HIT News

Summer 2004 (August)
Volume 7
Issue 2

A Publication of the American Health Lawyers Association Health Information and Technology Practice Group

Table of Contents

AMERICAN HEALTH LAWYERS ASSOCIATION

Leading Health Law to Excellence through Education, Information, and Dialogue

Offshore Outsourcing of PHI Processing: Is it Permitted Under HIPAA?[1]

John R. Christiansen, JD
PricewaterhouseCoopers
Seattle, Washington

Offshore outsourcing of technology-related jobs and functions is a controversial subject, and a partisan one in this election year. It is also an important one for many healthcare organizations,[2] for reasons that have nothing to do with politics.

This article does not take a position on the virtues or vices of offshore outsourcing in general. Rather, it reviews the compliance obligations and risks of healthcare organizations that may want to outsource functions involving the use or obtaining of protected health information (PHI) by offshore Business Associates or subcontractors.

Offshore outsourcing raises substantial issues not only of HIPAA compliance but also in some cases of national security. The fundamental question is, what obligations does a Covered Entity or Business Associate have to ensure that an offshore services provider is trustworthy, and that the services provider's host nation has a legal infrastructure that will allow it to enforce the data protection obligations imposed by American law? The short answer is that healthcare organizations probably do have a regulatory obligation of due diligence in these areas, and that in any case it would be prudent to act as if they do.

I. The "Data Haven" and Business Associate Problems

The problem of data "escaping" from legal protections is not a new one. Way back in 1988—almost prehistoric times in the evolution of information technology—science fiction writer Bruce Sterling postulated the development of lawless "data havens."[3] The privacy law equivalent of tax havens, data havens—island nations, perhaps, with small populations and otherwise minimal economic prospects—would refuse to enforce other nations' privacy laws, allowing for "regulatory arbitrage" by organizations or individuals seeking to use or disclose protected information in ways not permitted in most jurisdictions.[4]

> The international nature of data flows limits the ability of any single nation to enforce its data protection laws. . . . [E]ven a highly organized international effort to control data flows could be undermined by a *data haven*—the information equivalent to a tax haven—a single nation that offered to warehouse data.
>
> The existence of a data haven would undermine data protection laws in several ways. It could be used to store information about individuals that was illegal to store elsewhere. The owners, or the clients, could engage in massive "data mining" to cross-index that information. It could either market the data to companies unable to compile the data themselves, or firms located in the data haven could provide services—for example, direct marketing, detailed asset information, or consumer profiles—that companies located elsewhere are forbidden to acquire or provide. . . . [O]nce information leaks or is quietly sold to a data haven, it may be difficult to trace the leak to its source, and it is likely to be impossible to take action against firms located in the haven.[5]

The European Union confronted and tried to solve this problem in developing its own data protection laws, under the European Union Data Protection Directive (EU Directive), which requires all entities to protect personal data.[6] In order to avoid the data leakage problem, the directive prohibits the transfer of protected data from member states to jurisdictions, like the United States, that do not have laws protecting personal data to an equivalent or greater degree.[7] However, the practical need of many multinational organizations to transfer protected data between the United States and Europe led to a somewhat awkward legal work-around. Under

Continued on page 2

Continued from page 1

the "Safe Harbor" rules, organizations in the United States may voluntarily opt-in to a set of data protection obligations that meet European Union requirements, subject to enforcement by the US Federal Trade Commission or other agencies.[8]

HIPAA suffers from the same kind of problem, since as a jurisdictional matter it can only regulate the activities of health plans, healthcare clearinghouses, and healthcare providers that participate in covered electronic claims transactions (i.e., "Covered Entities").[9] Since few if any Covered Entities could operate for long without using services from non-regulated entities involving the use of PHI, whose use and disclosure of PHI could not be directly regulated under HIPAA, the privacy regulations permit Covered Entities to do so only under limited conditions, including in particular a requirement that Covered Entities establish a Business Associate Contract with any entity that obtains or uses PHI on behalf of the Covered Entity. Indirectly, then, the HIPAA regulations protect PHI by requiring Covered Entities to pass along their own data protection obligations.

The HIPAA Business Associate workaround is therefore intended to prevent the "escape" of PHI from non-covered entity "data havens," just as the EU Directive Safe Harbor rules are intended to prevent the "escape" of personal information from organizations operating in nations with less stringent data protection laws. But the Business Associate rules do not address the question of the via bility of this workaround when the enforcement of Business Associate Contracts may be problematic. In considering this issue, it may be useful to clarify what we mean by offshore outsourcing and its risks.

II. Offshore Outsourcing of Healthcare Functions

"Outsourcing" refers to a delegation of responsibility and ownership of functions and resources along a spectrum from traditional, complete ownership to nearly complete divesture by the primary party.

"At a high level, there are four general sourcing options:

- Insourcing—Using internal resources under internal management
- Buy-in—Bringing in external resources to run under in-house control
- Traditional outsourcing—Supplier taking ownership of customer resources and managing those resources on behalf of a customer
- ASP [application services provider]—Renting supplier-owned resources to customers and delivering over the Internet."[10]

Even analysis along this spectrum may be too simplistic, however, since outsourced services providers may themselves further outsource their own infrastructure or functions they have contracted to provide.

