noted herein may not be applicable to individual circumstances. © Poyner Spruill LLP 2010 All Rights Reserved

BREACH NOTIFICATION

from the Health Care Group of Poyner Spruill LLP

How Do These Requirements Apply to Your Organization and What Should You Do to Comply?



by Elizabeth Johnson

This document was prepared at the request of the Association for Home & Hospice Care of NC for its members by the law firm Poyner Spruill LLP.

As you may know by now, the stimulus bill passed last year to bolster the flagging U.S. economy included a number of changes relevant to the privacy and security of health information. These provisions (and others intended to increase use of electronic health records) are collectively known as the HITECH Act (the Health Information Technology for Economic and Clinical Health Act).

So why did Congress see fit to burden providers with the additional cost of implementing new privacy and information security controls at a time when it was trying to stimulate the economy? The bulk of the HITECH Act is intended to stimulate the economy by offering moneys to incentivize increased use of electronic health records that would, in turn, drive down health care costs. Congress, however, also saw fit to raise the stakes on privacy and information security requirements relevant to health information so that it would be protected in the course of transitioning to greater reliance on electronic records.

One of many ways Congress pursued this agenda was to mandate that HIPAA covered entities must notify affected individuals when their protected health information (hereinafter "PHI") is impacted by a "security breach." This requirement was, no doubt, inspired by similar requirements already established in 45 states, the District of Columbia and Puerto Rico that require notice to affected individuals residing in their jurisdictions when "personal information" has been affected by a security breach. The theory behind these laws is that consumers, upon realizing that their information has been breached, will be put on notice that they should be more vigilant in protecting themselves against identity theft or other fraud than would be the case had they not received these notifications.

The Problem: Disparate Breach Notification Requirements

Unfortunately for organizations that handle so-called "personal information," state laws vary in important ways, such as the types of information to which they apply, whether notice will be required to gov-

ernment regulators or consumer reporting agencies in addition to affected individuals, whether the law applies to hard copy information in addition to electronic information, and so on. As a further misfortune, these state laws also apply based on the residency of the affected individual, meaning that multiple laws may apply in a single security event. In English: if you experience a breach that affects information about residents of both North and South Carolina, you need to look to the requirements of both states to determine your obligations. Where the obligations are inconsistent, you will need to apply North Carolina's requirements to notification in North Carolina and South Carolina's requirements to notifications in South Carolina. The location of your business is arguably irrelevant to determining which law applies – the relevant factor is where the persons whose information was affected reside. Now imagine if you had a breach affecting residents of all the 45 states that have enacted these laws...it happens.

But back to the HITECH Act. Congress, presumably having decided that matters were not confusing enough with 45 different state laws on the topic, directed the Department of Health and Human Services (hereinafter, "the Department" or "HHS") to issue regulations that would require HIPAA covered entities to notify affected individuals of any breaches of unsecured PHI. The Department substantially complied, issuing "Breach Notification for Unsecured Protected Health Information" as an interim final rule (hereinafter, "the HHS/HITECH Breach Notice Rule") in August 2009. [As of the date of this article, no final rule has been issued.]



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

RALEIGH

CHARLOTTE

ROCKY MOUNT

SOUTHERN PINES

WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601 / P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Now, as you might have guessed, the HHS/HITECH Breach Notice Rule varies in some material ways from the assorted state breach notice laws. The HITECH Act did not seek to wholly preempt state laws, which makes some sense given that it generally does not apply to the same type of information (PHI) as do state laws (which tend to apply exclusively to types of information that would be used for identity theft, such as Social Security numbers and financial account numbers). As a result, it is now possible to experience a notifiable security breach that implicates any number of state laws (again, depending on the residency of the affected individuals), as well as the federal HHS/HITECH Breach Notice Rule (if PHI was affected).

So, in anticipation of the justifiable and entirely understandable confusion these requirements are certain to generate among health care providers nationwide, we offer the following tips and scenarios to help you walk through the relevant requirements. We will focus on the HHS/HITECH Breach Notice Rule, the North Carolina breach notice law and the South Carolina breach notice law. A chart at the end of this article summarizes some of the high points of these laws, contrasting their scope, requirements and penalties.

Some Answers: Responses to Important Questions about Breach Notification

HOW DO I KNOW WHICH LAW APPLIES TO ME?

To answer this question, you will need to know who was affected by the breach and where they live, as well as the type of information affected. If PHI was affected, the HHS/HITECH Breach Notice Rule will apply. If the PHI included names and SSNs, state laws also may apply. To know which state laws apply, you will need to know whose information was impacted. If the persons impacted all reside in North Carolina, then the North Carolina law applies. If the persons impacted reside in multiple states, then the laws of each of those states may apply.

Let's work through an example:

A burglar breaks into a hospice and steals a number of items, including some computers. Patient files, including patient names, prescriptions and diagnoses were saved on the computers' hard drives, which were not encrypted. The patients affected currently reside in the hospice, which is located in North Carolina, while others reside in a sister location in South Carolina.

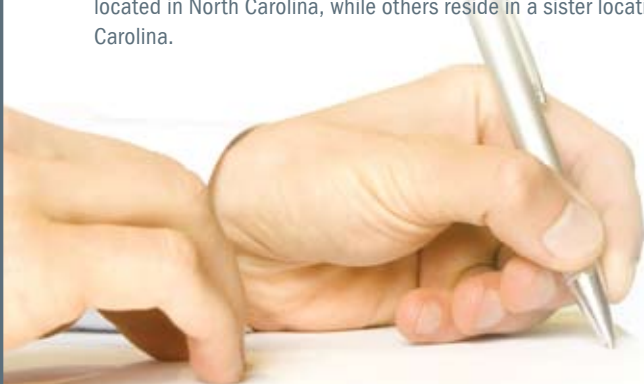
Because the information is not encrypted and is now in the possession of a bad actor, it is most likely you will conclude that this incident constitutes a breach (see response below for a discussion of how to determine whether a breach has occurred). Since PHI is included, the HHS/HITECH Breach Notice Rule applies. Since residents of both North and South Carolina were affected, those laws could apply but in this case do not, since the types of information affected are not covered by these laws. (Refer to the chart below for more detail on the types of information addressed by each law.) If the information also had included the patients' digital signatures, North Carolina law would apply while South Carolina would not (understanding this outcome may be unlikely for a hospice or home health care agency). If the information also had included financial account numbers, both North and South Carolina's laws would apply.

WHAT TYPES OF SCENARIOS CONSTITUTE A BREACH?

