Fox Rothschild LLP
ATTORNEYS AT LAW

Staying Well Within the Law

A newsletter on the current legal issues facing today's health care industry

First Quarter 2011

Why the Time for Security and Privacy Insurance Has Arrived

By Elizabeth G. Litten and Mark G. McCreary

You may think that a $30 USB drive does not seem like the most costly business asset you could lose, but you would be wrong.

Protected personal information (PPI) and protected health information (PHI) lurk in almost every business. Employee information, including IRS W-4 forms, health questionnaires, payroll and financial information fill file cabinets and computer hard drives across the country. Businesses often keep such information about individuals even when they have not been employed by the company for decades. Customer information, such as personal and financial information, fill CRM databases, e-mail archives and smartphones in every state (and every country, in the case of traveling employees practically or physiologically unable to leave the smartphone at home).

Even user information for online access to accounts, features and services permeate a substantial portion of modern businesses, with troves of full names, home addresses, credit cards and mother's maiden names stored in redundant databases, including those floating in that magical place referred to as "The Cloud."

Conscientious risk managers have known for decades that locked filing cabinets, restricted off-premises access and only-as-necessary employee and vendor access to paper files are best practices. Most businesses are now familiar with the risks associated with electronic data storage of PPI and PHI and have implemented policies and systems to prevent unauthorized access and data breaches. Encrypted transmission of PPI and PHI has been the norm for most savvy businesses for years, and encrypted storage is slowly trickling down to even smaller businesses.

PHI is often the data that when set loose in the wild creates the most startling and damning headlines. It is a fact of life in 2011 that hospitals and other health care providers and payers (health insurance carriers and other types of health benefits plans) must maintain, record and transmit PHI electronically. Transmission of PHI electronically does not stop within the walls of the business or even across secure intranets for providers with multiple locations. Transmission involves the submission of claims to government or third-party payers, sharing information with other health care providers and communicating with patients and their families.

An example of how far reaching a "transmission" can be is found in the proposed regulations from the Department of Health and Human Services, Office for Civil Rights (OCR). Under the proposed regulations, "electronic" health information transmissions include even those transmissions on paper, by facsimile or on a voice mail message, if the information being exchanged existed in electronic form before the transmission took place.[1]

By way of analogy, if we apply the foregoing proposed regulation to banking information, if an account manager calls her client and leaves a voicemail regarding confirmation of a securities purchase for account no. 8164540774, she would need to be certain that access to the voicemail is limited to the authorized persons, nobody intercepted the call and at all times the transmission, access to and storage of the voicemail was encrypted. There is no doubt that best practices dictate that the account manager should have never left a voicemail with such detailed information, but the point is there is arguably no regulation preventing the account manager from leaving the voicemail message. Back to the medical context, even those providers that are slow to implement electronic health records (EHRs), and vendors of providers that do not view themselves as coming into contact with PHI, have legal obligations to recognize and secure it under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) laws and implementing regulations.

While a major concern already for hospitals and other health care providers as well as for payers and others whose business

In This Issue:

[1] 75 Fed. Reg. 40868, 40913 (July 14, 2010) (proposed amendment to 45 C.F.R. 160.103): "Electronic media means... (2) Transmission media used to exchange information already in electronic storage media... Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form before the transmission." (Emphasis added.)

involves health care, the creation, transmission and storage of PHI and PPI should also be a concern for other types of businesses. Treatises have been written, and millions, if not billions, of corporate dollars have been spent, on the subject of handling and storage of PPI. The time and dollars spent on the actual formulation of policies and the handling of PPI by businesses grows every year, as requirements become stricter and more widespread. However, experience has taught businesses that no amount of prevention, protection and security can guarantee data is secure. Disgruntled and rogue employees, corporate espionage and a bored 12-year-old in Bulgaria are constant threats to any business with PHI or PPI that has any value on the black market or is a target for embarrassment in the media. It is often not the wild scenario of Ethan Hunt stealing the NOC list in "Mission Impossible" that creates the greatest risk of PHI or PPI loss or theft.

Consider the following examples. A personal wealth manager's car is broken into, and his laptop containing the unencrypted usernames and passwords for online brokerage accounts is stolen. The CFO of a cutting-edge gene therapy company loses her keys, which includes a keychain thumb drive containing unencrypted genetic profiles of all 140,000 customers of the company. The CEO of a social media site has his laptop routinely confiscated by Homeland Security when returning from business trips abroad—his laptop contains unencrypted account information for every user of the social media site, including credit card information used to verify users' identities—and Homeland Security promptly loses the laptop. On one hand, none of the people in the foregoing examples did anything malicious. Yet, none of the information should have been accessible by a third party and, under any competent security policy, the unencrypted storage of that data would have been prohibited.