> Most customer-supplier relationships in this space are very complicated. A net-sourcing [sic] supplier may have primary accountability to a customer, but hardware, monitoring, billing, help desk, and support services may actually be subcontracted to others. This subcontracting, of course, presents more risks to customers, who may not even be aware of the subcontracting. It also poses more risks to net-sourcing [sic] suppliers, who remain accountable for products and services outside their direct control.[11]

In this context, offshore outsourcing refers to the transfer of functions and activities to organizations in other nations where wages and other costs are expected to be lower. The concept is not new but the process has been considerably facilitated in recent years by the availability of the Internet and the development of data centers and related facilities in nations with sufficient technologically trained personnel to support them.[12] The provision of outsourced services to U.S. companies was pioneered in India, which has high numbers of well-educated, English-speaking professionals, but India's lead is rapidly being followed by other nations in Asia, Eastern Europe, and Central and South America.[13]

While the national security implications of outsourcing some kinds of defense-related functions are beginning to get recognition,[14] privacy issues are also emerging as a focus of potentially serious concern. A few recent incidents have already stimulated some legislative activity, and even in the absence of new legislation raise serious issues for healthcare organizations outsourcing PHI-related services offshore—as well as their potential responsibility for ensuring their onshore services providers do not outsource offshore without appropriate controls.

The same factors that make outsourcing attractive in general can make it appealing to healthcare organizations too, so it is no surprise that many are entering into such arrangements. Clinical transcription services seem to be the leading PHI-related function that healthcare organizations are moving offshore to date,[15] but other functions are following.[16] But unless the kinds of control problems already experienced in the transcription sector can be adequately addressed, the risks of offshore outsourcing may often outweigh the benefits for any PHI-related function.

The most notorious incident to date, and one emblematic of the problems posed by offshore outsourcing, involved the blackmail of the University of California at San Francisco Medical Center (UCSF) by a Pakistani transcriptionist—though based on published information, the transcriptionist herself appears to have been far more ethical and businesslike than some of the Americans involved.[17] Apparently UCSF had contracted for some twenty years with an established California transcription service. This service subcontracted some of its work to a transcriptionist in Florida, who in turn subcontracted with another in Texas,[18] who in turn subcontracted with the Pakistani transcriptionist.

When the Pakistani transcriptionist was not paid for her services, she emailed UCSF a threat to publish patient records on the Internet. UCSF initially had no idea who she was, and it took some sleuthing to trace the chain of relationships that led to the threat. This apparently trig-

gered some payments to the Pakistani transcriptionist, who then retracted her threat. Unfortunately, published information to date does not discuss the terms of the various contracts in this chain, though it appears that the UCSF-transcription service contract may not have permitted offshore subcontracting, and that the transcription service-Florida transcriptionist contract may not have permitted further subcontracting. To date, there appears to be no information about possible legal actions against any of the parties.

Publication of the story about the UCSF incident was quickly followed by publication of a report indicating that an Ohio-based transcription company that routinely outsources to India had also experienced an extortion attempt, in this case by two of its own offshore employees.[19] Another story reported that a computer systems administrator for a major Veterans Administration transcription contractor has alleged that it had services performed offshore, contrary to contract requirements, and that some of the records sent offshore included highly sensitive military information.[20]

Following publication of these stories some legislators have stated their intent to introduce legislation regulating offshore outsourcing of functions potentially involving personal information.[21] Whether or not such legislation is ever passed, existing HIPAA requirements already seem to prohibit healthcare organizations from doing so under some conditions.

III. Risk Management and the Outsourcing of PHI-Related Services

HIPAA expressly contemplates that Covered Entities may outsource PHI-related functions, since by definition, any party to which a Covered Entity outsources a function involving the obtaining or use of PHI on behalf of the Covered Entity is that Covered Entity's Business Associate.[22] It also contemplates that Business Associates may subcontract PHI-related functions, since the Business Associate Contract provisions include a requirement that PHI use and disclosure restrictions be passed on to any subcontractor.[23]

A minimalist interpretation of these provisions might suggest that the only condition to offshore outsourcing of PHI-related functions by a Covered Entity is a Business Associate Contract including the provisions specifically stated in the rule, in the language of the rule. A minimalist interpretation might also suggest that the only condition to offshore subcontracting by a Business Associate is that the subcontract include a use and disclosure limitation provision that mimics the primary Business Associate Contract's use and disclosure provisions. Under this interpretation, neither Covered Entity nor Business Associate would have any duty to assess whether an offshore services provider is trustworthy and has appropriate safeguards to protect PHI, or consider whether its contract is likely to be enforceable against the services provider.

This interpretation would treat the Business Associate Contract provisions as a safe harbor: As long as there is a contract in place that includes the provisions listed in the regulations, there can be no compliance failure. This kind of minimalist interpretation is not the most prudent one, however, and may not be correct.

Under HIPAA Covered Entities have a specific statutory obligation to maintain "reasonable and appropriate administrative safeguards" to protect PHI against "any reasonably anticipated" threats to the security of, or "unauthorized uses or disclosures of" the information,[24] while the privacy regulations require a Covered Entity to "reasonably safeguard [PHI] from any intentional or unintentional use or disclosure" that would violate the privacy regulations.[25]

"Safeguards" means "security measures," and with the publication of the HIPAA security regulations it has become clear—if it was not before—that in order to determine what safeguards are "reasonable," Covered Entities are required to assess their security risks, and implement appropriate measures to manage them.[26] Since the risk assessment is required to be "accurate and thorough,"[27] if the Covered Entity is aware of potential outsourcing risks—including those mentioned in this article—these need to be included when assessing any outsourcing arrangement. If the risk assessment finds that the arrangement creates any "reasonably anticipated threats" of unauthorized disclosure or use of PHI, the Covered Entity will need to implement "reasonable safeguards" that reduce the anticipated threats to a "reasonable and appropriate level."[28]

This does not mean that Covered Entities cannot outsource activities involving PHI offshore. It probably does mean that offshore outsourcing cannot be done without safeguards above and beyond the Business Associate Contract provisions that generally suffice where all entities and activities are located in jurisdictions where the legal system enforces contractual obligations with reasonable certainty and timeliness.