The answer to this question will depend on which law you have to apply. If the HHS/HITECH Breach Notice Rule applies, you will have to answer the following questions in order to know if you have had a breach:

- Did the disclosure violate the HIPAA Privacy Rule? If yes, it might be a breach. If no, it was not a breach.
- Does the breach pose a "significant risk of financial, reputational, or other harm to the individual"? To answer this question, HHS requires a formal, documented risk assessment. (Refer to the chart below for more detail.) If yes, it might be a breach. If no, it was not a breach.
- Did the information impacted include any of the data elements listed in the Privacy Rule at 45 C.F.R. § 164.514(e)(2), date of birth, or zip code? If yes, there might have been a breach. If no, there has not been a breach.
- Is the person who accessed, acquired or used the PHI someone acting under your authority (such as an employee or business associate), who acted in good faith and within the scope of their authority? If yes, there has not been a breach, provided there was no further disclosure that would violate the Privacy Rule.
- Do you have a good faith belief that the unauthorized person who received the disclosure will not be able to retain the information? This is most likely relevant in the case of verbal disclosures. If yes, there has not been a breach.

(Refer to the chart on the following pages for some additional considerations.) The North and South Carolina laws also stipulate that a breach has occurred only in certain circumstances, such as when "illegal use of the personal information has occurred or is reasonably likely to occur" or the incident "creates a material risk of



harm to a consumer.” (These factors are known as “harm thresholds” and not all state laws have one.) As a result, the question of whether a certain scenario constitutes a reportable breach is a highly fact-specific inquiry in which you must weigh the likelihood of harm in light of the circumstances.

There are, however, some rules of thumb to keep in mind:

- If the information has fallen into the hands of a bad actor it would be difficult to form a good faith belief that harm to the individual is not reasonably likely. As a result, loss of information due to hacking, theft of electronic devices storing information, theft of automobiles in which hard copy or electronic data were left, etc. are all more likely to result in a reportable breach.
- Information that is lost (misplaced records), sent in error (misdirected email or fax), or likely inaccessible because special equipment is required to retrieve the contents (backup tapes) poses a more difficult scenario. In these cases, you will have to consider the likelihood and severity of potential harm keeping in mind the factors HHS directs covered entities to consider in performing the required risk assessment.
- If you recover the information, you may still need to provide notice under HHS’s interpretation of its rule (“For example, if a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that it was not opened, altered, transferred, or otherwise compromised, such a breach may not pose a significant risk of harm to the individuals whose information was on the laptop.” [Emphasis added.] This assessment by HHS indicates that extensive analysis would be necessary in order to assure yourself that the information was not impacted, and even in that case, the agency leaves the door open to the possibility that notice may be necessary.)
- Remember that the HHS/HITECH Breach Notice Rule specifically references reputational harm, not only financial harm (such as identity theft). HHS notes, for example, that the fact an individual received care at a hospital may not pose a reputational harm, whereas information identifying that the individual received

specific services, such as oncology services or substance abuse treatment, is more likely to cause reputational harm.

- If the information impacted includes Social Security numbers, driver’s license numbers, or other data elements that could be used to open new lines of credit, it is common to offer affected individuals one year of credit monitoring service, at your expense, to help them protect against identity theft.
- If the information affected was encrypted, the incident may not constitute a breach under the HHS/HITECH Breach Notice Rule (see chart for more detail) and will not constitute a breach under either the North or South Carolina laws (note that some states require specific encryption, such as 128- or 256-bit, although North and South Carolina do not).

WHAT HAPPENS IF THE INFORMATION AFFECTED INCLUDES INFORMATION ABOUT DECEASED PERSONS?

State laws generally do not address what actions should be taken when the information affected relates to deceased individuals. North Carolina’s law, for example, provides that notice should be made to “the affected person.” Arguably, next of kin are “affected” when personal information about a deceased loved one is lost or stolen, but the notification requirements contemplate that the “affected person” to whom notice is due is the person whose information was lost or stolen, not their next of kin. Whether to provide notice to next of kin in compliance with state law thus becomes a question of interpreting the language of the statute and balancing legal risk with business and moral considerations.

The HHS/HITECH Breach Notice Rule does require that next of kin (or a personal representative) be notified in the event of a breach affecting a deceased individual’s PHI. See the chart below for details.

WHAT SHOULD I DO TO PREPARE FOR BREACH NOTIFICATION?

The HHS/HITECH Breach Notice Rule includes some burdensome administrative requirements that should be promptly addressed to ensure compliance. These include:

- Training all members of your workforce regarding breach notification;
- Updating your process for receiving complaints regarding privacy practices so that the complaint process also will address complaints regarding breach notification procedures;
- Providing that employees’ failure to comply with breach notification requirements and supporting policies and procedures will be sanctioned; and

p.s.

Poyner Spruill^{LLP}

ATTORNEYS AT LAW

Implementing written policies and procedures sufficient to address compliance with breach notification requirements. These procedures should include requirements to appropriately document incident response. The HHS/HITECH Breach Notice Rule places the burden of proof on covered entities which must demonstrate, in writing, that each potential breach had one of the following outcomes: the incident was appropriately analyzed (including documentation of the requisite risk assessment) and determined not to require notice; or notice was required and the covered entity properly and timely provided notice in the manner and form mandated by the rule.

It is also crucially important to ensure that your organization and your business associates are complying with the HIPAA Security Rule. (Although the Security Rule formerly applied directly to covered entities, it now applies in substantial part directly to business associates – a further change brought about by the HITECH Act.) There are two important reasons to ensure compliance with this rule:

1. Ensuring Security Rule compliance will help to avoid a breach of electronic PHI. With appropriate security measures in place there is a lower likelihood of experiencing a breach.
2. If you experience a breach, whether involving PHI or other personal information, government regulators may inquire as to your security practices. This has been the case for a number of entities experiencing security breaches of all types, including CVS Caremark (the subject of a joint FTC-HHS enforcement action) and Health Net of Connecticut (currently under investigation by the Connecticut Attorney General in the first known enforcement of HIPAA by a state attorney general since the HITECH Act granted them such authority). If a regulator seeks to review your security program, it should be, at minimum, compliant with applicable regulations, such as the HIPAA Security Rule. If it is not, past enforcement actions demonstrate that extensive fines (\$2.25 million in CVS's case) and equitable remedies (security audits every other year for 10-20 years) may result following a charge of HIPAA violations and under state law alleged unfair trade practices.

As a final preparatory step, you might also consider adding your outside counsel to your speed dial. Just a suggestion... ■

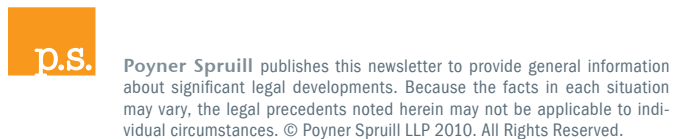


About Elizabeth Johnson

Elizabeth Johnson's practice focuses on privacy, information security and records management including identifying, assessing and remediating risks associated with these areas of law. She regularly assists in conducting privacy and information security assessments, developing and implementing privacy compliance and records management programs, and drafting privacy notices, contracts, policies and procedures. Elizabeth often serves in the role of counselor to clients regarding compliance with various statutory and regulatory requirements at the state, federal and international level.