The events leading up to the loss of PHI or PPI are wholly irrelevant. It is the loss itself that creates the problem for the business that experienced the loss.

Currently, in addition to HIPAA and HITECH—the federal breach notification laws applicable specifically to PHI—46 states, the District of Columbia, Puerto Rico and the Virgin Islands all have breach notification laws applicable to PHI and/or PPI. The residency of each person contained in the PHI or PPI loss will determine which law(s) apply, meaning it is likely a business would be dealing with several states' laws. There are variations among state laws, such that in some states you must notify the consumer within a set amount of time, while other states require you to contact law enforcement prior to notifying the consumer. It is rare that a business will be able to merely issue a mea culpa, purchase credit-monitoring coverage for affected persons and be back to business as usual. Rather, businesses will find rapidly mounting legal bills, public relations strategy decisions and compromises, and class action and private lawsuits in multiple states. In some cases, the costs associated with preparing, implementing and following the requisite data storage and handling policies, including hardware and software costs that should have been in place prior to the data loss, can be crippling because of the suddenness and all-at-once necessity.

If a business provides or pays for health care, "unsecured" PHI lurks among or alongside its PPI. Under HIPAA, PHI includes any "individually identifiable health information," and unsecured PHI exists wherever there is documentation of patient information, whether related to past, present or future conditions, services or items, and includes handwritten and oral notes. Any information connected with an identifying fact about a patient (patient's name, address, telephone number, address, Social Security number or e-mail address, to name a few), or any information that could be linked with an identifying fact about a patient (an accident reported in the newspaper, for instance) may be or create unsecured PHI. If this information is accessed, or could be accessed, by unauthorized individuals or entities, the HITECH breach notification requirements and potential civil monetary penalty provisions will apply.

The late-adopting, low-tech providers and unaware vendors may be less aware of these legal obligations and the potential costs associated with a PHI breach, but they are no less likely to face a PHI breach. In fact, a number of very sophisticated nationally recognized hospitals and esteemed educational institutions have recently had to deal with lapses in their privacy and security policies and procedures that resulted in breaches of PHI. Several recent examples include the Yale School of Medicine, the University of Rochester, the Henry Ford Health System, and the University of Tennessee Medical Center.[2] Undoubtedly, these entities incurred significant costs in terms of the breach notification requirements alone.

On Feb. 14, 2011, the OCR settled with the General Hospital Corporation and Massachusetts General Physicians Organization, Inc. over a loss of PHI that includes a payment to the U.S. government of $1,000,000 by Massachusetts General Hospital for potential violations of HIPAA.[3] On Feb. 4, 2011, HHS imposed a $4.3 million civil monetary penalty assessment (CMP) on Cignet Health and its affiliates (Cignet) for violations of the HIPAA Privacy Rule, including failure to provide patients access to their records and failure to cooperate with an investigation.[4] This is the first time the OCR has publicized its activities in enforcement actions involving heavy monetary payments. Until now, the publicized enforcement activity for monetary recoveries from covered entities under HIPAA/HITECH has been by attorneys general in Connecticut, Indiana and Vermont.

Unlike the handling of PPI, the loss of PHI is covered by the federal HIPAA and HITECH laws and regulations, which contain (relatively) clear direction and response parameters in the event of a breach. However, the preemption provisions of HIPAA contemplate that more restrictive state laws not "contrary" to HIPAA can complement the HIPAA requirements. Therefore, organizations facing a PHI breach or loss must still conduct an analysis to determine if the data breach law of a particular state

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
[3] http://www.hhs.gov/news/press/2011pres/02/20110222a.html
[4] http://www.hhs.gov/news/press/2011pres/02/20110222a.html (See also HHS Imposes $4.3 Million Penalty for HIPAA Violations, Bloomberg Law Reports - Privacy & Information, (March 2, 2011)).

includes medical information in its definition of PPI (and many do).

Under the HIPAA and HITECH laws and regulations, entities must provide written notification by first-class mail to all affected individuals or, where the individual has agreed to electronic notice, by e-mail, and must provide a description of what happened. The description is to include the date of the breach and date of the breach discovery, if known; a description of the types of unsecured PHI involved in the breach; information regarding steps the entity is taking to investigate the breach, to mitigate harm to the individuals and to prevent further breaches; as well as contact procedures for individuals to ask questions and get additional information. These contact procedures must include a toll-free telephone number, an e-mail address, a web site or postal address.