This implies a set of due diligence obligations for Covered Entities outsourcing PHI-related activities offshore.[29] (Note that health plans already have an obligation of due diligence with respect to all services providers, in all states that have adopted the "Standards for Safeguarding Customer Information Model Regulation" published by the National Association of Insurance Commissioners.[30] While the specific obligations will be driven by analysis of the specific risks presented by a specific outsourcing arrangement, as a general rule they should probably include:

- A data criticality analysis[31] that considers whether the PHI involved might include particularly valuable or sensitive data, such as information about care provided to military personnel, demographic data on senior defense or national security personnel, etc.[32]
- A background check (including references) for any provider of PHI-related services, to identify any risk factors arising from past performance (or lack thereof).[33]
- An independent assessment of the services provider's

Continued on page 4

Continued from page 3

administrative, physical, and technical safeguards for the protection of PHI.

- Confirmation of entity status and availability for service of process.
- Determination of the jurisdiction whose laws will apply, and venue for any action to enforce contractual provisions.
- Contractual provisions that specify the services provider's obligations in detail, and a right to audit contractual compliance at the Covered Entity's discretion.[34]
- Establishing an incident response plan for dealing with security and privacy breaches.[35]
- A prohibition on any subcontracting without the Covered Entity's prior approval (preferably at the Covered Entity's discretion). This might be prudent in *any* Business Associate Contract, even with domestic services providers, where there is a risk the Business Associate may outsource to a less trustworthy entity, offshore or otherwise.

Any Business Associate Contract made in contemplation of outsourcing should also have indemnification, limitation of defense, choice of law, jurisdiction and venue, and attorneys fees provisions that protect the Covered Entity in case of any breach, to the greatest extent possible.

IV. Conclusion

Offshore outsourcing may well be a financially appropriate, if politically sensitive solution for many healthcare organizations, and this article should not be taken as a brief for its prohibition. But as seems to be the case so often with information technology solutions, the devil is in the administrative and operational details, and the regulatory compliance and risk management burden may be much more substantial than it seems at first glance. Healthcare organizations should at least exercise greater than ordinary diligence in outsourcing PHI-related functions offshore, and should avoid doing so at all to nations where the enforceability of Business Associate Contracts may be problematic, or to entities that seem less than demonstrably trustworthy.

Endnotes

1 This article assumes that the reader has at least a basic familiarity with the Health Insurance Portability and Accountability Act of 1996 and the privacy and security regulations published pursuant to it (collectively HIPAA in this article).

2 The term "healthcare organizations" is used instead of "Covered Entity" as a category including not only Covered Entities, but also their Business Associates that may subcontract for offshore services. Business Associates may be subject to contractual limitations on their authority to outsource, and even in the absence of such limitations may be severely damaged if their subcontractors misuse PHI. And there are strong indications that the US Department of Justice, which has jurisdiction over criminal penalty prosecutions under HIPAA, will take the position that not only Covered Entities but also Business Associates may be subject to criminal prosecution for its violation. *See* Jana M. Berger, *HIPAA Privacy Rule Continues to Create Confusion*, Midwest In-House (May 25, 2004), available at www.midwestinhouse.com/200404issue/BERGERAPRIL-2004.htm (visited May 25, 2004).

3 *See* Bruce Sterling, *Islands in the Net* (1988):

> . . .Laura had never realized the profit to be gained by evading the developed world's privacy laws. Thousands of legitimate companies maintained dossiers on individuals: employee records, medical histories, credit transactions. In the Net economies, business was impossible without such information. In the legitimate world, companies purged this information periodically, as required by law. But not all of it was purged. Reams of it ended up in the data havens, passed on through bribery of clerks, through taps of datalines, and by outright commercial espionage. . .

The terminology and predicted technologies may be somewhat off, as well as the concept of what privacy laws would actually require—we do not speak of "Net economies" or "datalines," and privacy laws generally don't require routine "purging" of information—but the insight is still valid.

4 *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage* (1996), available at www.law.miami.edu/~froomkin/articles/arbitr.htm#xtocid1583414 (visited Jan. 14, 2003).

5 *Id.*

6 *See* Jane Kaufman Winn and James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 The Business Lawyer 213 (Nov. 2000) at 261–63.

7 *See* Froomkin, *supra* note 4.

8 *See* Winn and Wrathall, *supra* note 6, at 262; *see generally* U.S. Department of Commerce Safe Harbor Overview and related links, available at www.export.gov/safeharbor/sh_overview.html (visited Jan. 14, 2003).

9 *See* John R. Christiansen, *Electronic Health Information: Privacy and Security Compliance under HIPAA* (AHLA 2000) at 16-27.

10 Thomas Kern, Leslie P. Wilcocks, and Mary C. Lacity, *Application Services Provision: Risk Assessment and Mitigation*, 1 MIS Quarterly 113 (June 2002) at 114.