Recently, Elizabeth was listed among the top privacy professionals in Computerworld's "2008 Best Privacy Advisers" report. Named by Business North Carolina as one its "Legal Elite - Under 40 Young Guns" for 2009, she is also involved with the Carolina Privacy Officials Network and the International Association of Privacy Professionals. Elizabeth was also named a Law & Politics Magazine "North Carolina Super Lawyers - Rising Star" in 2009 and was a Triangle Business Journal "40 Under 40" award winner in 2007.

An active member of the community, Elizabeth serves on the board of directors for the Triangle Area Chapter of the American Red Cross. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.



The Conundrum: A Comparison of the HHS/HITECH Breach Notice Rule, North Carolina's Identity Theft Protection Act, and South Carolina's Financial Identity Fraud and Identity Theft Protection Act

by Elizabeth Johnson
Poyner Spruill LLP


HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
What Is a Breach?		
<p>“Breach means the acquisition, access, use, or disclosure of [PHI] in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of the protected health information.” “Compromises the security or privacy of the protected health information” means that there is a “significant risk of financial, reputational, or other harm to the individual.” To assess the risk, if any, posed by the security incident, a covered entity must perform a risk assessment. HHS has indicated that covered entities should consider “a number or combination of factors,” some of which it identifies in the preamble to its rule, including those included in OMB Memorandum M-07-16.</p> <p>An incident will not be considered a “breach” if:</p> <ol style="list-style-type: none"> 1. The PHI impacted does not include the identifiers listed at 45 C.F.R. § 164.514(e)(2), date of birth, or zip code; 2. It was limited to unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure that would violate the Privacy Rule; 3. It was limited to an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate (or organized health care arrangement in which the covered entity participates), and the information received as a result of such disclosure is not further used or disclosed in a manner that would violate the Privacy Rule. 4. The covered entity or business associate has a good faith belief that the recipient of the disclosure would not reasonably have been able to retain the PHI. 	<p>“Security breach’ – An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.”</p>	<p>The SC law provides a definition of “breach of the security of the system,” but also discusses what constitutes a breach in a separate section. The two provisions are somewhat inconsistent; both are given below.</p> <p>“Breach of the security of the system” means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. Good faith acquisition of personal identifying information by an employee or agent of the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.</p> <p>A breach has occurred when personal identifying information “was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident.”</p>

HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
Type of Information and Persons Covered by the Rule/Law		
<p>The Breach Notice Rule applies to disclosures of “protected health information” or “PHI,” regardless of the residency of affected individuals.</p> <p>PHI is any health information that:</p> <ol style="list-style-type: none"> 1. Either identifies or could reasonably be used to identify an individual; and 2. Is created or received by a HIPAA covered entity or employer and which relates to: <ul style="list-style-type: none"> · Any past, present or future physical or mental health condition · Provision of health care to the individual · Any past, present or future payment for the provision of health care to the individual. 	<p>“Any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form.”</p> <p>“Personal information” as defined by the NC law (for breach notice purposes) includes a person’s first name or first initial and last name plus any of the following:</p> <ol style="list-style-type: none"> 1. Social security or employer taxpayer identification numbers; 2. Drivers license, state identification card, or passport numbers; 3. Checking account numbers; 4. Savings account numbers; 5. Credit card numbers; 6. Debit card numbers; 7. Personal Identification (PIN) Code as defined in N.C. Gen. Stat. § 14-113.8(6); 8. Digital signatures; 9. Any other numbers or information (expressly including email address, parent’s legal surname prior to marriage and password) that can be used to access a person’s financial resources; 10. Biometric data; and 11. Fingerprints. <p>“Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed ... and does not include information made lawfully available to the general public from federal, state, or local government records.”</p>	<p>“‘Personal identifying information’ means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted:</p> <ol style="list-style-type: none"> 1. Social Security number; 2. Driver’s license number or state identification card number issued instead of a driver’s license; 3. Financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident’s financial account; or 4. Other numbers or information which may be used to access a person’s financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual. <p>The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.”</p>



HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
Applies to Hard Copy?		
Yes	Yes	No (applies to “computerized data” only).
Timing of Notification		
<p>Covered entities must notify affected individuals without unreasonable delay and in no case later than 60 calendar days from the date of discovering the breach. “Discovery” occurs on the first day the covered entity knew of the breach or should have known of the breach when exercising reasonable diligence. Knowledge is imputed to any person (other than the person committing the breach), who is a workforce member or agent of the covered entity. Business associates would presumably be considered “agents” for purposes of this rule, so the 60-day clock begins to run as soon as any person working for the covered entity, including via a business associate, becomes or should have become aware of a breach.</p>	<p>“[N]otification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement ... and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.”</p>	<p>“[Notice] must be made in the most expedient time possible and without unreasonable delay, consistent with the [permitted law enforcement delay], or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” Notice to the regulator must be made without “unreasonable delay.”</p>
Notice to Individuals		
<p>Notice may be given by first-class mail at the affected individual’s last known address or, if the individual agrees to receive electronic notice, by email. The notice must be written in “plain language” and include, “to the extent possible”:</p> <ol style="list-style-type: none"> 1. A brief description of the incident, including the date it occurred and the date of discovery, if known; 2. A description of the types of unsecured PHI affected; 3. Any steps individuals should take to protect themselves from potential harm resulting from the breach; 4. A brief description of actions the covered entity is taking “to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches;” and 5. Contact information so that individuals can ask questions or request additional information, which must include a toll-free telephone number, an email address, a website, or a postal address. 6. If the covered entity knows the affected individual is deceased and has an address for next of kin or a personal representative, notice must be provided to one of those parties by first-class mail. 	<p>Notice may be given by written letter, telephone, or email if the affected individuals have agreed to receive communications electronically (and if the communication is consistent with the E-Sign Act). Notice must be “clear and conspicuous” and include:</p> <ol style="list-style-type: none"> 1. A general description of the incident; 2. The type of personal information affected; 3. A general description of actions the notifying entity has taken to protect the personal information from further unauthorized access; 4. A telephone number for the notifying entity that the person may call for further information; 5. Advice to review account statements and monitoring free credit reports; 6. The toll free numbers and addresses for the major consumer reporting agencies. 7. The toll free numbers, addresses, and websites for the FTC and the NC Attorney General’s Office, along with a statement that these sources provide information about preventing identity theft. 	<p>Notice may be given by written letter, telephone, or electronically (if the communication is consistent with the E-Sign Act).</p> <p>The law does not specify what information must be included in the notice.</p>

HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
Substitute Notice		
<p>Permissible if there is insufficient or out-of-date contact information precludes written notification to the individual. In all cases, substitute notice must be “reasonably calculated” to reach the individual.</p> <p>Where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by “an alternative form of written notice, telephone, or other means.”</p> <p>Where there is insufficient or out-of-date contact information for 10 or more individuals, then substitute notice must include a toll-free phone number that remains active for at least 90 days where individuals can inquire whether their PHI was affected by the breach. In this case, substitute notice must consist of:</p> <ol style="list-style-type: none"> 1. Conspicuous posting for a period of 90 days on the covered entity’s web-site home page; or 2. Conspicuous notice in major print or broadcast media in geographic areas where affected individuals likely reside. 3. In the case of deceased individuals where contact information of the next of kin or personal representative is insufficient or out-of-date, substitute notice is not required. 	<p>Permissible if:</p> <ol style="list-style-type: none"> 1. The cost of providing notice can be demonstrated to exceed \$250,000; 2. More than 500,000 persons must be notified; 3. The entity providing notice has insufficient contact information for those to whom notice is due, for only those affected persons without sufficient contact information); or 4. If the business is unable to identify particular affected persons, for only those unidentifiable affected persons. <p>Substitute notice must consist of:</p> <ol style="list-style-type: none"> 1. Email notice when the entity giving notice has an email address for the affected persons; 2. Conspicuous posting of the notice on the entity’s web site; or 3. Notification to major statewide media. 	<p>Permissible if:</p> <ol style="list-style-type: none"> 1. The cost of providing notice can be demonstrated to exceed \$250,000; 2. More than 500,000 persons must be notified; or 3. The entity providing notice has insufficient contact information for those to whom notice is due. <p>Substitute notice must consist of:</p> <ol style="list-style-type: none"> 1. Email notice when the entity giving notice has an email address for the affected persons; 2. Conspicuous posting of the notice on the entity’s web site; or 3. Notification to major statewide media.
Notice to Regulators		
<p>Must notify the Secretary of the Department of Health and Human Services.</p> <p>For breaches affecting more than 500 individuals, the Secretary must be notified contemporaneously with the notice provided to individuals. For breaches affecting less than 500 individuals, the covered entity must maintain a log or “other documentation” of these breaches, which log must be submitted to the Secretary not later than 60 days after the end of each calendar year to report breaches occurring during the preceding calendar year. In both cases, notice to the Secretary should be provided via the Department’s website, following instructions available there (www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html).</p>	<p>Must notify the Consumer Protection Division of the Attorney General’s Office if the notifying entity is providing notice to any person pursuant to the NC law. Notice to the Attorney General’s Office must describe the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.</p> <p>The Attorney General’s Office has produced a form to be used for reporting breaches to the Consumer Protection Division.</p>	<p>Must notify the Consumer Protection Division of the Department of Consumer Affairs if the notifying entity is providing notice to more than 1,000 persons at one time pursuant to the SC law. Notice to the Department must describe the timing, distribution, and content of the notice to individuals.</p>

HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
Notice to Media		
Required for breaches affecting more than 500 residents of a State or jurisdiction; in this case, notice must be made to “prominent media outlets” serving the state or jurisdiction (“State” includes American Samoa and the Northern Mariana Islands). Content of the notice must be the same as that provided to affected individuals and made within 60 days of discovery of the breach.	Not required (but see substitute notice option).	Not required (but see substitute notice option).
Notice to CRAs		
Not required.	Notice is required to “nationwide consumer reporting agencies” including the timing, distribution and content of the notice to individuals if the notifying entity provides notice to more than 1,000 persons at one time pursuant to the NC law.	Notice is required to “nationwide consumer reporting agencies” including the timing, distribution and content of the notice to individuals if the notifying entity will provide notice to more than 1,000 persons at one time pursuant to the SC law.
Requirements for BAAs or Service Providers		
<p>Business associates must notify covered entities of breaches without unreasonable delay and in no case more than 60 calendar days from discovering the breach. “Discovery” occurs on the first day the business associate knew or should have known of the breach by exercising reasonable diligence. Knowledge is imputed to all employees (except those that might have committed the breach) and agents of the business associate, so the 60-day clock starts to run when anyone working for the business associate becomes (or should have become) aware of the breach.</p> <p>The notice provided by business associates must “to the extent possible,” identify each affected individual and “any other available information” that would be required to be included in the notice to individuals (listed above).</p>	<p>“Any business that maintains or possesses records or data containing personal information of residents of North Carolina that the business does not own or license, or any business that conducts business in North Carolina that maintains or possesses records or data containing personal information that the business does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement”</p>	<p>“A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.”</p> <div data-bbox="1478 1230 1976 1468" style="text-align: right;">  <p>p.s. Poyner Spruill ^{LLP} ATTORNEYS AT LAW</p> </div>

HHS/HITECH BREACH NOTICE RULE	NORTH CAROLINA LAW	SOUTH CAROLINA LAW
Relevance of Encryption		
<p>A security incident is not, by definition, a “breach” unless it affects “unsecured” PHI. Whether PHI is “unsecured” is determined by reference to guidance issued annually by the Department. Presently, that guidance provides that PHI is not “unsecured” if it is encrypted as specified by the HIPAA Security Rule. Furthermore, the Department has affirmatively stated that encryption technologies that meet specific NIST (National Institute of Standards and Technology) standards have been judged to meet the Security Rule’s requirements.</p>	<p>An incident is not, by definition, a “breach” if the information affected was encrypted. Encryption is defined as “[t]he use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without use of a confidential process or key.”</p>	<p>An incident is not, by definition, a “breach” if the information affected was “rendered unusable through encryption.” Encryption is not defined.</p>
Relevance of Redaction/Purging		
<p>A security incident is not, by definition, a “breach” unless it affects “unsecured” PHI. Whether PHI is “unsecured” is determined by reference to guidance issued annually by the Department. Presently, that guidance provides that PHI is not “unsecured” if it is “shredded or destroyed such that PHI cannot be read or otherwise reconstructed. Redaction is specifically excluded as a means of data destruction.” Electronic media are deemed “cleared, purged or destroyed” if measures consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization were applied.</p>	<p>A security incident is not, by definition, a “breach” if personal information was redacted.</p>	<p>An incident is not, by definition, a “breach” if the information impacted was “rendered unusable through ... redaction.” Since the law applies only to “computerized data” it is not clear how redaction (a method of blocking out hard copy information) could be used to avoid notice obligations.</p>
Penalties		
<p>Civil violations of HIPAA generally are enforced by the Department’s Office for Civil Rights. Violations of any HIPAA rule, including the Breach Notice Rule, are punishable by fines of \$100-\$50,000 per violation, the amount to depend on the offender’s culpability. In all cases, a maximum cap of \$1.5 million is applied for violations of an identical provision in a calendar year.</p> <p>Criminal violations of HIPAA generally are enforced by the Department of Justice. State attorneys general have recently gained the ability to enforce HIPAA violations on behalf of residents of their state. In this case, civil penalties range from \$100-\$25,000 with a maximum cap of \$1.5 million for violations of an identical provision in a calendar year. Private causes of action are not permitted to enforce HIPAA violations.</p>	<p>“A violation of this section is a violation of [NC’s unfair and deceptive trade practices statute]. No private right of action may be brought by an individual for a violation of this section unless such individual is injured as a result of the violation.”</p> <p>The NC Attorney General may pursue civil penalties of up to \$5,000 for each violation of NC’s unfair and deceptive trade practices statute.</p>	<p>South Carolina residents injured by violations of the breach notification law may:</p> <ol style="list-style-type: none"> 1. Institute a civil action to recover damages in case of a willful and knowing violation; 2. Institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section; 3. Seek an injunction; and 4. Recover attorney’s fees and court costs <p>Knowing and willful violations are subject to administrative fines of \$1,000 per resident “whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.”</p>