With respect to PPI data breaches, the Identity Theft Resource Center identified 498 breaches in 2009, exposing more than 222,000,000 records, as compared to 656 in 2008, exposing more than 35,000,000 records, and representing a 47 percent increase from 2007. Additionally, the average cost of a data breach in 2009 was $204 per affected consumer, as compared to $202 per affected consumer in 2008, and representing a 40 percent increase from 2005. While these numbers only include reported breaches, which likely makes the numbers very misleading about the scope of breaches, and the cost per affected consumer is an average, it does not take a great deal of imagination to multiply the costs by 5,000, 10,000 or 50,000 affected consumers.

In its Aug. 24, 2009, rule proposal, OCR estimated the cost implications associated with various PHI breach notification and contact requirements. It estimated the cost of setting up a toll-free telephone line for a breach affecting the PHI of between 10 and 500 individuals by assuming that a breach of this magnitude would generate 1,772 calls, whereas a breach affecting 500 or more individuals would generate 2,887,032 calls. It then calculated the set up, calling charge and labor costs per call and estimated a breach affecting 10 to 500 individuals would cost $5,067, whereas the cost associated with the toll-free line for breaches affecting more than 500 individuals would be $8,228,041. Clearly, even if one finds fault with OCR's estimates and assumptions, the financial implications of a PHI breach are significant – even before considering potential costs associated with such things as civil monetary penalties, indemnification and damaged reputation.

Knowing that most business have PPI and/or PHI, that policies and safeguards must be in place, that no amount of policies and safeguards will guarantee a breach- or loss-free existence and that the costs associated with a data breach or loss can be astronomical, the question of what can a business do to offset the potentially catastrophic effects of a data breach or loss becomes paramount.

Those persons most cognizant of the potential for breaches and their effects have observed the relatively recent proliferation of "cyber insurance" policies, also sometimes referred to as "Security and Privacy" (S&P) liability coverage. S&P policies have been developed to cover some or all of the out-of-pocket expenses incurred in connection with data breaches and losses and may make a lot of sense in light of our increasingly data-driven, electronically communicating world.

S&P insurance policies may cover a wide variety of expenses related to PPI and PHI breaches. The coverage may include protection for the entity not only in terms of the PPI and PHI breach notification costs, but may also cover some or all of the costs associated with the investigation needed to determine the cause of the breach, costs to restore or recollect the breached information, costs associated with public relations and crisis management related to the incident, legal costs, compensatory damages, criminal reward funds and costs associated with mitigating harm to affected individuals.

One S&P insurance carrier (Chartis) provided the following examples of amounts actually paid in connection with PHI and related privacy breaches:

- Employee of a credit union sold information to outsiders. Total amount paid on the S&P policy for liability claim and first party loss: $1,800,000
- Employee stole information and sold it to an identity theft ring. Total amount paid on the S&P policy for notice and liability claims: $2,600,000
- Employee of a medical provider stole and sold more than 40,000 patient records containing PHI. Total amount paid on claims pursuant to the S&P policy covering notification costs: $675,000
- Entity/insured lost tapes containing medical information and Social Security numbers. Total amount paid on the S&P policy covering call center services and credit monitoring of affected individuals: $400,000+

Another carrier (NAS E-MD™; NAS MEDEFENSE™ Plus) provided several real-life examples of S&P loss scenarios particular to health care entities and PHI. This carrier offers "privacy breach response coverage" that includes legal fees, information technology forensic costs, postage costs, advertising costs, public relations expenses, credit monitoring expenses, identity theft education and assistance expenses and call center expenses. Examples of claims paid include:

- Hospital fined by the state for failing to report a PHI breach of 532 patients' medical records within five days after the breach occurred. The state determined an unauthorized employee removed a computer containing PHI; as soon as the hospital determined the computer was unrecoverable, it reported the incident. Actual amount paid by the S&P carrier: $250,000+
- Hospital sued by Patient A after Patient B (a pregnant drug addict) stole Patient A's medical identity and delivered a baby testing positive for illegal drugs. Social workers subsequently attempted to remove Patient A's four children from her, thinking she was a drug addict, and Patient A incurred legal costs to keep her children. Actual amount paid by the S&P carrier: $1,200,000 (damages) and $80,000 (defense costs)
- Pharmacy sold a computer to a private individual; the computer contained prescription records including names, addresses, Social Security numbers and medication lists of pharmacy customers. Total amount paid by the S&P carrier: $410,000+

