Health Law Section Newsletter

Vol. 24, No. 1 – July 2015

Bayou Shores: Bankruptcy's Fresh Start vs. Governmental 'Police' Powers

by David N. Crapo

Providing the debtor with a 'fresh start' is a fundamental policy underlying Chapter 11 of the United States Bankruptcy Code. The Bankruptcy Code and its fresh start policy do not exist in a legal vacuum, however. They do not supplant, and, indeed, must often give effect to, non-bankruptcy laws—laws determining the existence and nature of property interests being a prime example. Nevertheless, it is not always clear whether bankruptcy or non-bankruptcy law governs the resolution of a given controversy. For example, since the enactment of the Bankruptcy Reform Act of 1978, numerous conflicts have arisen over the application of bankruptcy law to controversies in which tax, environmental or labor law also apply.

It should be no surprise, therefore, that conflicts have arisen over the application of bankruptcy law to controversies involving Medicare and Medicaid provider agreements. In no recent bankruptcy case has the conflict between bankruptcy and Medicare/Medicaid law been more intense than in *In re Bayou Shores SNF LLC*, which is currently pending before the United States Bankruptcy Court for the Middle District of Florida.[1] In *Bayou Shores*, the bankruptcy court: 1) enjoined the U.S. Department of Health and Human Services (HHS) from terminating Bayou Shores' Medicare provider agreement and 2) confirmed, over objections of HHS and the Florida Agency for Health Care Administration (AHCA), Bayou Shores' plan of reorganization, which provided for Bayou Shores to assume its Medicare and Medicaid provider agreements.

The bankruptcy court nevertheless also authorized AHCA to: 1) commence administrative proceedings to revoke Bayou Shores' existing skilled nursing facility (SNF) operating license or, alternatively, deny Bayou Shore's license renewal application. The bankruptcy court's rulings on those issues required it to address the three issues that will be discussed

continued on page 3

Inside this issue

Health Law Section Leadership

in this article: 1) when a Medicare provider agreement terminates; 2) whether, as an exercise of its 'police power,' HHS was authorized to terminate Bayou Shore's Medicare provider agreement, which had been the subject of a pre-bankruptcy termination notice; and 3) whether, by allowing Bayou Shores to assume its Medicare and Medicaid provider agreements, the bankruptcy court properly exercised its bankruptcy jurisdiction or impermissibly usurped HHS's Medicare jurisdiction.

The bankruptcy court's rulings on and reasoning with respect to those three issues may seem counterintuitive to a health law specialist unfamiliar with bankruptcy, but would not seem so to a bankruptcy practitioner, particularly one unfamiliar with health law.

Before addressing those issues, a brief summary of the factual and procedural background of *Bayou Shores* is necessary.

Factual and Procedural Background

Bayou Shores owns and operates a 159-bed SNF in St. Petersburg, Florida. The Bayou Shores facility is one of the few SNFs in the Tampa Bay area capable of meeting the needs of patients with challenging psychiatric conditions. More than 90 percent of its revenue is derived from Medicare and Medicaid reimbursements. It is beyond dispute, therefore, that Medicare and Medicaid revenues are crucial to Bayou Shores' continued operations.

Between February and July 2014, the Centers for Medicare and Medicaid Services (CMS) cited Bayou Shores for patient safety deficiencies on three separate occasions. In each case, CMS found an immediate jeopardy to resident health or safety. Bayou Shores took prompt corrective action, including hiring an outside compliance consultant, and advised CMS of its remediation efforts. CMS did not revisit Bayou Shores' facility to evaluate those efforts. Instead, by letter dated July 22, 2014, the secretary of HHS advised Bayou Shores that its Medicare provider agreement would be terminated, effective Aug. 3, 2014.

Bayou Shores filed an administrative appeal from the termination notice and requested an expedited hearing. Because the appeal would not preclude HHS from withholding payment from Bayou Shores, on Aug. 1, 2014, Bayou Shores sought and obtained from the United States District Court for the Middle District of Florida a temporary restraining order (TRO) enjoining the termination of the provider agreement through Aug. 15, 2014. HHS moved to dissolve the TRO. The district court dissolved the TRO on Aug. 15, 2014, at 12:58 p.m. Less than an hour later, at 1:52 p.m., Bayou Shores filed its Chapter 11 bankruptcy petition with the bankruptcy court. A week later, on Aug. 21, 2014, Bayou Shores filed an emergency motion to enforce the automatic stay seeking a ruling that the automatic stay prohibited HHS from terminating its Medicare provider agreement. HHS opposed the stay motion, contending, *inter alia*, that it had the authority to terminate Bayou Shores' Medicare provider agreement notwithstanding the bankruptcy filing. The bankruptcy court overruled HHS, and on Sept. 5, 2014, entered a final order enjoining HHS from terminating Bayou Shores' Medicare provider agreement.

Bayou Shores fast-tracked its bankruptcy case, filing a plan of reorganization on Nov. 20, 2014, and its first amended plan of reorganization the next day. The plan provides, *inter alia*, for Bayou Shores to assume its Medicare and Medicaid provider agreements. HHS objected to Bayou Shores' assumption of its Medicare provider agreement and the confirmation of the plan, contending the plan was not feasible because Bayou Shores' Medicare provider agreement had been terminated prepetition and, for that reason, could not be assumed.

AHCA did not file either an objection to confirmation or a joinder in HHS's objection. Rather, at the hearing on the confirmation of the plan, AHCA advised the bankruptcy court that it concurred in HHS's position. AHCA did, however, file a motion for clarification of or relief from stay, seeking leave to either: 1) commence an administrative proceeding to revoke Bayou Shore's existing SNF operating license or 2) deny Bayou Shore's pending request for renewal.

The bankruptcy court confirmed the plan at the confirmation hearing on Dec. 31, 2014, and entered a final confirmation order on Jan. 7, 2015. On Jan. 20, 2015, the bankruptcy court granted the clarification motion.

When is a Medicare Provider Agreement Terminated?

Upon the initiation of a bankruptcy case, a bankruptcy estate arises.[2] The Bankruptcy Code defines the estate broadly to include all of the debtor's property and interests in property.[3] The bankruptcy estate includes a debtor's rights under its 'executory' contracts. The

Bankruptcy Code does not define the term 'executory.' However, courts have generally found Medicare and Medicaid provider agreements to be executory.[4] As a general rule, debtors that are able to promptly cure existing defaults and provide adequate assurance of future performance are free to assume their executory contracts.[5] Debtors may not, however, assume contracts that have expired before the bankruptcy filing; a bankruptcy filing will not resuscitate an expired contract.[6] Because Bayou Shores depends almost entirely on Medicare and Medicaid reimbursements for its revenue, the success of its reorganization depended on its provider agreements having been executory at the time of its bankruptcy filing and, therefore, able to be assumed.

HHS and AHCA have repeatedly argued that Bayou Shores' Medicare provider agreement (and, therefore, its Medicaid provider agreement) expired before the bankruptcy filing. In particular, HHS has argued that the Medicare provider agreement expired on Aug. 3, 2014, the expiration date specified in its July 22, 2014, notice to Bayou Shores or, at the very latest, an hour before Bayou Shores' bankruptcy filing when the district court dissolved the TRO. In point of fact, as noted above, Bayou Shores did not file its bankruptcy petition until 1:52 p.m. on Aug. 15, 2015, or about one hour *after* the TRO was dissolved. AHCA contends Bayou Shore's Medicaid provider agreement automatically terminated when its Medicare provider agreement terminated.

To have divested Bayou Shores (and its bankruptcy estate) of its rights under its Medicare provider agreement (and, therefore, its Medicaid provider agreement), however, the termination had to have been complete and not subject to reversal at the time of the bankruptcy filing.[7] Both at the hearing on the stay motion and in its memorandum opinion on confirmation, the bankruptcy court concluded that Bayou Shores had not been completely divested of its rights under its provider agreements at the time of the bankruptcy filing.[8]

The bankruptcy court reasoned that HHS's issuance of the termination notice did not result in a complete and irreversible termination of Bayou Shores' rights under its Medicare provider agreement.[9] Only the completion—prior to the bankruptcy filing—of the administrative appeals process Bayou Shores had initiated could have had that result.[10] Under the bankruptcy court's reasoning, therefore, the mere issuance of a termination notice does not, as a matter of law, terminate a Medicare provider agreement (or result in the automatic termination of a Medicaid provider agreement) for bankruptcy purposes, as long as the debtor timely initiates an administrative proceeding challenging the notice and the proceeding is still pending when the bankruptcy petition is filed.