IMPORTANT CHANGES TO HIPAA Proposed by HHS

A Summary of Proposed Changes to HIPAA Privacy, Security and Enforcement Rules



by Elizabeth Johnson

The following summarizes the major changes to and new provisions of the HIPAA Privacy, Security, and Enforcement Rules proposed by the Department of Health and Human Services (HHS) in its notice of proposed rulemaking published July 14, 2010 (75 Fed. Reg. 40867). Many of these changes are proposed to implement the HITECH Act, but several of the changes go beyond the provisions of the statute. Other topics covered in this rulemaking were not raised by the HITECH Act and are instead proposed to address issues HHS has identified based on its experience interpreting and administering the rules. Some subjects covered by the HITECH Act, such as breach notification and accounting for disclosures from electronic health records, were not covered in this rulemaking and so are not discussed below. The public comment period on this proposed rulemaking ends September 13, 2010. **Unless otherwise noted below, the compliance deadline for these proposed requirements will be 180 days from the date of publication of the final rule.**

While there are many reasons for the regulated community to be concerned about these and other recent changes to HIPAA regulations, some of the more compelling reasons include:

- Covered entities must notify affected individuals, such as patients and customers, in the event of a security breach affecting unsecured protected health information; notification also must be made to the primary regulator (HHS), which has authority to enforce against any legal violation that may have occurred.
- Recent revisions to the Enforcement Rule changed the maximum annual penalty per identical violation from \$25,000 to \$1.5 million, a 60-fold increase.
- The interim final Breach Notice Rule has been effective for almost one year, during which time more than 140 covered entities have reported to HHS breaches of unsecured PHI affecting more than 4.8 million individuals (and those figures account only for individual breaches that affected more than 500 people each, meaning their occurrence is immediately noted on HHS's website).

- In addition to making HHS compliance audits mandatory, the HITECH Act authorized state attorneys general to enforce HIPAA; the first such action settled with an agreement by the covered entity to implement a corrective action plan and pay \$250,000 in damages.
- Two recent enforcement actions by HHS involving the insecure disposal of health information netted a combined \$3.25 million payday for HHS; the agency has reportedly said it will apply those moneys to fund additional enforcement actions and audits.
- Business associates now must comply fully with the Security Rule, which imposes substantial administrative, physical, technical, and organizational security requirements.
- If the proposed changes are finalized as written, business associates will be directly liable for HIPAA violations.
- If the proposed changes are finalized as written, covered entities will no longer be able to escape liability for business associates simply by virtue of having put appropriate contracts in place and not having known of any pattern or practice of violations by the business associate.

The attorneys of Poyner Spruill's Privacy and Information Security practice regularly assist clients with HIPAA implementation, and counsel organizations of all shapes and sizes on their HIPAA obligations, compliance posture, and risk. We provide this summary to assist your organization in commenting on these rules or implementing anticipated changes.



Poyner Spruill^{LLP}

ATTORNEYS AT LAW

New Privacy Rights of Individuals

Access to Electronic Protected Health Information

The current Privacy Rule generally provides individuals with the right to access and request copies of their protected health information (PHI). The proposed rules specify that, where the individual requests an electronic copy of PHI, the covered entity must comply with that request if the electronic PHI (ePHI) is maintained in one or more designated record sets and is readily producible in the requested format. If the ePHI is not readily producible in the requested format, covered entities must provide the ePHI in a readable electronic form and format to be agreed upon with the individual. The covered entity may charge a reasonable fee for both the supplies and labor used to provide the ePHI, which fee may not be greater than the actual costs. The fee may reflect only labor costs (and not cost of supplies) if the individual either provides his own electronic media to store the ePHI or requests transmission of the ePHI by email.

If the individual requests that a copy of PHI (whether hard copy or electronic) be provided directly to another person, the covered entity must comply with that request if it is made in writing, signed by the individual, and clearly identifies the recipient and where to send the copy of PHI.

Requests to Restrict Disclosures of PHI Related to Services Paid Out of Pocket

One of the more controversial privacy provisions in the HITECH Act was the requirement that covered entities restrict disclosures of PHI upon an individual's request, provided that:

1. The disclosure is to a health plan for purposes of carrying out payment or health care operations;
2. The disclosure is not otherwise required by law; and
3. The PHI pertains solely to a health care item or service for which the individual has paid the provider in full out of pocket.

A covered entity would not have to honor the individual's request for a restriction if:

1. The disclosure was for treatment purposes;
2. The individual did not pay in full;
3. Some or all of the payment is not made out of pocket; or
4. The disclosure was not to a health plan.

While the proposed rules implement this HITECH Act requirement, HHS foresees some complications in implementation, stating "[d]ue to the myriad of treatment interactions between covered entities and individuals, we recognize that this provision may be more difficult to implement in some circumstances than in others, and we request comment on the types of interactions between individuals and covered entities that would make requesting or implementing a restriction more difficult." HHS has requested comment on factors not elaborated upon by the statute, such as the provider's obligation, if any, to notify downstream providers (such as specialists that may provide treatment of the same condition) of the individual's request, particularly in cases where a prescribing provider may use an electronic system to submit prescriptions to a pharmacy, which in turn may fill the prescription and notify the individual's health plan before the individual actually arrives at the pharmacy and has an opportunity to request restriction of the disclosure. HHS requests comment on whether a requested restriction should be carried forward to downstream providers and what technological capabilities exist that could facilitate efforts to honor individuals' requests for restrictions.