11 *Id.* at 115. The authors use the term "netsourcing" to "capture the variety of service offerings" in which the "distinguishing characteristic is that IT infrastructure, products, and services are delivered over a network."

12 *See e.g.* Tracy Mayor, *Hands Across the Waters*, CIO Magazine (Sept. 15, 2000), available at CIO Magazine Web site, www.cio.com/archive/091500_hands.html (last visited April 8, 2004).

13 *See* Drew Robb, *5 Top Trends in Offshore Outsourcing* (Dec. 17, 2002), available at Datamation Web site, http://itmanagement.earthweb.com/erp/article.php/1558431 (last visited April 8, 2004). A fascinating interactive guide ranking the various nations where outsourced IT services are offered is provided by Stephanie Overby, *A Buyers' Guide to Offshore Outsourcing*, CIO Magazine (Nov. 15, 2002), available at CIO Magazine Web site, http://64.28.79.79/offshoremap/ (last visited April 8, 2004).

14 *See* Stephanie Overby, *How to Safeguard Data in a Dangerous World*, CIO.com Web site (Jan. 15, 2004), available at www.cio.com/archive/011504/outsourcing.html (last visited April 8, 2004).

15 *Medical Transcription Outsourcing Rumbles Along*, Healthcare Informatics Online (Oct. 2003), available at www.healthcare-informatics.com/issues/2003/10_03/trends.htm (last visited April 8, 2004).

16 *See e.g.* Maria Garriga, *U.S. Firms Sending Work to Low Wage Nations* (April 13, 2003), reprinted

from New Haven Register, available at U.S. Congressman Bernie Sanders' Web site, http://bernie.house.gov/documents/articles/20030516154515.asp (last visited April 8, 2004) (indicating insurance company Aetna "hired 350 claims representatives in India and 400 in Ireland").

[17] *See* David Lazarus, *Special Report - Outsourced UCSF Notes Highlight Privacy Risk: How One Offshore Worker Sent Tremor Through Medical System*, San Francisco Chronicle (Mar. 28, 2004), available at www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/03/28/MNGFS3080R264.DTL (last visited April 10, 2004).

[18] According to the article, there are some indications that the Texas transcriptionist may have been a fiction created by the Florida transcriptionist.

[19] *See* David Lazarus, *Extortion Threats to Patient Records – Clients Not Informed of India Staff's Breach*, San Francisco Chronicle (April 2, 2004), available at www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/04/02/MNGI75VIEB1.DTL (visited April 8, 2004).

[20] *See* Bill Fishburne, *Does Bin Laden Have U.S. Army Medical Files?* Asheville Tribune (2004), available at www.ashevilletribune.com/ash1.htm (visited April 10, 2004).

[21] *See* Paul McDougall, *Prove It's Secure–Legislators Want CIOs and Service Providers to Prove that Customer Data Sent Overseas Is as Safe as It Is At Home*, Information Week (Mar. 15, 2004), available at www.informationweek.com/story/showArticle.jhtml?articleID=18400011 (visited April 12, 2004). Senators Clinton and Dayton have introduced the "Safeguarding Americans from Exporting Identification Data Act" (SAFE-ID), S.2471, in Congress, which would require "health care businesses" to give consumers notice and an opportunity to opt-out before certain personally identifiable information is disclosed to "any foreign branch, affiliate, subcontractor, or unaffiliated third party located in a foreign country," and would require that the HIPAA privacy and security regulations be amended to require an outsourcing Covered Entity's notice of privacy practices to provide:

(1) notification that the covered entity outsources protected health information to business associates (as defined under such regulations) for processing outside the United States;

(2) a description of the privacy laws of the country to which the protected health information will be sent;

(3) any additional risks and consequences to the privacy and security of protected health information that arise as a result of the processing of such information in a foreign country;

(4) additional measures the covered entity is taking to protect the protected health information outsourced for processing outside the United States;

(5) notification that the protected health information will not be outsourced outside the United States if the consumer objects; and

(6) a certification that–

(A) the covered entity has taken reasonable steps to identify the locations where protected health information is outsourced by such business associates;

(B) attests to the privacy and security of the protected health information outsourced for processing outside the United States; and

(C) states the reasons for the determination by the covered entity that the privacy and security of such information is maintained.

SAFE-ID § 4. The legislation would also make outsourcing entities liable "to any person suffering damages resulting from the improper storage, duplication, sharing, or other misuse of such information by the transferee." *Id.* at § 3(d).

[22] *See* 45 C.F.R. § 160.103: A "Business Associate" is a person who "with respect to" and "on behalf of" a Covered Entity, performs or assists in the performance of "a function or activity involving the use or disclosure of individually identifiable health information," etc.

[23] *See* 45 C.F.R. §§ 164.314(a)(2)(i)(B), 164.504(e)(2)(D).

[24] *See* 42 U.S.C. § 1320d-2(d)(2)(B).

[25] *See* 45 C.F.R. § 164.530(c).

[26] *See* 45 C.F.R. § 164.308(a)(ii)(A), (B). *See also* 45 C.F.R. § 164.306(b)(2)(iv) (in applying "flexible approach" to security implementation, Covered Entities required to take "probability and criticality of potential risks to electronic [PHI]" into account. The security regulations apply only to PHI in electronic form, *see* 45 C.F.R. §§ 160.103 and 164.302, but effective outsourcing will always require information in electronic form.