"An ounce of prevention" may, indeed, be worth "a pound of cure" in the PPI and PHI privacy and security context. Written data storage and handling policies and systems to prevent unauthorized access and data breaches and losses (which must be effective and dutifully implemented and should be frequently tested) are an absolute necessity for a business of any size and for anyone who "touches" PPI and PHI. In the context of hospitals and other health care organizations, it is easy to make the argument that S&P insurance policies also are an absolute necessity. Nevertheless, businesses and providers of all sizes should analyze the realities of increasing cyber crime and the rapidly expanding use of and access to various modes of electronic communication in measuring the relative economic costs and benefits of the added protection of an S&P insurance policy.

For more information on this topic, please contact Elizabeth G. Litten at 609.895.3320 or elitten@foxrothschild.com or Mark G. McCreary at 215.299.2010 or mmccreary@foxrothschild.com.

This article first appeared in *Bloomberg Privacy & Information Law Report* and is reprinted here with permission.

Disruptive Behavior Jeopardizes Staff Privileges and Hospital Accreditation

By William H. Maruca

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) has declared a zero-tolerance policy on threatening, intimidating or otherwise disruptive behavior. Accordingly, hospitals will need to get tough on offenders or risk losing their JCAHO accreditation. Physicians can expect closer review of conduct that may have been tolerated in the past. That said, hospitals that inconsistently apply the tougher policies for questionable purposes or economic reasons are likely to be subject to litigation.

A JCAHO leadership standard, which became effective January 1, 2009, requires hospitals and other accredited organizations to adopt and implement a code of conduct that defines and manages disruptive or inappropriate behavior by physicians and administrators. Leadership Standard LD.03.01.01 was announced in Sentinel Event Alert 40 issued on July 9, 2008, titled "Behaviors That Undermine a Culture of Safety," posted at http://www.jointcommission.org/assets/1/18/SEA_40.PDF.

Targeted behavior patterns include overt actions such as verbal outbursts and physical threats as well as passive activities such as refusing to perform assigned tasks or quietly exhibiting uncooperative attitudes during routine activities, reluctance or refusal to answer questions, return phone calls or pages, condescending language or voice intonation and impatience with questions. Policies adopted by hospitals have been defined broadly to encompass acts that may also constitute gross negligence or malpractice, HIPAA violations, workplace discrimination, fraud and even assault. For instance, some examples of disruptive behavior cited in policies include:

- Abusive behavior to patients, families, colleagues or visitors, including rudeness, discourtesy or negative comments about physicians or nurses with the intent to discredit; belittling, berating and/or threatening another individual; non-constructive criticism, addressed to its recipient in such a way as to intimidate, degrade, demean, undermine confidence, belittle or imply stupidity or incompetence; shaming or inappropriately blaming others for negative outcomes.
- Physical or verbal harassment, threats or assault on a physician, nurse, employee or other member of the hospital organization; threats of physical violence; assault/battery; throwing of instruments or equipment; inappropriate touching or gestures.
- Falsification of medical or other hospital records.
- Unauthorized possession, use, copying or reading of hospital records or disclosure of information contained in such records to unauthorized persons.
- Disregard of established safety, housekeeping or sanitary control conditions.
- Use of profanity, vulgarity, violent, intemperate, intimidating or threatening language or behavior.
- Harassment, i.e., unwelcome conduct, whether verbal, non-verbal, physical or visual, that is based on a person's status, such as sex, color, race, ancestry, national origin, age, disability, job status or other recognized group status, and including retaliation against persons who report disruptive behavior or sexual harassment, or conduct that interferes unreasonably with an individual's work performance or creates an intimidating hostile or offensive work environment.
- Inappropriate and impertinent medical record entries, including "cute" abbreviations or illustrations, or other notations insulting patients or families, impugning the quality of care being provided by the hospital or any other individual or attacking particular physicians, nurses or hospital policies. ("GOMER" is a good example – Google it if you're not familiar with it).
- Imposing idiosyncratic requirements on the nursing staff that have nothing to do with better patient care but serve only to burden the nurses with "special" techniques and procedures.
- Unauthorized handling, possession or use of any drugs or alcoholic beverages on hospital premises or working under the influence of controlled substances or intoxicants.

Disruptive physician behavior has been the subject of medical staff investigations and sanctions for decades and has resulted in considerable litigation over the years. The Physicians Health Programs of the Pennsylvania Medical Society, which was established to address substance abuse, also evaluates physicians with behavior issues.