Under the proposed rules, the individual's right to request restrictions on disclosures of PHI in the above-described circumstances must be noted in the covered entity's notice of privacy practices.



New and Revised Restrictions on Uses and Disclosures of PHI

The Minimum Necessary Principle

The HITECH Act currently provides that a covered entity will be deemed to have complied with the minimum necessary principle if it limits uses and disclosures of PHI to a limited data set (to the extent practicable). This statutory requirement is currently effective but will sunset on the effective date of guidance HHS is required to issue on compliance with the minimum necessary principle (the statutory deadline to issue that guidance has already passed). In preparation for its release of that guidance, HHS has requested, through this rulemaking, comments on what aspects of the minimum necessary standard covered entities and business associates believe would be most helpful to have HHS address in guidance, and the types of questions these organizations may have about how to appropriately determine “minimum necessary” for purposes of complying with the Privacy Rule. No changes to the principle as currently stated in the Privacy Rule are proposed or anticipated in the future.

(As described below in the discussion of changes affecting business associates, the proposed rules would apply the minimum necessary principle directly to business associates.)

Use of PHI for Marketing

The new rules revise the definition of marketing to refine the types of communications excluded from the term. This adjustment is important because, generally speaking, covered entities are required to obtain a written authorization from individuals in order to use their PHI for marketing. While “marketing” is generally defined as “a communication about a product or service that encourages recipients of the communication to purchase or use the product or service,” the following types of communications are specifically excluded:

1. Communications for treatment of an individual by a health care provider, including case management or care coordination for the individual, or communications to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. (If the communication is made in writing and the health care provider receives remuneration in exchange for making the communication, other new restrictions will apply – see category below entitled “Use of PHI for Treatment Communications.”)
2. Communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity’s cost of making the communication.

3. Communications for the following health care operation activities, except where the covered entity receives financial remuneration in exchange for making the communication: (a) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including: (i) communications about participating providers in a health care provider network or health plan network, (ii) replacement of, or enhancements to, a health plan, and (iii) health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or (b) case management or care coordination, contacting individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

If the marketing involves direct or indirect financial remuneration, the authorization obtained from the individual must disclose that such remuneration is involved. “Financial remuneration” means “direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.”

Use of PHI for Treatment Communications

Use of PHI for treatment communications made by health care providers in exchange for financial remuneration will not qualify as “marketing” under the proposed rules and so would not necessitate a written authorization from individuals, provided the following two conditions are met:

1. The notice of privacy practices must disclose that such communications may be sent, that the health care provider will receive financial remuneration in exchange for such communications, and that the individual may opt out of receiving such communications at any time.
2. The treatment communication must disclose that the health care provider is receiving financial remuneration in exchange for providing the communication and must provide the individual with a “clear and conspicuous” opportunity to opt out of further treatment communications. The opt-out method cannot be unduly burdensome or cause the individual to incur more than a nominal cost.

HHS is encouraging use of toll-free phone numbers, email addresses, or other easy and cost-free methods for individuals to opt out of receiving these types of treatment communications. HHS has noted that requiring individuals to respond by postal mail could constitute an “undue burden.”



Sale of PHI

Like marketing activities, under the proposed rules the sale of PHI for any direct or indirect remuneration (financial or otherwise) generally would necessitate a prior written authorization from individuals, which authorization must recite that the covered entity will receive remuneration for the disclosure. Under the proposed rules, the following exceptions would apply such that PHI could be exchanged for direct or indirect remuneration in the following circumstances without a prior written authorization:

1. Disclosures of PHI for public health activities;
2. Disclosures of PHI for research purposes if the remuneration received is a reasonable cost-based fee to cover the actual cost of providing the PHI;
3. Disclosures of PHI for treatment or payment purposes;
4. Disclosures of PHI for the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence (described in the definition of health care operations);
5. Disclosures of PHI to the individual or to provide an accounting of disclosures to the individual;
6. Disclosures required by law;
7. Disclosures otherwise permitted by the Privacy Rule when performed in accordance with the relevant requirements and the remuneration received is a reasonable cost-based fee to cover the actual cost of providing the PHI, or the fee is otherwise expressly permitted by law (such as state laws that may specify a maximum charge that can be imposed for providing copies of medical records); and
8. Disclosures of PHI for payment purposes (disclosures made to obtain payment will not constitute "sales" of PHI).

Use of PHI for Fundraising

Covered entities are currently permitted to disclose PHI to business associates or institutionally-related foundations for fundraising purposes without individual authorization if the information disclosed is limited to demographic information and the dates on which health care was provided to the individual. The proposed rules require that the covered entity's notice of privacy practices disclose that the individual may be contacted for fundraising purposes and that the individual may opt out of being contacted at any time. In addition, every fundraising communication must include a "clear and conspicuous" option to opt out of further fundraising communications. The opt-out method cannot be unduly burdensome or cause the individual to incur more than a nominal cost. As noted above, HHS encourages use of toll-free phone numbers, email addresses, or other easy and cost-free methods for individuals to opt out of receiving fundraising communications and has noted that requiring individuals to opt out via postal mail could constitute an "undue burden." Importantly, treatment and payment may not be conditioned on the individual's choice with respect to receipt of fundraising communications.

Compound Research Authorizations

Generally speaking, authorizations required by the Privacy Rule cannot be combined, and the provision of treatment or payment, enrollment in a health plan, or eligibility for benefits may not be conditioned on receipt of an authorization unless the treatment is research-related. HHS now proposes limited exceptions for research authorizations whereby covered entities would be permitted to combine conditioned and unconditioned authorizations (forming "compound" authorizations) presented for research purposes, provided that the authorizations clearly denote which, if any, research components are conditioned upon receipt of authorization and clearly disclose the individuals' right to opt in to any unconditioned research activity.

In addition, HHS is seeking comment on whether and how the Privacy Rule could be amended to permit authorizations for future or secondary research uses of PHI. At present, authorizations may be valid only if the research is expressly described in the authorization, which can inhibit future or secondary research that may not have been fully formulated or anticipated at the time of the initial authorization. HHS has not proposed a specific modification to the Privacy Rule to accommodate the contemplated change, but rather is seeking comment on several options outlined in the proposed rules' preamble, such as whether a research authorization might be deemed adequate to cover future or secondary research when an individual could reasonably expect such future or secondary uses based on the information provided.