[27] 45 C.F.R. § 164.308(a)(ii)(A).

[28] 45 C.F.R. § 164.308(a)(ii)(B).

[29] It has been suggested that HIPAA includes a "chain of trust" concept that "might be interpreted as implying that the transferor and transferee [of PHI] are under an obligation of due diligence to determine the conditions under which data is held prior to transfer and to ensure that the same conditions prevail after the transfer." Winn and Wrathall, *supra* note 6, at 267. This might be a valuable concept, but it is not actually present in HIPAA as enacted. *See* Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Pub.L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996). The proposed HIPAA security regulations published in 1998 included a provision requiring "a chain of trust partner agreement (a contract entered into by two business partners in which the partners agree to electronically exchange data and protect the integrity and confidentiality of the data exchanged)." Proposed 45 C.F.R. § 142.308(a)(2), U.S. Department of Health and Human Services, *Security and Electronic Signature Standards; Proposed Rule*, 63 Fed.Reg. 43263 (Aug. 12, 1998) at 43266. Whether or not this draft provision could be interpreted as suggested, the final form of the security rule does not in any case refer to a "chain of trust," but instead requires that Business Associate Contracts include provisions that require the Business Associate to implement safeguards that will "reasonably and appropriately protect" electronic PHI, ensure that any agents or subcontractors also implement such safeguards, and report security incidents to the Covered Entity, and that authorize termination of the contract for breach by the Business Associate. *See* 45 C.F.R. § 164.314(a)(2).

It is therefore hard to see how a due diligence implication of the suggested type arises from HIPAA or the Business Associate Contract provisions of the security regulations, since there is nothing that implies that the Business Associate has any obligation to determine pre-transfer data protection conditions. Whether or not the Covered Entity has a due diligence obligation to determine post-transfer conditions is a risk management question, as discussed in the text.

[30] *See* National Association of Insurance Commissioners, Standards for Safeguarding Customer Information Model Regulation (2002) at § 8.

[31] *See* 45 C.F.R. § 164.306(b)(2)(iv) (required as part of HIPAA security "flexible approach").

[32] *See supra* note 20.

[33] It might not be unreasonable to include confirmation of financial stability, since PHI may be a valu-

Continued on page 6

Continued from page 5

able asset that a financially strapped entity would be inclined to sell. *Compare* Winn and Wrathall, *supra* note 6, at 226–228 (discussing sales of electronic customer data by bankrupt ecommerce companies).

[34] Jaikumar Vijayan, *Offshore Outsourcing Poses Privacy Perils*, ComputerWorld (Feb. 20, 2004), available at www.computerworld.com/managementtopics/outsourcing/story/0,10801,90343,00.html (visited April 12, 2004) at 2.

[35] *Id.*

The Health Information Law Roller Coaster

Kristen Rosati, Esquire
Coppersmith Gordon Schermer Owens & Nelson PLC
Phoenix, Arizona
Co-editor, HIT News

It's been a wild ride for health information and technology lawyers, and it's getting wilder. Not only have we had to deal with the complicated web of HIPAA privacy regulations, we now need to advise our clients on implementing the HIPAA security standards, offshore outsourcing of functions involving health information, electronic prescribing, the development of electronic health records, and emerging federal law for protecting genetic information, just to mention a few topics.

We hope this newsletter will provide you informative guidance on some of these new and evolving issues. John Christiansen writes on "Offshore Outsourcing of PHI Processing: Is It Permitted Under HIPAA?"; Bruce Fried explains the new e-Health initiatives in "Congress, Administration Off to a Good Start on eHealth: Now What?"; Patricia King outlines the new electronic prescribing requirements in the Medicare Prescription Drug Act; and Kenneth Schuman provides us with a useful crosswalk between HIPAA privacy and security compliance to assist us in advising our clients on security compliance. As always, we also include the Year in Review, compiled by Edward Shay.

Hang on tight for the ride, and feel free to let the HIT Practice Group leadership know how else we can be of assistance in your HIT practice!

Health Information and Technology

Practice Group Leadership 2004-05

Marilyn Lamar
Chair
McDermott Will & Emery
227 West Monroe Street, Suite 56
Chicago, IL 60606-5055
(312) 984-7586 • mlamar@mwe.com

Gordon J. Apple
Vice Chair - Educational Programs
Law Offices of Gordon J. Apple PC
787 Osceola Avenue, Suite 400
Saint Paul, MN 55105-3327
(651) 292-1524 • gapple@healthlawgeek.com

Kristen B. Rosati
Vice Chair - Publications
Coppersmith Gordon Schermer Owens & Nelson PLC
2800 North Central Avenue, Suite 1000
Phoenix, AZ 85004-1007
(602) 381-5464 • kristen@cgson.com

Edward F. Shay
Vice Chair - Research
Post & Schell PC
1800 JFK Blvd, 19th Floor
Philadelphia, PA 19103-7421
(215) 587-1151 • eshay@postschell.com

Robert Q. Wilson
Vice Chair - Membership
The Bogatin Law Firm PLC
1661 International Place Drive, Suite 300
Memphis, TN 38120
(901) 474-6164 • rwilson@bogatin.com

Congress, Administration Off to a Good Start on eHealth: Now What?[1]

Bruce Merlin Fried, Esquire
Sonnenschein Nath & Rosenthal LLP
Washington, DC

A review of congressional activities and Bush administration initiatives in the past few months suggests a growing recognition of the importance of health care information technology, both to achieve improved clinical outcomes and to realize greater operational and financial efficiencies. Yet, for all the activity, the core challenges of capitalizing on an IT infrastructure, removing regulatory barriers to dissemination and carefully preparing for the fiscal consequences of a fully wired health care IT system, remain largely unexplored.