Physicians are not the only ones whose outbursts are under heightened scrutiny. JCAHO has noted, "While most formal

research centers on intimidating and disruptive behaviors among physicians and nurses, there is evidence that these behaviors occur among other health care professionals, such as pharmacists, therapists and support staff, as well as among administrators."

Of particular concern is the widely reported perception of a double standard that allows high-volume physicians (and powerful administrators) more leeway to engage in egregious conduct. Such perceived favoritism may also result in allegations of inappropriate inducements to profitable physicians and harsher treatment of their less-profitable colleagues.

It may be tempting for hospitals to go easier on a busy, profitable physician, but that is a mistake. Failure to adequately monitor a high-volume practitioner who allegedly performed medically unnecessary procedures was the basis for a criminal prosecution that resulted in a three-year prison term and seven-figure fine in the United Memorial Hospital case in Greenville, Michigan, involving pain management physician Dr. Jeffrey Askanazi. Although it was his quality, not his behavior, that caught the Justice Department's attention, there was clear evidence the administration was willing to overlook problems with its most profitable physician, and that evidence contributed to the prosecution's victory.

The JCAHO standards require each accredited organization to adopt a code of conduct that defines acceptable and disruptive and inappropriate behaviors and requires its leaders to create and implement a process for managing disruptive and inappropriate behaviors. Further, the Sentinel Event Alert recommends health care organizations take 11 specific steps:

1. Educate all team members – both physicians and non-physician staff – on appropriate professional behavior defined by the organization's code of conduct.
2. Hold all team members accountable for modeling desirable behaviors and enforce the code consistently and equitably among all staff.
3. Develop and implement policies and procedures/processes appropriate for the organization that address:
   - "Zero tolerance" for intimidating and/or disruptive behaviors, especially the most egregious instances of disruptive behavior such as assault and other criminal acts. Incorporate the zero tolerance policy into medical staff bylaws and employment agreements as well as administrative policies.
   - Medical staff policies regarding intimidating and/or disruptive behaviors of physicians within a health care organization should be complementary and supportive of the policies present in the organization for non-physician staff.
   - Reducing fear of intimidation or retribution and protecting those who report or cooperate in the investigation of intimidating, disruptive and other unprofessional behavior.
   - Responding to patients and/or their families who are involved in or witness intimidating and/or disruptive behaviors.
   - How and when to begin disciplinary actions (such as suspension, termination, loss of clinical privileges, reports to professional licensure bodies).
4. Develop an inter-professional organizational process for addressing intimidating and disruptive behaviors
5. Provide training and coaching for all leaders and managers in relationship-building and collaborative practice.
6. Develop and implement a system for assessing staff perceptions of the seriousness and extent of instances of unprofessional behaviors and the risk of harm to patients.
7. Develop and implement a reporting/surveillance system (possibly anonymous) for detecting unprofessional behavior.
8. Support surveillance with tiered, non-confrontational interventional strategies. These interventions should initially be non-adversarial in nature, with the focus on building trust, placing accountability on and rehabilitating the offending individual and protecting patient safety.
9. Conduct all interventions within the context of an organizational commitment to the health and well-being of all staff, with adequate resources to support individuals whose behavior is caused or influenced by physical or mental health pathologies.
10. Encourage inter-professional dialogues across a variety of forums as a proactive way of addressing ongoing conflicts, overcoming them and moving forward through improved collaboration and communication.
11. Document all attempts to address intimidating and disruptive behaviors.

These recommendations recognize the inherent subjectivity of behavior problems and, by utilizing a measured, respectful approach, establish some limited "due process" to protect the wrongly accused as well as the accuser. Many physicians accused of disruptive behavior suspect ulterior motives or double standards, and following these recommendations would help make the process more fair and transparent.

The Joint Commission notes that hostile and dysfunctional environments are readily recognized by patients and their families as well as hospital staff and failure to address and manage behavior problems exposes facilities to litigation from both patients and employees. Now that the new standards are in effect, plaintiffs' malpractice attorneys can be expected to use them to their advantage when there is evidence of tolerance of abusive, hostile or unprofessional conduct by physicians or non-physicians.

If the standards are applied unevenly to favor or reward high-volume physicians, there may be serious consequences: Qui tam whistle-blowers may allege illegal inducements, co-workers subjected to disruptive behavior may sue hospitals, and patients may allege incompetent or dangerous practitioners were permitted to remain on staff where their conduct resulted in poor care or injury.