Disclosures of PHI Regarding Decedents

Historically, HIPAA did not distinguish between living individuals and decedents in restricting disclosures of PHI, with certain exceptions for disclosures to law enforcement, coroners, medical examiners, and funeral directors, and to organizations involved in organ or tissue procurement, transplant, banking, or donation. HHS has noted that the current regulations' restrictions on disclosures of PHI about decedents have hindered appropriate use of historical data and have hampered covered entities' ability to communicate with decedents' friends and relatives. To address these problems, HHS has proposed to loosen the restrictions as follows:

1. By providing that covered entities must abide by the requirements of the Privacy Rule with respect to a decedent's records only until the date that is 50 years from the date of the decedent's death;
2. By revising the definition of "individually identifiable health information" so that information regarding persons who have been deceased for more than 50 years will not constitute PHI (although HHS has only expressly discussed sunseting the Privacy Rule's restrictions 50 years from the date of death, implementing this revision to the definition of PHI would effectively place the same duration on the requirements imposed by the Security Rule and the Breach Notice Rule, which requirements tie back to the definition of PHI); and
3. By permitting disclosures of PHI to family members, or to other relatives or close personal friends who were involved in the decedent's care or payment for care prior to death, unless doing so is inconsistent with the previously expressed preference of the decedent.

Disclosure of Student Immunization Records

The proposed rules recognize that state law may now require schools to acquire student immunization records prior to enrollment. In states imposing such requirements, covered entities will be able to disclose student immunization records directly to schools without written authorization from parents or guardians. Covered entities would still have to obtain parents' or guardians' "agreement" to the disclosure, which agreement could be obtained verbally. HHS has requested comment on whether covered entities should be required to document receipt of such agreement by the parent or guardian.

New and Revised Provisions Related to Privacy Notices

Amendments to Notice of Privacy Practices

Several of the changes proposed by HHS will necessitate corresponding changes to notices of privacy practices, namely the following:

1. The notice must describe uses and disclosures requiring an authorization, which will include sales of PHI, uses or disclosures of PHI for marketing, and uses or disclosures of psychotherapy notes (see above categories entitled "Use of PHI for Marketing" and "Sale of PHI");
2. The notice must describe uses and disclosures of PHI for fundraising, but in addition the individual's right to opt out of such uses and disclosures must be described (see above category entitled "Use of PHI for Fundraising");
3. If the covered entity intends to send treatment communications in exchange for financial remuneration, the notice must disclose that fact and describe the individual's right to opt out of such communications (see above category entitled "Use of PHI for Treatment Communications"); and
4. The notice must describe the individual's right to request restrictions of disclosures to health plans for payment or health care operations regarding services for which the individual has paid in full out of pocket (see above category entitled "Requests to Restrict Disclosures of PHI When Paid Out of Pocket").

The first three categories listed above must be described in separate statements within the notice of privacy practices. Covered entities not engaging in any of the activities that are the subject of these revised notice requirements may not need to update their notice of privacy practices.

Redistribution of Notice of Privacy Practices

HHS has clearly stated that the above-described changes to notices of privacy practices will each constitute a material change to the notices, thereby triggering the Privacy Rule's requirement to redistribute the revised notices. For non-health-plan covered entities, this will usually entail posting the revised notice in prominent locations, making the revised notice available to individuals upon request, and providing the revised notice rather than the former notice at the time of initial contact with new patients or customers. HHS has stated that this obligation to redistribute notices is not overly burdensome for providers. HHS has stated, however, that the redistribution requirements imposed on health plans (which necessitate that the plan actively notify participants within 60 days of making any material change to the notice) may be overly burdensome and solicits comment on revising the redistribution requirements applicable to health plans. HHS has advanced a number of proposed options on which it specifically requests comment, such as replacing the 60-day requirement with a requirement for health plans to redistribute revised notices only in their next annual mailing to members such as at the beginning of the plan year or during the open enrollment period.



New and Revised Provisions Related to Business Associates

Additional Types of Entities Designated “Business Associate”

The proposed rules expand and clarify the definition of “business associate” to include:

1. Subcontractors of business associates that create, receive, maintain, or transmit PHI on behalf of the business associate;
2. Vendors of personal health records acting on behalf of a covered entity;
3. Organizations transmitting PHI on behalf of a covered entity, such as Health Information Organizations and E-Prescribing Gateways, assuming they require routine access to PHI (acting as a “conduit” with only random and infrequent access will not trigger the definition); and
4. Patient Safety Organizations (as defined by the Patient Safety and Quality Improvement Act of 2005).

Business Associate Privacy Requirements

Business associates are prohibited from using or disclosing PHI other than in accordance with the provisions of their business associate agreements, as required by law, or as needed for certain of their own business functions. Business associates also may not disclose PHI in a manner that would violate the Privacy Rule if done by the covered entity. (As such, the new proposed restrictions on certain uses and disclosures of PHI, described above, are relevant to business associates.) While these provisions were historically made part of business associate agreements (as required by the current Privacy Rule), the proposed rules now make the Privacy Rule’s requirements direct obligations (rather than contractual obligations) of the business associate. In addition, business associates now have a direct obligation to abide by the “minimum necessary” standard.

Under the proposed rules, business associates would be expressly required to disclose PHI in the following circumstances:

1. When required by HHS as part of an investigation to determine the business associate’s compliance; and
2. To the covered entity, the individual to whom the PHI pertains, or that individual’s designee in response to an individual’s request for an electronic copy of PHI (a new individual right described in the above category entitled “Access to Electronic Protected Health Information”).

(Note: Subcontractors meeting the new definition of business associate will also have to meet these same compliance obligations.)

Business Associate Security Requirements

The entire Security Rule now applies directly to business associates, including the provisions regarding evaluation of the reasonableness of addressable implementation specifications and other provisions related to implementation of the substantive security requirements. While this change is easy to articulate, actual implementation will be daunting for most business associates, which may not appreciate the detailed and comprehensive nature of the provisions set forth by the Security Rule. The Security Rule mandates, for example, several required elements including: periodic risk analyses; sanction policies; information system activity review (such as system logging and monitoring); procedures to authorize, supervise, modify, and terminate workforce access to ePHI; information access management procedures; training; incident response procedures; data backup plans; contingency plans; disaster recovery plans; periodic program evaluations; facility access controls; workstation security; portable media controls; emergency access procedures; unique user IDs; audit controls; integrity controls; and appropriate written agreements with contractors (see category below entitled “Amendments to Business Associate Agreements”).

Multiple other “addressable” controls also are listed, and will be deemed required unless the business associate engages in a mandatory process to evaluate the control and whether it is appropriate to the organization, in light of several factors specified by the Security Rule. As is presently the case for covered entities, that process and the outcome must be documented and compensating controls must be implemented in order for business associates to decline implementation of “addressable” safeguards.

(Note: Subcontractors meeting the new definition of business associate will also have to meet these same compliance obligations.)