In the Medicare Modernization Act, Congress enacted several important health IT provisions. As part of the new prescription drug program, the law provides a process to create standards for electronic prescribing that physicians and pharmacists can use. The e-prescribing section also provides for the development of a safe harbor in the Stark and Anti-Kickback Acts that would allow hospitals to disseminate technology to physicians, but only when it is used "solely to receive and transmit electronic prescription information." The law also authorizes grants, beginning in fiscal year 2007, for physicians to purchase the necessary technology to implement e-prescribing. Fifty percent cost-sharing is required.

In addition, the law creates a "chronic care improvement program" in traditional fee-for-service Medicare. The program will test disease management strategies and calls for the use of monitoring technologies to exchange clinical information. The program will be phased in gradually beginning in 2005. The second phase, which is due to begin by mid-2008, would move toward national implementation.

The second session of the 108th Congress has been an active one for health-IT related bills. Rep. Nancy Johnson (R-Conn.) has introduced the "National Health Information Infrastructure Act" (H.R. 2915), which calls for the development of an NHII strategic plan.

Sen. Hillary Rodham Clinton (D-N.Y.) introduced the "Health Information for Quality Improvement Act," (S. 2003). Among other things, the bill would establish an NHII office at HHS, require interoperability standards within 12 months, require submission of a NHII strategy to Congress within two years and provide for grants to hospitals and other providers.

Sen. Edward Kennedy (D-Mass.) has proposed the "Health Care Quality Modernization, Cost Reduction and Quality Improvement Act," (S. 2421). The legislation is quite ambitious, not only providing grants, but also establishing a revolving loan fund for IT purchases. It also creates economic incentives beginning in 2005 for providers to use clinical informatics systems and sets economic penalties for providers who do not use such systems beginning in 2010. Kennedy's bill also requires health plans to have an automated adjudication and fraud detection system by 2009.

Sen. Judd Gregg (R-N.H.), chair of the Senate Health, Education, Labor and Pensions Committee, has announced that he will introduce legislation to implement the president's call for electronic health records for all within 10 years.

The White House has been busy as well. Perhaps most significant has been Bush's appointment of Dr. David Brailer as the National Health Information Technology Coordinator. Brailer is charged with creating a national strategy for digitizing the health care system, in particular achieving the president's goal of EHRs within 10 years. Brailer is expected to reveal his plans at HHS' conference: NHII 2004: Cornerstones for Electronic Healthcare, set for July 20-23.

In addition to Brailer's effort, a growing number of federal agencies increasingly are involved in developing, implementing, demonstrating, funding and testing technology in health care. The Defense Department and the Veterans Administration have been building and implementing very sophisticated health IT systems for years. HHS agencies, including the CDC, CMS, AHRQ, the Health Resources and Services Administration and others are conducting demonstration projects, grant programs and other developmental activities.

The momentum at the federal level is obvious, and there is palpable excitement in the health care community. Everyone at the eHealth Initiative's recent Washington, D.C. "Connecting Communities for Better Health" conference was knocked out by the energy, enthusiasm and turnout. Change is coming. Still, the real work remains. Here are a few significant challenges:

- How do we pay for a digitized health care system? We're not just talking about hardware, software and connectivity. There's training for thousands of clinicians and support staff. To fully optimize digital health care we need to re-engineer the entire clinical process. At a recent meeting, a senior official from one of the largest health care systems did a quick estimate of the system's IT costs. The bottom line cost estimate was $250 billion. There are huge savings to be realized, but priming the pump will take real money.
- Getting physicians to buy into the new world of digital medicine is a major challenge. There are all sorts of reasons why docs are reluctant to change. One way to accelerate that transition is to allow hospitals and health plans to distribute key technologies to clinicians. Standing in the way are fraud and abuse laws that were developed in the context of health care as it existed 50 years ago. Recent reforms to fraud laws are of almost no value. Policymakers, both in Congress and the Bush administration, must balance their zeal to stamp out fraud and abuse with an equal zeal to realize and accelerate the clinical and administrative benefits of IT adoption.

While there are many benefits to be realized, let's not forget that they will present new challenges. Better management of chronic illnesses, something that requires an IT strategy, will

Continued on page 8

Continued from page 7

result in fewer acute care needs. That's great for consumers and health plans, but not so great for providers. As the wonders of bio-informatics become real, the ability to determine with precision which drug will work best for which patient may cause a substantial reduction in trial and error drug therapy strategies. Again, it's good for consumers and health plans, but not so good for drug companies, pharmacy benefit managers and pharmacists. We must remember that the health care system is just that, a system. Technology's impact will ripple through all aspects of health care. The sooner we begin to understand those ripples and plan for them, the better.

So, let's celebrate the important work being done by the administration and Congress. But let's remember, the real benefits of a digital health care system are at the end of a long road. Current efforts are laying the foundation for that road. But a good deal of very hard and exciting work remains ahead.

Endnotes

[1] From iHealthBeat, published daily for California HealthCare Foundation by The Advisory Board Company. Subscribe to iHealthBeat at www.iHealthBeat.org

And the winner of the Silver Hippo Award is....