HHS's and ACHA's Police Powers v. Bayou Shores Right to Assume Its Contracts

The bankruptcy court's finding that Bayou Shores' provider agreements had not been terminated before its bankruptcy filing did not resolve of the question of whether they could be terminated after the filing. Pursuant to Section 362(a) of the Bankruptcy Code, a bankruptcy filing triggers an automatic stay. The automatic stay prohibits, *inter alia*, actions to exercise control over property of the bankruptcy estate.[11] Among the actions prohibited are a non-debtor's termination of a contract with a debtor. However, the automatic stay includes a 'police power' exception that permits a governmental unit to take action to enforce its police and regulatory powers against a debtor, even if the action would otherwise violate the automatic stay.[12]

HHS contended in opposition to the stay motion that, notwithstanding the bankruptcy filing, it could terminate Bayou Shores' Medicare provider agreement (which would automatically terminate the Medicaid provider agreement as well) as a valid exercise of its police power. Both at the stay hearing and (in more detail) in the confirmation memorandum, the bankruptcy court rejected HHS's contention. In doing so, the bankruptcy court relied on established authority that distinguishes between actions taken by a governmental unit to enforce its police or regulatory authority, which enjoy the protection of the police power exception, and those taken to protect its 'pecuniary' interest, which do not. More specifically, the bankruptcy court drew a distinction between the termination of a Medicare provider agreement and actions taken to close an SNF facility on the basis of patient care or safety concerns.[13]

At the hearing on the stay motion, the bankruptcy court noted that HHS alleged pre-bankruptcy patient safety issues that might have warranted the immediate transfer of patients and the closure of the facility. Closure of the facility under those circumstances could have been a legitimate exercise of police power.[14] By seeking to terminate Bayou Shores' Medicare provider

agreement, however, HHS merely sought to protect its pecuniary interests.[15] Indeed, it appeared to the bankruptcy court that, as far as HHS was concerned, Bayou Shores could continue operating its facility; HHS simply was not going to reimburse Bayou Shores for doing so.[16] Consequently, because it would further only HHS's pecuniary interests, the termination of Bayou Shores' Medicare provider agreement would not constitute a valid exercise of HHS's police power and, therefore, was barred by the automatic stay.[17]

Assuming a Medicare Provider Agreement: A Bankruptcy or Medicare Issue?

As noted above, the administrative proceeding Bayou Shores commenced in response to the termination notice was not complete at the time of the bankruptcy filing. Apparently, it was not even complete at the time of the hearing on the confirmation of the plan. In other words, Bayou Shores had not exhausted its administrative remedies when it filed its bankruptcy petition and apparently had not done so when it filed its plan. Nevertheless, the plan provided for Bayou Shores to assume its Medicare and Medicaid provider agreements. By so providing, the plan triggered the question of the bankruptcy court's jurisdiction to authorize Bayou Shores' assumption of its provider agreements.

HHS has contended that by authorizing Bayou Shores to assume its Medicare provider agreement under the plan, the bankruptcy court effectively exercised jurisdiction over that agreement in violation of 42 U.S.C. § 405(h). Section 405(h) generally bars courts from exercising jurisdiction over Medicare controversies such as the termination of a provider agreement before a provider has exhausted all administrative remedies. As originally enacted, Section 405(h) expressly precluded the exercise of *bankruptcy* jurisdiction over Medicare controversies. As the bankruptcy court noted in the confirmation memorandum, however, when Congress amended Section 405(h) in 1984 it omitted any reference to the bankruptcy jurisdictional statute, 28 U.S.C. § 1334. Moreover, although Congress has enacted several amendments to the Bankruptcy Code since 1984, it has not amended Section 405(h) to exclude the exercise of bankruptcy jurisdiction over Medicare controversies. That being the case, the bankruptcy court concluded (in what it acknowledged was not a universally accepted position) that, as currently written, Section 405(h) does not preclude the exercise of *bankruptcy* jurisdiction over Medicare controversies.[18]

The bankruptcy court's interpretation of Section 405(h), however, was not its only or primary grounds for authorizing Bayou Shores to assume its provider agreements. In point of fact, the bankruptcy court effectively dismissed HHS's invocation of Section 405(h) as a red herring. Rather than relying on an admittedly controversial interpretation of Section 405(h), the bankruptcy court grounded its authority to approve Bayou Shores' assumption of its provider agreements in what it characterized as the independent *bankruptcy* jurisdiction it enjoyed pursuant to 28 U.S.C. § 1334.[19] The bankruptcy court also avoided reviewing HHS pre-bankruptcy determination of Bayou Shores' noncompliance with Medicare statutes and regulations (likely a violation Section 405(h)) by expressly acknowledging and factoring into its analysis Bayou Shores' pre-bankruptcy noncompliance.[20]

In determining whether Bayou Shores could assume its provider agreements, the bankruptcy court focused on the peculiarly bankruptcy question of whether Bayou Shores had met the conditions set forth in Section 365(b) of the Bankruptcy Code for assuming an executory contract—prompt cure of existing defaults and adequate assurance of future performance. As a first step in its analysis, and relying on the express provisions of Section 365 of the Bankruptcy Code and the Third Circuit's opinion in *In re University Medical Center*,[21] the bankruptcy court quickly rejected the notion, imputed to HHS, that Section 365 does not apply to Medicare provider agreements because, under Medicare law, SNF's lack the right to cure pre-bankruptcy defaults.

The bankruptcy court noted in that regard that Section 365 does not provide special treatment for Medicare provider agreements.[22] Considering the record before it, the bankruptcy court then determined that Bayou Shores easily met the conditions of Section 365(b) for assuming its provider agreements.[23] Crucial to the bankruptcy court's determination were the expeditious corrective actions Bayou Shores undertook in response to CMS's citations, the effectiveness of which were corroborated by several witnesses, including the court-appointed patient care ombudsman in Bayou Shores' bankruptcy case. Those corrective measures demonstrated that Bayou Shores had cured its pre-bankruptcy defaults under its provider agreements, as required by 11 U.S.C.

§ 365(b)(1)(A).[24] Bayou Shores' remedial measures, together with its compliance with applicable law while in bankruptcy and its continued retention of a regulatory consultant, similarly demonstrated adequate assurance of Bayou Shores' future performance under the provider agreements, as required by 11 U.S.C. § 365(b)(1)(C).[25]

In sum, the bankruptcy court grounded its decision to authorize Bayou Shores to assume its provider agreements not in an admittedly controversial reading of Section 409(h), but in a conventional reading of Section 365 (particularly Section 365(b)) of the Bankruptcy Code.

Post-confirmation Proceedings and Appeals

HHS and AHCA each appealed the stay and confirmation orders to the district court. Their appeals have been consolidated. Both the bankruptcy and district courts have denied HHS's emergency motions to stay the consummation of the plan pending the resolution of its appeals. HHS and AHCA have filed their opening appellant's briefs. Bayou Shores has filed its appellee's briefs. HHS filed its reply brief, and Bayou Shores has file a motion to strike: 1) arguments raised in the reply brief as not having been raised in the bankruptcy court and 2) an attached exhibit. That motion remains to be heard and decided.

Bayou Shores also filed a motion to dismiss AHCA's appeals, as well as a motion to renew an earlier motion to dismiss HHS's appeals. Both motions were denied on May 19, 2015.

While the consolidated appeals were pending, HHS notified Bayou Shores of its intention to withhold payments for newly admitted Medicare patients. In response, on April 9, 2015, Bayou Shores filed a motion to compel HHS's compliance with the plan, contending that HHS's failure to reimburse Bayou Shores for newly admitted Medicare patients violates the plan and the confirmation order. HHS subsequently agreed to withdraw its notice, and on May 27, 2015, Bayou Shores withdrew its motion.

Conclusion/Relevance

The Bayou Shores saga is by no means over. As of the date this article was submitted for review and publication, AHCA had not filed its reply brief. Oral argument on the appeals and Bayou Shores' motion to strike with respect to HHS's reply brief has not yet been scheduled. The district court could decide the consolidated appeals and Bayou Shores' motion to strike this summer. However, it is virtually certain that appeals will continue to the 11th Circuit, if not to the Supreme Court.

Although the saga is not complete, the Bayou Shores bankruptcy case provides some takeaways.