For more information about this topic, please contact William H. Maruca at 412.394.5575 or wmaruca@foxrothschild.com.

This article first appeared in *The BULLETIN* of the Allegheny County Medical Society and is reprinted here with permission.

New CMS Guidance on the Performance of Histories and Physicals at ASCs

By Victoria Heller Johnson

CMS issued guidance to state surveyors on Dec. 17, 2010, clarifying the requirements contained in the Ambulatory Surgical Center (ASC) Interpretive Guidelines for medical histories and physical examinations (H&Ps).

This guidance was issued in response to confusion among state surveyors who did not know whether the requirement that H&Ps be performed not more than 30 days before a scheduled surgery allowed the H&Ps to be performed on the same day of the surgery.

The guidance clarifies three major issues in connection with Medicare surveys of ASCs:

1. **The comprehensive H&P can be performed on the same day as the surgical procedure.**

   Pursuant to the Medicare conditions for coverage for ASCs at 42 CFR 416.52, each patient must have a comprehensive medical H&P assessment by a physician or other qualified practitioner within 30 days before the date of the patient's scheduled surgery. The new CMS guidance clarifies there is no prohibition against performing the H&P on the same day as the surgery, including performing the H&P in the ASC, as long as the H&P is comprehensive and the results are placed in the patient's medical record before the procedure. It is **not** acceptable, according to the CMS guidance, to conduct the H&P after the patient has been prepped for surgery and brought into the operating or procedure room.

2. **If the H&P is performed on the date of the surgery in the ASC, the H&P assessment may be combined with some, but not all, of the elements of the required pre-surgical assessment.**

   The Medicare conditions for coverage for ASCs also require patients to undergo a pre-surgical assessment that documents, at a minimum, any changes in the patient's condition since the completion of the H&P. The CMS guidance makes it clear that if the H&P was conducted before the date of the surgery, then the pre-surgical assessment will require a separate examination in the ASC on the date of the surgery. However, if the H&P is conducted on the same day as the surgery, some of the elements of the pre-surgical assessment may be incorporated into the H&P. This does **not** apply to the anesthetic/procedure risk assessment required to be performed pursuant to 42 CFR 416.42, which must be performed separately immediately prior to the surgery and after the H&P. The H&P must still be placed into the patient's medical record prior to the procedure.

3. **A comprehensive H&P is required regardless of the type of surgical procedure.**

   CMS makes clear there is no exemption for ASCs that perform less invasive procedures from the requirement to perform a comprehensive H&P. CMS cautions those ASCs that believe the comprehensive H&P requirement is too burdensome given the types of procedures they perform to consider voluntarily terminating their Medicare certification as an ASC and instead perform those procedures as physician office-based surgical services.

The guidelines contained in the memorandum are effective immediately.

For more information about this topic, please contact Victoria Heller Johnson at 610.458.4980 or vjohnson@foxrothschild.com.

Health Care Reform Challenges - In Congress and the Courts

By William H. Maruca

The newly Republican-controlled House of Representatives voted 245-189 on Jan. 19, 2011, to repeal the controversial 2010 health care reform law, the Patient Protection and Affordable Care Act (PPACA). Two federal courts have also held the law unconstitutional. While no one expects this vote to spell the end of what its opponents call "Obamacare," the PPACA will remain a political football this year and next, and the judiciary, not the legislative branch, is more likely to have the final word.

Many provisions of the law are highly popular with voters: coverage of children under their parents' plans to age 26; elimination of pre-existing condition coverage restrictions and lifetime caps; phase-out of the "doughnut hole" in Medicare drug coverage; and elimination of co-pays for certain preventative care, for starters. Other provisions are highly unpopular, particularly the "individual mandate" requiring the uninsured to buy coverage; the financial penalties that kick in after 2013 on certain employers that do not provide basic coverage to their full-time employees; and the expansion of Form 1099 tax reporting requirements, a provision nobody likes but was included as a way to help fund the bill's costs. Some critics claim the law simply does too little to rein in runaway health care costs.

Here is a look at the various challenges to the law, their possible outcomes and their potential impact on health care in the United States.

Legislative Challenges

The House's repeal vote was more of a symbolic broadside than a realistic effort to derail the PPACA. With only three Democratic House members voting for repeal, the Democratic party continuing to

control the Senate and no chance for a veto-proof 2/3 vote in both houses, the measure will primarily serve as means to reopen debate on the best way to address the health care system's ills.