Donald E. Koenig, Jr, Esquire • ***Catholic Healthcare Partners, Cincinnati, Ohio***

One of our facilities welcomed a local celebrity — the noon TV news anchor ("Suzie Anchor") — within a few days of HIPAA taking effect, to deliver her child. At registration, the news anchor chose to opt-out of the patient directory to maximize her privacy, after she was dutifully told by our staff that we would turn away visitors, cards, calls, or flowers that came in her name. She thought that sounded great. Our staff immediately made the proper electronic record notations and swung into action to put the patient's wishes into effect.

Unbeknownst to us, the anchor's husband called her TV station to happily inform them that he was a new father, as his wife had just given birth at the hospital.

At 10:00 am, the news crew swung into action and called our hospital for information. We indicated that we had no information on a patient by that name. At 10:30 am, the news crew called back and asked to be connected to Suzie Anchor's room. Our switchboard indicated that we had no information on a patient by that name. The news crew persisted that they knew she was there, because her husband had told them. We then dutifully replied, "we can neither confirm nor deny the presence of a patient by that name."

At 11:00 am, the news crew called the anchor's husband back – "the hospital won't tell us jack." The husband told the news crew her room number. The news crew called back at 11:30 am and asked to be connected to the room number. The switchboard noticed that the room number corresponds to an opt-out patient and declined to connect the call. The news crew called back at 11:40 and identified itself as the local TV station news team. Call is transferred to the Director of Communications.

The whole litany is repeated, including the news station begging "we're close to news deadline and want to share the happy news with all the folks in Anytown on the noon news."

The Communications Director checked the patient directory and politely explained that due to HIPAA, we have to honor the requests of all our patients to protect their privacy and we, therefore, could not confirm or deny the presence of a patient by the name they were seeking.

The news came on at 12:00 noon and Suzie Anchor was watching her station on the TV in her hospital room. The news anchor announced that their regular anchor has had her baby at the hospital but they are unable to confirm any information and have not been able to speak to her. The anchor intoned in a serious voice: "Here are the only baby photos we have been able to obtain." The station then broadcasts the file footage of Michael Jackson dangling his child over the balcony railing in Paris. Everyone on the news set was laughing.

Our patient was surprised and hurriedly called the news station, inviting them up to interview her and giving them the room number.

The patient did not tell anyone at the hospital that she invited the local news crew to come into the hospital to film her. The news van pulled up 15 minutes later in front of the hospital with news crew and camera team broadcasting and they began to walk in the front door. They were stopped by the facility officials and asked about their filming. The news team explained they were on the way to Suzie Anchor's room to film her and her new baby. Hospital staff checked the patient directory, informed them "we have no such patient by that name here." The news crew was getting cranky. The Hospital reception staff also called the Director of Communications, who immediately came down to speak with the media. She told the crew to wait and called the patient, who confirmed that she wanted them to interview her, and gladly rescinds her opt-out decision orally over the phone.

The interview with the anchor and film of the new baby makes the 6:00 pm news that night. Ultimately, we had a good laugh, but were justifiably pleased that our staff took patient privacy seriously, even though we were way behind the patient and the patient's family member's actions that were inconsistent with such tight protection.

The eHealth Initiative's Report on Electronic Prescribing: The Message for HIT Lawyers

Patricia D. King, Esquire
Law Office of Patricia D. King
Chicago, Illinois

On April 14, 2004, after a year's effort by a diverse group of national experts, the eHealth Initiative issued its formal report on recommendations for electronic prescribing.[1] Entitled "Electronic Prescribing: Toward Maximum Value and Rapid Adoption," the report strongly urges rapid adoption of electronic prescribing, citing advantages both for reducing medical errors and for realizing cost savings. The report includes detailed recommendations for design of electronic prescribing systems and implementation of such systems in the ambulatory care setting. While written primarily from the standpoint of physician practices implementing electronic prescribing, the eHealth Initiative also concludes that the greatest potential benefit is realized when the electronic prescribing component in the physician's office is one part of a complete electronic medical record that can interface with eligibility, benefit and formulary databases of payors, and pharmacy computer systems. The eHealth Initiative challenges physician practices considering implementation of electronic prescribing to view this as a first step toward a complete electronic medical record.

The report offers much of interest to developers of e-prescription systems and their customers, including a list of recommended and desired electronic prescribing system components. It identifies five key aspects of electronic prescribing,[2] describes each with a high degree of specific detail, and concludes with thoughtful recommendations.

From a lawyer's standpoint, other noteworthy aspects of the report are the observations concerning barriers raised by current regulations to implementing electronic prescribing; discussion of upcoming requirements for electronic prescribing standards in the Medicare Prescription Drug, Improvement, and Modernization Act of 2003[3] (MMA); initiatives in proposed legislation toward enhancing interoperability of healthcare information technology systems; and the evaluation of potential incentives for implementation.

I. The Current Regulatory Environment Hinders Development of E-Prescribing

The report notes that state pharmacy regulators lack a uniform approach to electronic prescribing, and have varying requirements for the format of printed prescriptions. While state regulations largely address the same substantive requirements, "[t]he *NAPB Survey of Pharmacy Law* that describes all of these variations contains nearly 100 pages of dense tables illustrating the various state requirements."[4] Consequently, software for e-prescribing must have flexibility to incorporate variations for the state where the purchaser operates—and attorneys advising clinics that are contemplating purchase of e-prescribing systems must assure that local regulatory requirements are met.