The first takeaway is that a SNF served with a termination notice should file its bankruptcy petition *before* the termination date set forth in the notice. Doing so will maximize the possibility of a finding that the provider agreement was not terminated before the bankruptcy filing and minimize the possibility that HHS and/or a state Medicaid agency will be permitted to terminate Medicare or Medicaid reimbursements. A corollary to this takeaway is that precious and limited time and effort should not be wasted seeking injunctive relief outside of bankruptcy. The SNF must, however, timely commence an administrative appeal from a termination notice. The second takeaway is that, although the automatic stay may prevent the termination of a provider agreement after a bankruptcy filing, it will not prevent the revocation of an operating license and the resultant closure of a SNF facility based on legitimate patient care and safety issues. As the bankruptcy court made clear, those actions likely constitute valid exercises of police power. Consequently, a SNF entering bankruptcy in the wake of a termination notice *must* quickly attain (if necessary) and maintain appropriate levels of patient care and safety to avoid loss of its operating license and the resultant closure of its facility.

The third takeaway from *Bayou Shores* is that parties-in-interest to a bankruptcy must act expeditiously. The debtor-SNF must fast track its case to obtain confirmation of a plan before the completion of an administrative appeal from a termination notice. Conversely, it behooves HHS and state Medicare agencies to move administrative proceedings along as expeditiously as possible. *Bayou Shores* leaves open the question of the effect of an adverse ruling by an administrative law judge *after a bankruptcy filing* on a SNF-debtor's ability to assume its Medicare and Medicaid provider agreements, which may be decided in a ruling on Bayou Shore's motion to strike.

Finally, the bankruptcy court's reasoning in *Bayou Shores may* also be of particular relevance to hospitals in New Jersey. The recently issued Navigant report had generated heated controversy. Acute care hospitals slated in the report for conversion to ambulatory care facilities

have objected vehemently to the proposed change in their status. The success—thus far—of Bayou Shores in preserving its provider agreements may persuade those hospitals to use bankruptcy as a means of avoiding the proposed conversions of their facilities to ambulatory care facilities. It is a virtual certainty that the state of New Jersey will contest such filings on the basis that a decision to repurpose a hospital falls within the state's police power, a position for which the rulings of the bankruptcy court in *Bayou Shores* provide support. Time will tell whether a creative debtor's counsel can convince a bankruptcy court that repurposing hospitals serves New Jersey's pecuniary as opposed to regulatory interests.

On June 29, 2014, the district court reversed the confirmation order, but only to the extent that it provided for Bayou Shore's assumption of its provider agreements. The district court ruled that the bankruptcy court lacked jurisdiction to consider issues concerning the provider agreements until the debtor had exhausted its administrative remedies with respect to the termination of the agreements. Bayou Shores' counsel advised that Bayou Shores would appeal the district court's order to the 11th Circuit.

David N. Crapo is of counsel to Gibbons P.C., practicing in the financial restructuring and creditors' rights department and on the healthcare team.

Endnotes

1. Case No. 8:14-bk-09521-MGW ("Bayou Shores Bankruptcy Case").
2. 11 U.S.C. § 541(a).
3. *Id.*
4. *See, e.g., In re University Med. Center*, 973 F.2d 1065, 1075 n. 13 (3d Cir. 1992).
5. *See* 11 U.S.C. § 365(a) and (b).
6. *Moody v. Amoco Oil Co.*, 734 F.2d 1200, 1214 (7th Cir. 1984).
7. *In re Fountainbleau Hotel Corp.*, 515 F.2d 913, 915 (5th Cir. 1975).
8. Bayou Shores Bankruptcy Case ECF Docket No. 282 at 12-14.
9. *Id.*, p. 13.
10. *Id.*
11. 11 U.S.C. § 362(a)(3).
12. 11 U.S.C. § 362(b)(4).
13. ECF Docket No. 80, pp. 116-17; ECF Docket No. 282, pp. 18-19.
14. ECF Docket No. 80, p. 117.
15. ECF Docket No. 282, pp. 18-19.
16. *Id.*, p. 19.
17. *Id.*, pp. 18-19
18. *Id.*, pp. 10-11.
19. *Id.*, p. 9.
20. *Id.*, p. 11.
21. 973 F.2d at 1077.
22. ECF Docket No. 282, p. 15.
23. *Id.*, p. 14-17.
24. *Id.*, p. 15-16.
25. *Id.*, p. 16-17.

Telemedicine in New Jersey: The Past, Present and Future

by Lani M. Dornfeld and Michele L. Gipp

Many believe telemedicine (also known as telehealth) is the future of healthcare, and with providers' efforts focused on consolidation, cost-savings, increased access to care and efficiency, this prediction may be accurate.

Telemedicine accomplishes all of these goals by allowing healthcare providers to service patients remotely, benefitting both patients and providers. Although the exact legalities and boundaries of telemedicine are still up in the air, it is hard to ignore the realities of current medicine as the federal and many state governments take great strides to advance telemedicine throughout the United States.

Under current New Jersey law, there is nothing that prohibits (or expressly permits) telemedicine. The New Jersey Legislature seeks to clarify the telemedicine landscape in New Jersey with Assembly Bill A-4231—an all-encompassing bill that expressly authorizes telehealth services in New Jersey by physicians, nurses, physician assistants, licensed clinical social workers and more, so long as the providers are licensed in New Jersey to perform the services. The bill also would allow physicians to prescribe medications via telehealth and require state insurance payors to reimburse providers for telehealth services.[1] If enacted into law as currently proposed, A-4231 would advance New Jersey healthcare by allowing New Jersey licensed providers to continue servicing patients and to prescribe medication remotely. Even if it is not passed, A-4231 sheds light on where New Jersey telemedicine may go in the future.

What is Telemedicine?

Telemedicine is the remote delivery of healthcare services and clinical information by means of telecommunications technology, such as Internet, wireless, satellite, and telephone media. Common examples of telemedicine include patient consultations via video conferencing, remote patient monitoring, review of electronic images, patient portals, and patient-interactive wireless applications. Telemedicine can be used in all medical specialties, by all healthcare providers, and is currently in practice at hospitals, ambulatory surgical centers, home health agencies, hospices, physician groups and more across the United States.

Telemedicine supplements traditional services and is not intended to preclude in-person consultations or treatment. The benefits of telemedicine are substantial, as many providers report an increase in patient access and quality of care and a simultaneous reduction in the cost of services. Patient satisfaction also has increased because telemedicine caters to the on-demand access patients seek and makes it easier for patients to receive specialized healthcare and obtain quick answers.

Affordable Care Act

Although the concept of telemedicine has been around for decades, awareness of telemedicine has surged within the past 10 years because of the increased use of technology in healthcare and the Patient Protection and Affordable Care Act (ACA), which contained many initiatives promoting the utilization of telemedicine and technology in healthcare. For example, the ACA created the Center for Medicare & Medicaid Innovation, a federal agency dedicated to the development and support of innovative healthcare payment and service delivery models that aim to achieve better care for patients and lower costs.[2] These models incorporate telemedicine into healthcare services and rely on electronic remote monitoring of patients or patient-based remote monitoring systems.

Another example of the promotion of telehealth under the ACA includes the requirement that accountable care organizations coordinate care through the use of telehealth, remote patient monitoring and other such enabling technologies.[3] Additionally, under the ACA physicians can use telehealth to certify the need for home health services or durable medical equipment, and a pharmacist or other qualified provider can use telehealth

technologies to perform an annual comprehensive medication review of Medicare drug plan medication therapy management programs or follow-up interventions.[4]

Model Policy from the Federation of State Medical Boards

In response to the growth of telemedicine and the confusion around state regulations, in April 2014, the Federation of State Medical Boards released a model policy for the use of telemedicine entitled, *Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine*.[5] Although state medical boards are not required to adopt the policy, it is intended to guide state medical boards in addressing telemedicine, including defining telemedicine, licensure issues, the establishment of a physician-patient relationship, and the prescription of medicine via telemedicine. The 2014 policy supersedes the federation's 2002 policy on the appropriate use of the Internet in medical practice and incorporates guidance on the latest technological developments.

Definition of Telemedicine

The model policy defines telemedicine as "the practice of medicine using electronic communications, information technology or other means between a licensee in one location and a patient in another location with or without an intervening healthcare provider."[6] Telemedicine is more than an audio-only, telephone conversation, email conversation, instant messaging or fax, and typically involves secure videoconferencing or other means to replicate the traditional in-person encounter between a physician and a patient.

Licensure

Physicians must be licensed to practice medicine in the state where the patient is physically located.[7] The policy also clarifies that physicians who treat or prescribe medication via online service sites are practicing medicine and must be licensed in all jurisdictions where patients receive care.