On Feb. 2, 2011, the Senate voted against the House's repeal bill.

The GOP does not have the votes for a comprehensive repeal, but it does control the appropriation process in the House, and it is likely funding for components of the PPACA will be targeted by the law's opponents during the budget debate. This approach could spell gridlock. One proposal floated would require every bill that comes before the House appropriations committee to exclude any funding for implementing or enforcing the PPACA.

More likely is an effort to reform the reforms, under the banner of "repeal and replace." One such effort to address a major omission in the PPACA, dubbed the Help Efficient, Accessible, Low-Cost, Timely Healthcare (HEALTH) Act of 2011, was introduced on Jan. 7, 2011, and has received the support of the American Medical Association and many specialty societies. This bi-partisan tort reform bill, introduced by House members Phil Gingrey, M.D. (R-GA), David Scott (D-GA) and Lamar Smith (R-TX), is patterned after existing efforts in California and Texas. Dr. Gingrey, who had been a practicing ob-gyn before entering politics, had sponsored this effort previously in 2007 and again in 2009, to no avail. If enacted, the bill would cap non-economic damages such as pain and suffering at $250,000, limit punitive damages and establish a national three-year statute of limitations for malpractice claims.

The constitutionality of the individual mandate will also be challenged in Congress while it works its way through the courts. Beginning in 2014, most U.S. citizens and legal residents will be required to purchase health insurance or pay a penalty. Commentators on both sides of the debate have acknowledged it is unprecedented for the federal government to require citizens to purchase a product from private vendors. The insurance industry contends requiring younger, healthier people to participate in the insurance pool is the only way it can afford to meet PPACA's insurance reform obligations such as covering individuals with pre-existing conditions and meeting medical loss ratio requirements. If the individual mandate is repealed or invalidated, look for alternatives to support the insurance pool such as tax credits, surcharges on individuals who delay buying coverage and limiting enrollment windows to specific times.

As noted above, one change both sides of the aisle would support is scaling back the PPACA's requirement that businesses report all payments of $600 or more in a year for goods or services to single providers on IRS Form 1099, a huge administrative burden. The requirement was expected to identify, capture and tax payments to independent contractors that had been slipping past the IRS and was predicted to raise $19 billion over the next 10 years. The Senate approved a measure to repeal the reporting requirement by a wide bipartisan margin of 81-17 on Feb. 2, which now awaits action in the House.

Also in the House's crosshairs:

- Reducing PPACA's tax on health insurers set to take effect beginning in 2014.
- Allowing purchase of health insurance across state lines, which could create more competition among carriers but would limit the roles of the state insurance commissioners and state-level insurance requirements.
- Scaling back the expansion of Medicaid coverage, which is reportedly threatening many state budgets. Earlier this year, the Arizona state legislature passed a bill requesting a federal waiver from these rules.
- Eliminating the independent Medicare payment advisory board.
- Repealing the Community Living Assistance Services and Support (CLASS) Act, the PPACA's little-noticed, federally administered, consumer-financed long-term insurance plan that critics say is expected to run deep deficits.
- Modifying or repealing the Sustainable Growth Rate (SGR) formula, i.e., the "doc fix," which was most recently given another temporary patch to prevent a 25 percent Medicare physician fee cut from occurring on Jan. 1.

Court Challenges

As of this writing, the judicial score is 3-2 in favor of the constitutionality of the PPACA, setting up appeals that are certain to reach the U.S. Supreme Court.

On Jan. 31, 2011, Judge Roger Vinson of the U.S. District Court for the Northern District of Florida ruled the individual mandate exceeded Congress' authority and invalidated the entire statute by determining the mandate was not severable from the PPACA The suit, *Florida v. HHS*, was joined by 20 state attorneys general and has been the most closely watched battle over the reform legislation.

Judge Vinson held the individual mandate impermissibly regulated "inactivity" and rejected the administration's argument that the law regulated the "activity" of individuals choosing to finance inevitable health care purchases out-of-pocket instead of through insurance. His opinion stated, "[T]he defendants' argument that people without health insurance are actively engaged in interstate commerce based on the purported 'unique' feature of the much broader health care market is neither factually convincing nor legally supportable."

The opinion rejected the states' attack on the PPACA's expansion of the Medicaid program. The states had contended the Act imposed unaffordable, coercive burdens on state budgets but states had no choice but to continue to participate in Medicaid. Judge Vinson concluded the states could not, as a matter of law, argue participation in Medicaid was involuntary or the federal government had the power to coerce the states into remaining in the program.