Poyner Spruill^{LLP}
ATTORNEYS AT LAW

Business Associates Directly Liable for Violations

Prior to the HITECH Act, business associates were not directly liable under HIPAA but rather were liable to the extent provided by their business associate agreements or other contracts with covered entities. Under the proposed rules, business associates are directly required to abide by certain Privacy Rule restrictions and all Security Rule requirements, and they also are directly liable for violations of those provisions.

(Note: Subcontractors meeting the new definition of business associate will also face this direct liability.)

Covered Entity Liability for Business Associates

While the proposed rules render business associates directly liable for HIPAA violations, as described above, this proposal also would cause covered entities to lose the benefit of an exception that previously allowed them to avoid liability for the actions of business associates acting as agents if:

1. The relevant contract requirements had been met;
2. The covered entity did not know of a pattern or practice of the business associate that violated the contract; and
3. The covered entity did not fail to act with regard to those violations.

With this change, covered entities could be held liable for the acts or omissions of business associates who are agents, or even if the appropriate contractual measures were in place and the covered entity did not know of violations by the business associate. That possibility raises the stakes for covered entities and exacerbates the need to conduct appropriate diligence on business associates, a need that was already heightened by the increased penalty amounts and breach notification obligations, both imposed by earlier rulemakings.

Amendments to Business Associate Agreements

In addition to retaining much of the previously required contract language, HHS proposes to require amendment of business associate agreements to expressly provide:

1. To the extent the business associate will carry out a covered entity's obligation under the Privacy Rule, that the business associate will comply with the requirements of the Privacy Rule that would apply to the covered entity in its performance of the obligation;
2. That the business associate will comply with the applicable requirements of the Security Rule;
3. That the business associate will require subcontractors that create, receive, maintain, or transmit ePHI on behalf of the business associate to enter into a contract in which the subcontractors agree to comply with the applicable requirements of the Security Rule; and

4. That the business associate will report to the covered entity any security incident of which it becomes aware, including any breaches of unsecured PHI.

Any existing business associate agreement that complies with current HIPAA requirements and is not renewed or modified during the time that is 60 to 240 days after publication of the final rule will be presumed compliant until the earlier of:

1. The date the contract is renewed or modified on or after the date that is 240 days from publication of the final rule; or
2. The date that is one year and 240 days from the date of publication of the final rule.

New and Revised Provisions Related to Subcontractors

Subcontractors as Business Associates

Subcontractors that meet the new definition of "business associate" will now face the same compliance obligations and potential liability as do business associates (see section above regarding changes affecting business associates).

Implementation of Subcontractor Agreements by Business Associates

Business associates will now have an express obligation to implement contracts with their subcontractors (the current requirement is simply to ensure that the subcontractors "agree" to the same obligations imposed on the business associate, but a contract was not expressly required). That contract would essentially mirror the business associate agreement.

Business Associates Demanding Cure of Contractual Violations by Subcontractors

Under current requirements, covered entities must demand cure of contractual violations if they know of a pattern or practice of activity by a business associate that would constitute a material breach or violation of the business associate agreement. Following a cure period, if the breach or violation had not ended, the covered entity was required to terminate the agreement or report the violation to HHS when terminating the contract would be infeasible. While the proposed rules continue to require termination of the agreement in the absence of cure, they eliminate the duty to report to HHS. In addition, a parallel requirement has been imposed for business associates, who must similarly terminate their agreements with subcontractors in the event the business associate knows of a pattern or practice of activity by the subcontractor that would constitute a material breach or violation of the agreement, and the subcontractor has failed to cure the violation.

New and Revised Provisions Related to Enforcement

Previous revisions to the Enforcement Rule changed the annual maximum civil penalty for HIPAA noncompliance from \$25,000 per violation to \$1.5 million per violation, a 60-fold increase. Changes to the Enforcement Rule contained in this rulemaking clarify a number of key provisions, including the following:

- References to business associates are included throughout in order to effectuate business associates' direct liability for HIPAA violations (see above category entitled "Business Associates Directly Liable for Violations").
- In keeping with the HITECH Act's mandate that HHS must audit compliance, a revision is proposed to state that HHS "will" investigate complaints and conduct compliance reviews (the current wording provides that the agency "may" do so).
- Compliance reviews by HHS will be mandatory when a review of the facts indicates possible incidents of "willful neglect," even if no complaint has been received.
- HHS will no longer be required to resolve cases of willful neglect by informal means, but may do so if it chooses.
- HHS proposes giving itself the right to disclose PHI for law enforcement purposes in order to facilitate enforcement actions by (or in cooperation with) state attorneys general or other federal agencies such as the Federal Trade Commission.
- HHS proposes additional factors that it may consider in determining the amount of a civil penalty, key among them the addition of reputational harm as a factor (reputational harm also must be considered in determining whether a security breach is reportable under the current Breach Notice Rule).

The proposed rules also modify the definition of "reasonable cause" in order to more clearly delineate penalty tiers. "Reasonable cause" will mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." Accordingly, the penalty tiers will apply in the following degrees:

- Violations of which the alleged violator did not know and would not have known by exercising reasonable due diligence (\$100-\$50,000/violation, up to an annual maximum of \$1.5 million/violation);
- Violations due to "reasonable cause" as defined above, rather than willful neglect (\$1,000-\$50,000/violation, up to an annual maximum of \$1.5 million/violation); and
- Violations due to willful neglect (\$10,000-\$50,000/violation, up to an annual maximum of \$1.5 million/violation if the violation was corrected in a 30-day period running from the day the covered entity or business associate knew of the violation or would have known of it by exercising reasonable diligence; absent correction in that 30-day period the penalty is \$50,000/violation up to an annual maximum of \$1.5 million/violation).

About the Author

Elizabeth Johnson's practice focuses on privacy, information security, and records management. Her comprehensive, practical approach to privacy law is reflected by the diversity of her clients, which hail from a variety of industries including health care, financial services, insurance, retail, telecom, utility, technology, consumer goods, and client services. Elizabeth has also worked with organizations of various size and scope, ranging from Fortune 100 companies with international reach to local charities. She was listed among the top privacy professionals in Computerworld's "2008 Best Privacy Advisors" report. Elizabeth may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

Kim Licata, Of Counsel to the firm's Raleigh office, assisted with this article. She has advised health care providers and facilities on regulatory and compliance issues for over thirteen years. Her practice is designed to take the legal worry out of business ideas and assist her clients in actualizing their goals. Kim prides herself on being accessible and creative in her approach to complex situations. In addition to her regulatory work, Kim has years of litigation experience that make her a well-rounded advocate for her clients, understanding the true legal and litigation risks faced by health care entities and offering sound, practical legal advice. She may be reached at 919.783.2949 or klicata@poynerspruill.com.