Establishment of the Physician-Patient Relationship

The federation recognizes the difficulty in precisely defining the beginning of the physician-patient relationship and notes it may begin when an individual seeks assistance from a physician for a health-related matter. The policy states "the relationship is clearly established when the physician agrees to undertake diagnosis and treatment of the patient, and the patient agrees to be treated, whether or not there has been an encounter in person between the physician (or other appropriately supervised health care practitioner) and patient."[8]

Because the physician-patient relationship is fundamental to medical care, physicians providing services via telemedicine should disclose their identity and credentials to the patient and should verify and authenticate the location and, if possible, the identity of the requesting patient.[9] The model policy states an appropriate physician-patient relationship has not been established when the patient does not know the physician's identity. Physicians also should inform patients of the delivery model, the treatment method or limitations, and obtain informed consents for the use of telemedicine technologies. The patient must be able to select his or her physician where appropriate.

Prescribing Medication

Physicians may use their professional discretion to prescribe medications via telemedicine, and are held to the same standards of practice, ethics and professional accountability as if prescribing medications in person. As long as physicians uphold these standards and evaluate the indication, appropriateness, and safety considerations for each telemedicine prescription, the model policy recommends physicians be able to prescribe medication through telemedicine.[10]

Physicians using telemedicine to prescribe medication do not conduct a traditional physical examination. Therefore, physicians must implement additional patient safety measures to clearly establish the identity of the patient and provider, and maintain detailed documentation of the clinical evaluation and prescription. The policy encourages measures that assure informed, accurate and error prevention prescribing practices, such as integration with e-prescription systems.[11]

New Jersey's Current Telemedicine Landscape

New Jersey is considered one of the leading states in the promotion of telemedicine because its current statutory and regulatory framework supports the provision of healthcare services through telemedicine in certain circumstances. The state, however, still lags behind many others in reimbursement for telemedicine services.

A-4231 is the Legislature's latest effort to further advance telemedicine and create insurance parity in New Jersey, and if enacted would create benefits for both New Jersey patients and healthcare providers.

Current Legal Framework

Under current New Jersey law, there is no prohibition on the provision of telemedicine services if a physician is licensed to practice medicine in New Jersey and the patient is located in the state at the time of treatment. With limited exceptions, however, a physician cannot prescribe medication to the patient through telemedicine because the New Jersey Board of Medical Examiners' regulations require the physician to conduct a personal examination of the patient.[12] An exception exists if the patient is an established patient of the physician and the physician, based on sound medical practice, does not believe the patient requires a new examination before issuing a new prescription.[13]

New Jersey Insurance Companies

Even though physicians may perform services via telemedicine in the state, a common problem New Jersey providers face is reimbursement for the services. Currently, providers are limited to the amounts they can collect from patients because many private payors and New Jersey Medicaid do not reimburse for telehealth services.

Legislative Efforts

In the past year, the New Jersey Legislature has taken steps to advance telemedicine in the state. For example, in response to insurance payors' practice of denying claims for telehealth services, in Aug. 2014 Senator Shirley K. Turner introduced S-2337 and S-2338, which, if they had been enacted, would have prohibited payors such as New Jersey Medicaid from requiring in-person contact before a telemedicine encounter as a condition of payment.[14] Although the bills have not been enacted, insurance parity for telemedicine services is incorporated into A-4231.

Assembly Bill A-4231

On Feb. 24, 2015, the New Jersey Assembly introduced A-4231, a 53-page bill that expressly authorizes telemedicine services in New Jersey. The bill contains provisions similar to the federation's model policy for physicians and also expands telehealth services to other types of healthcare providers.

A-4231 states "a health care practitioner may remotely provide health care services to a patient in [New Jersey], and a bona fide relationship between health care practitioner and patient may be established, through the use of telemedicine."[15] Like the model policy, healthcare practitioners providing telemedicine services are subject to the same standards of care and rules of practice that apply to traditional in-person practice and the use of telemedicine does not alter or diminish any existing duty or responsibility of the healthcare practitioner, including recordkeeping and confidentiality obligations.[16]

Key definitions in the bill are:

> *Health care practitioner:* an individual who provides a health care service to a patient in [New Jersey] and includes, but is not limited to, a physician, nurse practitioner, psychologist, psychiatrist, psychoanalyst, licensed clinical social worker, physician assistant or any other health care professional acting within the scope of a valid license or certification issued pursuant to Title 45 of the Revised Statutes.
>
> *Telemedicine:* the delivery of a health care service using electronic communications, information technology, or other electronic or technological means to bridge the gap between the health care practitioner who is located at one site, and a patient who is located at a different, remote site, either with or without the assistance of an intervening health care provider, and which typically involves the provision of health care services through the application of secure, two-way videoconferencing or store-and-forward technology that is designed to replicate the traditional in-person encounter and interaction between health care practitioner and patient by allowing for interactive, real-time visual and auditory communication, and the electronic transmission of images, diagnostics, and medical records. Telemedicine does not include the use of audio-only telephone conversation, electronic mail, instant messaging, phone text, or facsimile transmission.[17]

The definition of telemedicine set forth in A-4231 includes some of the concepts used in the model policy's definition of telemedicine.

A-4231 broadens the scope of telehealth services in New Jersey, so long as the practitioner is licensed in the state to provide the services. Additionally, healthcare practitioners are permitted to consult with out-of-state peer professionals using electronic or other means, and are not required to obtain an additional license or separate authorization to do so.[18]

The New Jersey State Board of Medical Examiners (BME) and other New Jersey licensing boards are tasked with adopting rules and regulations to implement the provisions of the bill.[19] This presumably would include developing parameters for the establishment of the physician-patient relationship, which, unlike the federation's model policy, A-4231 does not address. Further, the BME would be required to evaluate the Federation of State Medical Boards' Telemedicine Licensure Compact, a proposal setting forth procedures to obtain reciprocal licensure for physicians across states, and determine what legislation or state actions are necessary to enable New Jersey to participate in the compact.[20]

A-4231 also would create insurance parity for telehealth services. The bill provides that telemedicine services would be covered under the New Jersey Medicaid and NJ FamilyCare programs to the same extent they would be covered if they were delivered through traditional in-person means, and telehealth services receive the same reimbursement rates as in-person services.[21] In-person contact cannot be a requirement as a condition of payment under the Medicaid or NJ FamilyCare programs. The insurance parity requirements also apply to managed care plans and other state health benefits.

Lastly, the bill would permit physicians to prescribe medications through the use of telemedicine if they have first engaged in a face-to-face examination of a patient.[22]

What Does This Mean for Providers?

As currently proposed, A-4231 is expansive and applies not only to telemedicine services by physicians, but also by nurse practitioners, psychologists, psychiatrists, psychoanalysts, licensed clinical social workers, physician assistants and more. The bill would permit physicians to prescribe medications through a telemedicine encounter, and importantly would allow providers to obtain reimbursement from state payors for telehealth services. With regard to licensure, as under current law, practitioners must be licensed in New Jersey to perform telehealth services for patients located in New Jersey, but the bill creates more opportunity for out-of-state providers to obtain reciprocal licensure to perform services in this state.

Until the bill is passed, however, providers must continue to operate under current law, which means physicians cannot prescribe medication through a telemedicine encounter unless an exception applies. Further, providers likely will not obtain reimbursement for their telehealth services. Therefore, until A-4231 (or similar legislation) is passed, New Jersey providers are at a crossroads in terms of expanding their telehealth services versus continuing to further their traditional in-person service models. Because the popularity of telemedicine in healthcare will only continue to grow, providers should explore their telemedicine capabilities while keeping in mind the restrictions placed on telemedicine services in New Jersey.

Conclusion

The authors believe enactment of A-4231 would be an important step in clarifying telemedicine services in New Jersey. New Jersey physicians and other healthcare providers would be able to serve patients and prescribe medication remotely, creating greater access to care, promoting efficiency, and cutting healthcare costs. Providers also would obtain insurance parity from state payors for telehealth services. Until then, as telemedicine services continue to advance throughout the United States, A-4231 sheds light on what telemedicine in New Jersey may look like in the future, and New Jersey providers and their healthcare counsel should be prepared to move forward. ■

Lani M. Dornfeld is a member of the health law practice group of Brach Eichler L.L.C., based in Roseland. Michele L. Gipp is an associate in the health law practice group of Brach Eichler L.L.C., based in Roseland.