Finally, in what may prove the most controversial element of the decision, Judge Vinson held the individual mandate is not severable from the remainder of the law. He cited the defendants' own description of the mandate as an "essential" part of the Act at least 14 times in their motion to dismiss. Unlike most complex legislation, the PPACA did not include a "severability" clause that preserves all remaining portions of the law if part of it is deemed invalid. In its absence, Judge Vinson stated, "The Act, like a defectively designed watch, needs to be redesigned and reconstructed by the watchmaker," i.e., Congress, not the courts.

On March 3, Judge Vinson issued a ruling staying his decision striking down the law and permitting states to continue with implementation efforts, conditioned on the administration filing its notice of appeal within seven days and its seeking expedited review on appeal in the Eleventh Circuit. This could pave the way for a quicker route to the Supreme Court.

The case that dominated the headlines in December was *Virginia v. Sebelius*, in which Judge Henry Hudson of the U.S. District Court for the Eastern District of Virginia ruled the individual mandate exceeded Congress' authority under the Constitution's Commerce Clause, the Necessary and Proper Clause and the General Welfare Tax Clause. He noted, "Neither the Supreme Court nor any federal circuit court of appeals has extended Commerce Clause powers to compel an individual to involuntarily enter the stream of commerce by purchasing a commodity in the private market." He also agreed with the Commonwealth of Virginia's characterization of the Act's economic sanction for failing to purchase insurance as a "penalty," rather than a tax. The judge denied Virginia's request for an injunction and noted:

> This case, however, turns on atypical and uncharted applications of constitutional law interwoven with subtle political undercurrents. The outcome of this case has significant public policy implications. And the final word will undoubtedly reside with a higher court.

Judge Hudson's decision is under appeal to the U.S. Court of Appeals for the Fourth Circuit.

Other federal courts in Virginia, Michigan and the District of Columbia have found the PPACA is constitutional. So far, all the decisions have followed the party lines of the presidents who appointed the judges. The other Virginia case was decided by Judge Norman Moon, who wrote:

> The "fundamental need for health care and the necessity of paying for such services received" creates the market in health care services, of which nearly everyone is a participant. … Far from "inactivity," by choosing to forgo insurance, Plaintiffs are making an economic decision to try to pay for health care services later, out of pocket, rather than now, through the purchase of insurance.

In the most recent of these cases, *Mead v. Holder*, Judge Gladys Kessler of the U.S. District Court for the District of Columbia ruled in favor of the law by holding the decision to forgo insurance is economic "activity," but rejected the administration's alternative defense of the penalty for failure to purchase insurance as a permissible tax. This argument is unlikely to prevail if the "activity" premise is ultimately rejected by the Supreme Court.

Thirteen separate lawsuits are pending that challenge the constitutionality of portions of the PPACA. The AMA has established a blog to track the progress of these cases, which can be found at http://acalitigationblog.blogspot.com/.

Commenters agree the buck will ultimately stop at the U.S. Supreme Court. If the individual mandate is ruled unconstitutional, can the rest of the law survive? The law is unsettled whether the balance of the statute would remain intact, but notably, Judge Hudson's opinion did not mention the severability issue at all.

One thing is clear: The signing of the PPACA last March, while a "big deal" (to paraphrase Vice President Biden), was only the beginning of the story. There remains a fundamental disagreement among lawmakers and judges about the nature of the crisis, whether there is a crisis at all and whether the PPACA is a valid and constitutional response.

For more information about this topic, please contact William H. Maruca at 412.394.5575 or wmaruca@foxrothschild.com.

This article first appeared in *The BULLETIN* of the Allegheny County Medical Society and is reprinted here with permission.

About the Health Law Practice

Fox Rothschild's Health Law Group comprises more than 40 attorneys who counsel clients locally, regionally and nationally. Our multioffice, multidisciplinary approach allows us to offer practical, cost-effective solutions to issues faced by longstanding stakeholders, as well as a variety of industry newcomers.

For more information about any of the articles in **Staying Well Within the Law**, please contact any member of the Fox Rothschild Health Law Practice. Visit us on the web at **www.foxrothschild.com**.

Practice Co-Chair
David S. Sokolow
215.299.2712 or 609.895.3308
dsokolow@foxrothschild.com

Practice Co-Chair
Todd A. Rodriguez
610.458.4978
trodriguez@foxrothschild.com

Newsletter Editor
William H. Maruca
412.394.5575
wmaruca@foxrothschild.com