Endnotes

1. *See* A. 4231, 216th Leg. (N.J. 2015).
2. *See* 42 U.S.C. § 1315a.
3. *See id.* § 1395jjj(b)(2)(G).
4. *See id.* § 1395f(a)(2)(C); *see also id.* § 1395w-104(c)(2).
5. *See* Model Pol'y for the Appropriate Use of Telemed. Techs. In the Prac. of Med. (Fed'n of St. Med. Boards, 2014).
6. *Id.* § 3.
7. *See id.* § 4.
8. *Id.* § 2.
9. *See id.*
10. *See id.*
11. *See id.*
12. *See* N.J.A.C. § 13:35-7.1A(a).
13. *See id.* § 13:35-7.1A(b)(4).
14. *See* S. 2337, 216th Leg. (N.J. 2014); S. 2338, 216th Leg. (N.J. 2014).
15. A-4231, 216th Leg. (N.J. 2015).
16. *See id.*
17. *Id.*
18. *See id.*
19. *See id.*
20. *See id.*
21. *See id.*
22. *See id.*

Medical Identity Theft: The Need to Protect Consumers through Compliance

by Kate Slavin

Medical identity theft is a growing concern in the United States, especially in light of the growth of technology in healthcare in recent years. The cost of a medical identity on the black market far exceeds that of a financial identity, being 10 to 20 times more expensive.[1] The Federal Bureau of Investigation (FBI) recently specifically issued a warning to the healthcare industry stating that the risk has increased and action must be taken accordingly.

Medical identity theft can be devastating to consumers' physical and financial wellbeing. In addition to debt collections and financial woes, it can also result in a host of harms to the patient: medical records containing incorrect information, receipt of the wrong treatment, exhaustion of health insurance, and uninsurability for health and life insurance.[2] These intangible harms can be accompanied by loss of reputation, time, and privacy.[3]

The methods of medical identity theft vary. It can occur by a thief using another's identity to obtain medical care and/or prescriptions.[4] The thief might be uninsured, or may not want the care or prescriptions on his or her medical record. It can result from fraud—the submission of false claims to insurance providers for services not rendered.[5]

There are many real-life examples of the impact on individuals' lives, including:

1. Social services accused a mother of four children of having a newborn baby that tested positive for methamphetamine. She had not given birth recently, and had no substance abuse issues. Notwithstanding the threat to take her four children away, she was able to work with law enforcement to link the incident to medical identity theft.[6]
2. A Massachusetts psychiatrist entered false records on individuals who were not his patients, giving them behavioral health diagnoses affecting the victims' employment and insurance coverage.[7]
3. Medical identity theft resulted in a change to a woman's medical record to include a foot amputation she never received and to add a diabetes diagnosis. She learned of the diagnosis shortly before a surgery during an emergency admission and was able to correct the medical staff before any fatal impact could occur.[8]

The Federal Trade Commission (FTC) defines medical identity theft as someone using "another person's name or insurance information to get medical treatment, prescription drugs or surgery."[9] It also includes "dishonest people working in a medical setting [using] another person's information to submit false bills to insurance companies."[10] Many times, medical identity theft is caused by a data breach within the organization holding the information. Criminal attacks on healthcare organizations' networks have increased by 100 percent in the last five years.[11] The "persistent and growing threat of healthcare breaches" represents one of the top six data breach trends for 2015.[12] Such breaches have a potential cost of $7 billion.[13] Not only are organizations subject to hefty Health Insurance Portability and Accountability Act (HIPAA) fines,[14] but they also foot the bill for post-breach costs amounting to about $233 per record, including victim notification, credit reporting, incident handling, and lost opportunities.[15]

A large barrier in effectively preventing data breach threats is the cost. Many smaller organizations do not have the resources to protected health information (PHI).[16] Some providers are forced to choose medical equipment over adequate protection against medical identity theft.[17] In addition to not having the resources, some organizations are frankly failing to focus their resources on protecting health information. In a survey of healthcare organizations, 32.7 percent of the organizations stated they spend less than 10 percent of their information technology (IT) budget on securing patient data.[18] Even more alarmingly, eight percent did not spend any of their budgets on it.[19] However, the cost of a breach can far exceed the prevention costs.

In order to fully address and understand the current

state and threat of medical identity theft, this article will explore the threat to the healthcare industry, federal law, enforcement mechanisms, and federal guidance regarding steps that can be taken to guard against these breaches. In assessing compliance by organizations, the article will also explore best practices and organization compliance.

The three most vital elements that organizations must address are risk assessments, workforce training, and data encryption. Continual and comprehensive review of those areas must be done to properly safeguard the PHI of patients, as well as protect the organization. Applicable New Jersey state law will be discussed, including the new encryption mandate on health insurance carriers, and whether expansion of the law would best protect consumers from medical identity theft.

The Threat of Identity Theft on the Healthcare Industry

Industry forecasts credit the increase in threat to healthcare breaches in part to the switch to electronic health records (EHRs) and the introduction of wearable technology.[20] The economic gain in obtaining healthcare records is very attractive to the cybercriminal. Not only do medical records include personally identifiable information (PII),[21] but they also include PHI.[22]

PII is defined as:

> [A]ny information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.[23]

PHI is defined as "individually identifiable information." Individually identifiable information is:

> [I]nformation that is a subset of health information, including demographic information collected from an individual, and: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.[24]

The value of a medical record is about 10 to 20 times the value of credit card information.[25] Any PII increases the price of the identity as well, which is typically included in a medical record.[26]

As the healthcare industry grows, new efforts and trends present additional opportunities for medical identity theft. Participation in accountable care organizations increases exposure for organizations.[27] There is also much concern regarding the security of new health information exchanges (HIEs).[28] There will always be new concepts and technology that potentially increase exposure.

Governmental focus and executive action regarding identity theft continues to increase in recent years. In 2009, President Barack Obama created the Identity Theft Task Force in an effort to strengthen federal efforts to protect against identity theft.[29] The task force intends to accomplish this through more aggressive law enforcement actions and improved public outreach.[30] The strategic plan involves four areas of focus: data protection, data integrity, victim assistance, and deterrence.[31] In addition, the White House announced on Feb. 10, 2015, the creation of a new $35 million agency—the Cyber Threat Intelligence Integration Center—to combat cyber threats.[32] The agency is to facilitate bridging the gaps between departments and agencies regarding cyberthreats in the United States by sharing information as close to real-time as possible.[33] Last year, the Cyber Division of the FBI issued a private industry notification to warn the healthcare industry that it is at increased risk for cyber attacks.[34] The FBI is concerned the industry is less equipped to handle these threats than other industries.

There have been several large healthcare data breaches recently. In July 2014, Community Health Systems in Tennessee confirmed a breach occurred in April and June of 2014.[35] Hackers from China used malware to obtain patient information.[36] The breach affected 4.5 million patients in 29 states.[37] Community Health Systems is currently facing multiple class action lawsuits because of the data breach.[38] Most recently, Anthem Blue

Cross Blue Shield announced a data breach affecting over 80 million patients.[39] The hackers accessed the following: names, dates of birth, Social Security numbers, healthcare ID numbers, home and email addresses, and work information (such as income data).[40] This was announced in early Feb. 2015, and there was a $5 million class action filed in early March 2015.

As numerous serious data breaches continue to occur in the healthcare industry, it is imperative to have an understanding of the law, guidance, and best practices for compliance.

Federal Law

HIPAA and HITECH

While a slew of laws exist to protect personal information,[41] healthcare privacy is governed separately. HIPAA[42] and the Health Information and Technology for Economic and Clinical Health Act (HITECH Act), [43] which amended HIPAA in 2009, comprise the primary federal regulation structure that governs data breach in healthcare. The omnibus rule again amended this body of law in 2013.[44] HIPAA attempts to "improve portability and continuity of health insurance coverage in the group and individual markets," and "to *combat waste, fraud, and abuse* in health insurance."[45]

The Office of Civil Rights (OCR) of the U.S. Department of Health and Human Services (DHHS) enforces HIPAA.[46] The privacy rule,[47] the security rule,[48] and the breach notification rule[49] within HIPAA are most pertinent to the issues concerning medical identity theft. Healthcare organizations must constantly review their data security practices and compliance with information safeguard provisions within the privacy and security rules in order to prevent charges of wrongful disclosure of information, and other sanctions.[50]

Disclosures of patient information are governed by the privacy rule, which requires that covered entities[51] only disclose protected health information when specifically permitted by the law.[52] Furthermore, even if disclosure is permitted, the rule governs the extent of disclosure. Specifically, the rule requires that covered entities employ a minimum necessary standard when using, disclosing, or requesting PHI.[53] The minimum necessary standard requires evaluation of practices and enhancement of safeguards in order to guard against unnecessary and inappropriate uses and disclosures.[54] The privacy rule requires that the holder of PHI provide all patients with a notice of privacy practices for the organization and inform patients of their privacy rights.[55] In addition, it provides patients with rights to notifications of disclosures of their information, as well as the ability to make corrections to their information.[56] There are many administrative requirements under the rule regulating covered entities.[57] These requirements include: documentation of a privacy official, contact for complaints, workplace training, sanctions, mitigation of violations, compliance policies and procedures, and notice of privacy practices changes; no intimidation or retaliatory acts; compliance with updates to laws and regulations; and retention of documentation for six years.[58] The privacy rule also created criminal and civil penalties for those who violate the privacy of PHI, which were amended by the HITECH Act.

The security rule applies to electronic PHI (ePHI) and focuses on the security of three areas of patient information: administrative, technical, and physical.[59] The security rule requires that organizations have both required and addressable safeguards to ensure the security of PHI.[60] While required safeguards must be implemented, addressable safeguards can be assessed per covered entity based on reasonability and appropriateness, as long as the decision is documented.[61] The three categories of safeguards are: administrative,[62] technical,[63] and physical.[64]

The security rule designates as a 'business associate' any organization that creates, maintains, receives, or transmits PHI on behalf of a covered entity.[65] Business associates (BAs) include any certified public accountant, attorney, consultant, transcriptionist, etc. with access to the covered entity's PHI.[66] Business associates must enter into a business associate agreement with the covered entity, which outlines the responsibilities and duties the organization will have to the covered entity.[67] These business associates must also comply with safeguards and administrative requirements to ensure privacy and security of PHI.[68]

The breach notification rule, which strengthened HIPAA when the HITECH Act was enacted and even more so when amended by the omnibus rule (discussed below), requires that patients know when their information has been breached. The law imposes the duty to accomplish this obligation on the holder of the information. The first question is when this duty to notify arises. The breach notification rule defines a breach as

"the acquisition, access, use, or disclosure of [PHI] in a manner not permitted…which compromises the security or privacy of the [PHI]."[69] Compromising the security or privacy of PHI occurs when "significant risk of financial, reputational, or other harm to the individual" is posed.[70] Organizations must conduct notifications, based on the succeeding circumstances, within 60 days of discovery of the breach. Individuals affected must be notified when a breach occurs.[71] Organizations must notify HHS if there are 500 or more individuals affected,[72] and the media if more than 500 state residents are affected.[73] Business associates are required to notify covered entities of breaches within 60 days of discovery.[74]

Most recently, all of these rules were strengthened and amended by the 2013 modifications to the HIPAA privacy, security enforcement, and breach notification rules under the HITECH Act and the Genetic Information Nondiscrimination Act (the omnibus rule).[75] The omnibus rule introduced a presumption that any access, use, or disclosure of PHI must be reported to HHS *unless* the entity can prove low probability of compromise of PHI.[76] This must be done through assessment of a four-part test exploring: 1) the nature and extent of information involved in the access, use, or disclosure; 2) who the unauthorized person was; 3) whether information was actually viewed or acquired; and 4) the extent to which risk was mitigated after the disclosure.[77] This new assessment standard results in more reportable breaches than the previous breach notification assessment standard.[78]

The omnibus rule provides for three exceptions to a disclosure being considered a breach.[79] A disclosure is not a breach if the disclosure was: 1) "an unintentional access to [PHI] in good faith in the course of performing one's job, and such access does not result in further impermissible use or disclosure;" 2) "inadvertent disclosure of [PHI] by a person authorized to access the information to another person authorized to access information at the same healthcare entity;" or 3) "improper but the healthcare entity believes in good faith that the recipient of the information would not be able to retain the information."[80]

The omnibus rule also addressed liability for BAs.[81] The definition of BAs was expanded to include entities that provide data transmission services for PHI, and even to entities that maintain PHI without ever viewing or accessing the information.[82] Not only are BAs now directly liable for many of the same provisions as covered entities, but the covered entities are now liable for certain actions of BAs under a new agency provision of the omnibus rule.[83] This has increased liability and exposure to both BAs and covered entities dramatically.

HHS posts all breaches affecting over 500 people on its website.[84] This is commonly known in the healthcare industry was the "Wall of Shame."[85] It is suggested by the American Health Information Management Association (AHIMA) that healthcare executives analyze the breaches on the wall in order to prevent them within their own organizations.[86]

Enforcement

The omnibus rule changed the penalty structure to a tiered system.[87] The general penalty for noncompliance with HIPAA is no more than $100 per violation, not to exceed $25,000 per calendar year.[88] If noncompliance takes place knowingly, one may be charged with the wrongful disclosure of individually identifiable health information.[89] Under this offense, the entity may be subject to much more substantial penalties.[90] Those who commit medical identity theft may be subject to criminal fines,[91] restitution,[92] prison time,[93] civil money penalties,[94] and exclusion from Medicare and Medicaid programs.[95] In addition to general penalties under HIPAA, state attorneys may assess penalties as well. Although state liability theories may provide alternatives for a wronged individual, there is no federal private right of action under HIPAA.[96]

As HIPAA enforcement is on the rise, the prosecution of HIPAA violations has not slowed down. On April 10, 2013, the owner of a medical supply company was sentenced to 12 years in prison for her part in a medical identity theft scheme.[97] On Aug. 28, 2014, a former Texas hospital employee was sentenced to 18 months in prison for wrongful disclosure of individually identifiable health information.[98] He had obtained the PHI to use for personal gain.[99] On April 17, 2015, a Chicago man was sentenced to 10 years in prison for a medical identity theft scheme and ordered to pay $23 million in restitution to Medicare for this fraud.[100] These prosecutions are being reported weekly, with no hint of slowing down.

The FTC retains enforcement authority over ensuring that any privacy and security practices are neither unreasonable nor deceptive.[101] This is not limited to healthcare organizations, but applies to them if they are violative. If an organization fails to use reasonable security measures, the FTC can charge them with 'unfair'

or 'deceptive' trade practice under the Federal Trade Commission Act.[102] Although the FTC cannot impose monetary penalties as HHS is permitted, its settlements can be highly burdensome, and litigation can be lengthy and exorbitant.[103] Organizations may also be charged with aggravated identity theft under the Identity Theft and Assumption Deterrence Act.[104] This is in addition to the enforcement under HIPAA by HHS and the Department of Justice.

Federal Preemption of State Law

Although HIPAA and its counterparts comprise a robust regulatory structure of this body of law, state laws are not exclusively preempted. The supremacy clause of the United States Constitution declares federal law to be the "supreme Law of the Land."[105] Federal law can preempt state law either expressly or impliedly.[106] Preemption can be either explicitly stated in the federal statute or implicit by nature and structure of the clear congressional intent to preempt state or local law.

Considering the states proximity to the actual issues that arise in their jurisdiction, they may be best to construct laws that protect the healthcare industry and patient privacy.

HIPAA expressly addresses preemption. State law will generally not be preempted unless it is contrary to HIPAA, thus making it impossible for entities to comply with HIPAA if they comply with the state law.[107] If the state law is "more stringent" than the HIPAA standards, requirements, or implementation specifications, it will stand.[108] Each state law must be individually examined for this determination.[109] However, it is clear that states have ample room to enact supplementary laws to best protect consumers from medical identity theft that will not be preempted by HIPAA.[110] State laws possess the benefit of subsidiarity, in which the representatives of the state legislature are closer to the issues their consumers and businesses face, here healthcare privacy and security. This may be either unique or ubiquitous to that particular state. The representatives of the state must be free to experiment and test whether specific remedies should be applied to address these issues, which may result in more innovative, or simply better-attuned remedies. These remedies are best to fit the needs of their constituents than the laws of the federal government when tailored to the specific consumers and businesses of the state. "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[111] It is imperative that states take advantage of their opportunities to supplement HIPAA in order to best serve their consumers.

Federal Guidance

In a joint conference held by OCR and the National Institute of Standards and Technology (NIST),[112] they stated that safeguarding health information should be broken into three phases.[113] The phases are: 1) risk assessment, 2) workforce training, and 3) adequate encryption. OCR noted that it sees failure in the adequate completion of risk assessments in healthcare organizations, which is not an excuse for non-compliance. The security risk assessment tool was cited as one of the many resources available by the Office of the National Coordinator for Health Information Technology (ONC), OCR and NIST to ensure compliance. At the conference, the acting chief of NIST's Computer Security Division, Matthew Scholl, stated that education is the best compliance tool. The speakers asserted that although no breach or loss can be completely prevented, encryption protects the actual data when such an event occurs. They stated that *all* breaches resulting from theft and loss on OCR's "Wall of Shame"[114] could have been prevented by encryption.

New Jersey State Law

Current New Jersey Statutes

New Jersey has a breach notification law that applies to businesses and public entities, requiring notification and free credit reports to consumers when a security breach occurs.[115] The law is not exclusive to the healthcare industry, but is applicable to it. Under the statute, a "breach of security" is defined as:

> [U]nauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.[116]

The scienter required for a breach of security is "to

willfully, knowingly or *recklessly* violate" the statute.[117] Therefore, a business or public entity need not specifically be willful or knowing in the breach; it is enough that it acted recklessly in regard to the breach. In addition, there is an encryption safe harbor that excuses businesses and entities if the personal information was encrypted.[118] This provides a huge incentive for businesses and entities to encrypt their data, aside from ensuring their consumers' privacy and security.

There is a new law in New Jersey that will go into effect on Aug. 1, 2015, relating to encryption of healthcare data.[119] This law will apply only to health insurance carriers who are authorized to issue health benefits.[120] Under this law, in addition to requirements under HIPAA and the HITECH Act, the carriers will be required to encrypt personal information that is stored electronically.[121] The definition of personal information will be the same as the previously discussed New Jersey breach notification law. This encryption mandate applies to "end user computer systems"[122] and "computerized records[123] transmitted across public networks."[124]

This law appears to be in response to the Horizon Blue Cross Blue Shield breach resulting from two stolen unencrypted laptops that occurred in 2013, potentially affecting over 840,000 subscribers.[125] A class action lawsuit was filed, but denied in April 2015, for lack of sufficient injury to show standing, but may have been successful with proof of identity theft.[126] The plaintiffs attempted to rely on Horizon's failure to implement security measures after a 2008 breach of subscriber data.[127] Implementation of the security measures, especially encryption, could have prevented the 2013 breach and, in turn, the litigation costs of this class action lawsuit.

Both of these New Jersey laws are within the New Jersey Consumer Fraud Act (NJCFA).[128] For violations of the NJCFA, treble damages, attorney fees, and reasonable costs of the lawsuit may be awarded to a successful plaintiff, in addition to any legal or equitable claim.[129] Providing consumers with these additional remedies is in line with the NJCFA's purposes of: 1) compensating victims, 2) punishing and deterring fraudulent business practices, and 3) providing incentives to competent attorneys to litigate these consumer protection matters.[130]

New Jersey State Law Should Include Encryption for All Healthcare Entities

As stated earlier, state law is not preempted if it is more stringent than HIPAA, and is not contrary to it. This provides New Jersey with ample room to regulate the healthcare industry to prevent medical identity theft and protect consumers who fall victim to it. Although the state has made strides in the form of the encryption mandate on health insurance carriers, the author believes the law should be exclusive of the entire healthcare industry. The federal government has advised encryption to be an effective prevention technique, as it would prevent access to health information despite theft or breach. There is no allegation or evidence that it would be any less effective for the remainder of the healthcare industry, outside of carriers. The author believes New Jersey's encryption mandate should apply to all entities in the healthcare industry to best prevent data breach, and best protect New Jersey consumers.

Conclusion

Medical identity theft is a pressing issue in the healthcare industry. There have been warnings and increased focus by the federal government. The key to avoiding fines and other enforcement mechanisms is to ensure that personal information and PHI are secure and protected. The solution to this is organizational compliance. It is increasingly imperative that organizations regularly and consistently conduct comprehensive risk assessments to ensure compliance and best practices. Properly addressing workforce training based on guidance and legislation is essential to prevent breaches and ensure protection of information. Encryption must be in place and adequate in order to ensure that protected information is secure even when a breach does occur. It is crucial that healthcare organizations devote resources to guarding against medical identity theft in order to protect themselves and their consumers. The author believes the New Jersey encryption mandate should be applied to all of the healthcare industry, rather than limited to carriers, in order to best protect consumers from medical identity theft due to data breach. ■

Kate Slavin is a rising fourth year evening student at Seton Hall University School of Law concentrating in health law. Prior to law school, she explored a career in healthcare management. She is currently serving as a law clerk at Summit Medical Group.

Endnotes

1. Caroline Humer and Jim Finkle, Your medical record is worth more to hackers than your credit card, Reuters, Sept. 24, 2014, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.
2. Pam Dixon, Medical Identity Theft: The Information Crime That Can Kill You, *The World Privacy Forum*, pg. 6, (Spring 2006).
3. *Id*. at 29-30.
4. Daniel R. Levinson, CMS Response to Breaches and Medical Identity Theft, Office of Inspector General, Oct. 2012, http://oig.hhs.gov/oei/reports/oei-02-10-00040.pdf.
5. *Id.*
6. Caitlin Johnson, Protect Against Medical Identity Theft, CBS News, Oct. 9, 2006, http://www.cbsnews.com/news/protect-against-medical-id-theft/.
7. *United States v. Skodnek*, 933 F. Supp. 1108, 1109 (D. Mass. 1996).
8. Katherine Sullivan, But Doctor, I Still Have Both Feet! Remedial Problems Faced by Victims of Medical Identity Theft, 1, (2009).
9. Medical Identity Theft: FAQs for Health Care Providers and Health Plans, Federal Trade Commission, Jan. 2011, http://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.
10. *Id.*
11. Fourth Annual Benchmark Study on Patient Privacy & Data Security, ID Experts, March 2014, https://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents.
12. 2015 Second Annual Data Breach Industry Forecast, Experian, http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last visited April 21, 2015).
13. Erin McCann, Healthcare data breaches on the rise, with potential $7B price tag, *Healthcare IT News*, Dec. 6, 2012, http://www.healthcareitnews.com/news/healthcare-data-breaches-trend-upward-come-potential-7b-price-tag.
14. Wellpoint Resolution Agreement, U.S. Department of Health & Human Services, July 8, 2013, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/wellpoint-agreement.pdf.
15. 2013 Cost of a Data Breach, Ponemon, May 2013, http://www.ponemon.org/local/upload/file/2013%20Report%20CODB%20FINAL%205-2.pdf.
16. 2015 Second Annual Data Breach Industry Forecast, Experian, http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last visited April 21, 2015).
17. Caroline Humer and Jim Finkle, Your medical record is worth more to hackers than your credit card, Reuters, Sept. 24, 2014, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.
18. Finding a Cure for Medical Identity Theft, CSID, Oct. 2014, http://www.csId.com/wp-content/uploads/2014/10/CSID_Whitepaper_Medical-ID-Theft.pdf.
19. *Id.*
20. 2015 Second Annual Data Breach Industry Forecast, Experian, http://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf (last visited April 21, 2015).
21. GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, United States Government Accountability Office, May 2008, http://www.gao.gov/new.items/d08536.pdf.
22. 45 C.F.R. 160.103.
23. GAO Report 08-536, Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information, United States Government Accountability Office, May 2008, http://www.gao.gov/new.items/d08536.pdf.
24. 45 C.F.R. 160.103.
25. Caroline Humer and Jim Finkle, Your medical record is worth more to hackers than your credit card, Reuters, Sept. 24, 2014, http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.
26. I*d.*
27. Fourth Annual Benchmark Study on Patient Privacy & Data Security, ID Experts, March 2014 https://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents.
28. *Id.*
29. Executive Order 13402, May 10, 2006.
30. *Id.*

31. The President's Identity Theft Task Force Report Combating Identity Theft—A Strategic Plan, Federal Trade Commission, pg. 3-6 (Sept. 2008).
32. Dustin Volz, Obama is Creating a New Agency to Combat Cyberthreats, *National Journal*, http://www.nationaljournal.com/tech/obama-is-forming-a-new-agency-to-combat-cyber-threats-20150210.
33. *Id.*
34. FBI Cyber Division Private Industry Notification, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain, *Public Intelligence*, April 8, 2014, https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.
35. Andi Bosshart, Data Breach Notification, Community Health Systems, http://www.chs.net/media-notice/ (last visited April 21, 2015).
36. *Id.*
37. Cynthia Larose, Massive Data Breach Affects 4.5 Million Patients in 29 States, *Privacy and Security Matters*, Aug. 20, 2014, http://www.privacyandsecuritymatters.com/2014/08/massive-data-breach-affects-4-5-million-patients-in-29-states.
38. Darius Tahir, Community Health Systems faces data-breach class action, *Modern Healthcare*, Oct. 13, 2014, http://www.modernhealthcare.com/article/20141013/NEWS/310139945; Second Lawsuit Filed Over Community Health Systems Data Breach, iHealthBeat, Oct. 14, 2914, http://www.ihealthbeat.org/articles/2014/10/14/second-lawsuit-filed-over-community-health-systems-data-breach.
39. Anthem created a website dedicated to the breach. How to Access & Sign Up for Identity Theft Repair & Credit Monitoring Services, *Anthem*, http://www.anthemfacts.com (last visited April 21, 2015).
40. *Id.*
41. For example, the Fair Credit Reporting Act (FCRA) governs privacy of general personal information. 15 U.S.C. § 1681 *et al.*
42. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 1936 (1996).
43. Health Information Technology for Economic and Clinical Health Act (HITECH Act), Pub. L. No. 111-5, 123 Stat. 115 (2009).
44. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 FR 5566-01 (*incorporated at* 45 C.F.R. Parts 160 and 164), (hereinafter the Omnibus Rule).
45. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 1936 (1996) (emphasis added).
46. *Id.*
47. 45 C.F.R. Pt. 160; 45 C.F.R. Pt. 164.
48. 45 C.F.R. Pt. 160; 45 C.F.R. Pt. 164, subparts A and C.
49. 45 C.F.R. Pt. 164, subpart D.
50. Medical Identity Theft: FAQs for Health Care Providers and Health Plans, Federal Trade Commission, Jan. 2011, http://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.
51. Covered entities include healthcare providers, health plans, and healthcare clearinghouses. HIPAA, Pub. L. No. 104-191, 110 Stat. 1936, 2021-2023.
52. There are permitted uses, as well as required disclosures. 45 C.F.R. 164.502.
53. 45 C.F.R. 164.502(b), 164-514(d).
54. Minimum Necessary, United States Department of Health & Human Services, April 4, 2003, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.pdf.
55. 45 C.F.R. 164.520.
56. *Id.*
57. 45 C.F.R. 164.530.
58. *Id.*
59. 45 C.F.R. Pt. 164.
60. *Id.*
61. Security Rule FAQs, United States Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2020.html.
62. 45 C.F.R. 164.308.
63. 45 C.F.R. 164.310.
64. 45 C.F.R. 164.312.
65. 45 C.F.R. 164.308(b).
66. Business Associates, United States Department of Health & Human Services, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (last visited April 21, 2015).
67. *Id.*

68. 45 C.F.R. 164.316.
69. 45 C.F.R. 164.402.
70. *Id.*
71. 45 C.F.R. 164.406.
72. 45 C.F.R. 164.410.
73. 45 C.F.R. 164.408.
74. 45 C.F.R. 164.412.
75. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 FR 5566-01 (*incorporated at* 45 C.F.R. Parts 160 and 164) (Omnibus Rule).
76. *Id.*
77. *Id.*
78. Cindy Gallee, The Importance of Data Encryption and Security Rules: Breaches of Electronic Protected Health Information Under HIPAA and HITECH, 26 DCBA Brief 16, 18 (2014).
79. *Id.*
80. Cindy Gallee, The Importance of Data Encryption and Security Rules: Breaches of Electronic Protected Health Information Under HIPAA and HITECH, 26 DCBA Brief 16, 18 (2014).
81. Omnibus Rule.
82. *Id.*
83. *Id.*
84. Breach Portal, United States Health & Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
85. Mark Taylor, Hospital Battle Data Breaches With a Cybersecurity SOS, *Hospitals & Health Networks*, Feb. 10, 2015, http://www.hhnmag.com/display/HHN-news-article.dhtml?dcrPath=/templatedata/HF_Common/NewsArticle/data/HHN/Magazine/2015/Feb/fea-hospital-cybersecurity.
86. *Id.*
87. Omnibus Rule.
88. 45 U.S.C. § 1320-5(a).
89. 42 U.S.C. § 1320d-6(a)-(b).
90. *Id.*
91. 31 U.S.C. § 3729(a)-(b).
92. *Id.*
93. 18 U.S.C. § 287.
94. 42 U.S.C. § 1320.
95. 42 U.S.C. § 1320b-6(b).
96. 65 FR 82566.
97. Long Island Health Care Provider Sentenced to 12 Years in Prison for $10 Million Medicare Fraud and HIPAA Identity Theft, Federal Bureau of Investigation, April 10, 2013, http://www.fbi.gov/newyork/press-releases/2013/long-island-health-care-provider-sentenced-to-12-years-in-prison-for-10-million-medicare-fraud-and-hipaa-identity-theft.
98. Former Hospital Employee Sentenced for HIPAA Violations, United States Department of Justice, Feb. 17, 2015, http://www.justice.gov/usao-edtx/pr/former-hospital-employee-sentenced-hipaa-violations.
99. *Id.*
100. Leader of $23 Million Medicare Fraud Conspiracy Sentenced to 10 Years in Prison, United States Department of Justice, April 17, 2015, http://www.justice.gov/usao/iln/pr/chicago/2015/pr0417_02.html.
101. 15 U.S.C. 8404.
102. 15 U.S.C. § 45(a)(1).
103. 13 No. 12 Employer's Guide HIPAA Privacy Requirements News l.
104. 18 U.S.C. § 1028.
105. U.S. Const. art. VI, cl. 2.
106. *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 383, 112 S. Ct. 2031, 2036, 119 L. Ed. 2d 157 (1992).
107. 45 C.F.R. 160.203.
108. 45 C.F.R. 160.203(b).
109. Jennifer Guthrie, Time Is Running Out—The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the "Minimum Necessary" Standard, and the Notice of Privacy Practices, 12 *Annals Health L.* 143, 150 (2003).
110. Stanley C. Ball, Ohio's "Aggressive" Attack on Medical Identity Theft, 24 *J.L. & Health* 111, 131 (2010).
111. *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).
112. 14 No. 1 *Guide Med. Privacy & HIPAA Newsl.* 8. Although standards set forth by the NIST are only directly binding on federal agencies, they are often consulted by organizations as best practices.
113. Safeguarding Health Information: Building Assurance through HIPAA Security, 2014 Webcast, National Institute of Standards and Technology, Sept. 23-24, 2014, http://www.nist.gov/itl/csd/hipaa-2014-webcast.cfm.

114. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
115. N.J. Stat. Ann. § 56:8-163.
116. N.J. Stat. Ann. § 56:8-161.
117. N.J. Admin. Code § 13:45F-5.2 (emphasis added).
118. N.J. Stat. Ann. § 56-8-163.
119. N.J. Stat. Ann. §§ 56:8-196 - 56:8-198.
120. N.J. Stat. Ann. §§ 56:8-197.
121. *Id.*
122. Defined as "any computer system that is designed to allow end users to access computerized information, computer software, computer programs, or computer networks. End user computer system includes, but is not limited to, desktop computers, laptop computers, tablets or other mobile devices, or removable media." N.J. Stat. Ann. §§ 56:8-196.
123. Defined as "any record, recorded or preserved on any computer, computer equipment, computer network, computer program, computer software, or computer system." N.J. Stat. Ann. §§ 56:8-196.
124. N.J. Stat. Ann. §§ 56:8-196.
125. Horizon BCBS notifying 840,000 members after laptops stolen with personal data, *The Star-Ledger*, Dec. 3, 2015, http://www.nj.com/business/index.ssf/2013/12/horizon_bcbs_notifying_840000.html.
126. Elizabeth Snell, Data Breach Lawsuit Against Horizon Denied, *Health IT Security*, April 7, 2015, http://healthitsecurity.com/2015/04/07/data-breach-lawsuit-against-horizon-bcbs-dismissed/.
127. Linn Foster Freedman, Data breach class action suit against Horizon Blue Cross dismissed, *Data Privacy and Security Insider*, April 9, 2015, http://www.dataprivacyandsecurityinsider.com/2015/04/data-breach-class-action-suit-against-horizon-blue-cross-dismissed/.
128. N.J. Stat. Ann. §§ 56:8-1 *et seq.*
129. N.J. Stat. Ann. §§ 56:8-19.
130. P.L. 1960, c. 39, p.137.