The MMA provides that federal standards established for electronic prescribing will supersede contrary state law that "pertains to the electronic transmission of medication history and information on eligibility, benefits, and prescriptions with respect to covered part D drugs under this part."[5] It is not clear whether state requirements that pertain not to electronic transmission, but rather to the required content of a prescription, would be superseded.

II. Requirements for Electronic Prescribing

Appendix B to the report contains an overview of federal legislation dealing with information technology and health system improvement, including an in-depth discussion of the MMA. The MMA calls for establishment of an electronic prescription program, which will include:

- Electronic transmittal of the following to the prescribing healthcare professional and the pharmacist:
  a. The prescription;
  b. Information on eligibility and benefits (including the drugs included in the applicable formulary, any tiered formulary structure, and any requirements for authorization); and
  c. With respect to a drug covered under the Medicare prescription drug benefit, information on the drug being prescribed and other drugs listed on the patient's medication history (including information on drug interactions, warnings or cautions, and dosage adjustments as indicated), and information on the availability of lower cost, therapeutically appropriate alternatives for the drug prescribed.[6]
- Electronic transmittal of the medical history of the patient relating to the drug being prescribed or dispensed, on request of the prescribing healthcare professional or pharmacist.[7]

Information may be disclosed only as permitted under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Standards.[8]

To the extent feasible, information is to be exchanged on an interactive, real-time basis. The joint explanatory statement on the MMA notes, however, that "[t]he conferees do not intend for the provision relating to 'interactive, real-time' transmission of information to preclude an individual or entity from complying with the standards under this part by virtue of such individual's or entity's inability to transmit information on an interactive, real-time basis."[9]

The MMA requires that uniform standards be developed for electronic transmission of prescriptions. Providers who continue to use paper to prescribe will not be required to convert to electronic prescribing, but pharmacies and providers that do use electronic means to prescribe and fill prescriptions for drugs covered under Medicare Part D must comply. The National Committee on Vital and Health Statistics (NCVHS) will provide recommendations for the standards.[10] The objectives for the electronic prescribing standards are to improve patient safety and the quality of patient care,

Continued on page 10

Continued from page 9

and to encourage efficiencies, including cost savings in the delivery of care.[11] Also, the standards should be designed to avoid imposing an undue administrative burden on prescribing healthcare professionals and pharmacists; to be compatible with the HIPAA Administrative Simplification standards and general health information technology standards; and to permit electronic exchange of drug labeling and drug listing information maintained by the Food and Drug Administration and the National Library of Medicine.[12] The standards must allow for messaging of information about appropriate prescribing of drugs, and permit a beneficiary under a Medicare prescription drug benefit plan to designate the pharmacy to dispense the prescribed drug (to the extent consistent with the plan).[13]

The MMA sets an aggressive timetable for the development of uniform electronic prescribing standards: initial uniform standards for e-prescribing not later than September 1, 2005; a one-year pilot project starting January 1, 2006; and final standards by April 1, 2008.[14] On August 3, 2004, the Centers for Medicare and Medicaid Services (CMS) published proposed rules for the establishment of the Medicare Prescription Drug Benefit Program[15] and the Medicare Advantage Program.[16] These proposed rules do not contain the initial standards for e-prescribing. CMS explains that the MMA directs the NCVHS to gather information on and formulate recommendations for e-prescribing, and the NCVHS has already held public hearings for this purpose. The proposed regulations do require Prescription Drug Plan (PDP) sponsors and Medicare Advantage (MA) organizations to comply with the final standards for electronic prescribing when they are in effect.[17]

Section 1012 of the MMA establishes the Commission on Systemic Interoperability, whose members are to be appointed by the President and Congress. The Commission has the mandate to develop a comprehensive strategy for adoption and implementation of healthcare information technology standards, and is to submit a report by October 31, 2005.[18]

A number of pending bills encourage adoption of healthcare information technology systems to reduce medication errors and otherwise improve quality.[19] With the appointment of Dr. Brailer as the National Health Information Technology Coordinator, the momentum is building for industry-wide efforts to modernize the healthcare system's antiquated paper-based information system.

III. Potential Incentives for Adoption of Electronic Prescribing

The eHealth Initiative predicts substantial benefits from e-prescribing for all stakeholders: for patients, through reduction in medical errors and improved management of therapy; for pharmacies, through increased efficiency; for payors, through cost savings due to increased formulary adherence and better management of chronic disease; and potentially for researchers, through the aggregation of large databases of clinical information. However, the cost in time and lost productivity is borne disproportionately by clinicians, who have to raise the capital to buy electronic prescribing systems, devote time of staff and clinicians to training, and likely endure decreases in productivity during implementation.

The report comments on various methods of creating incentives for physicians to implement electronic prescribing. First, the report notes that the MMA establishes a safe harbor from penalties under the Medicare Anti-Kickback Statute, and a safe harbor under Stark II for certain group practices, hospitals, and plans. The safe harbor applies only to nonmonetary remuneration, in the form of hardware, software, or information technology and training that is *necessary and used solely* to receive and transmit electronic prescriptions. The safe harbor would permit a hospital to offer information technology support to members of its medical staff; a group practice to offer such support to its members; and an Medicare Advantage (MA) organization or Prescription Drug Plan (PDP) sponsor to support pharmacies participating in their networks, and prescribing healthcare professionals.[20] Since MA organizations and PDP sponsors will be likely to realize cost savings from encouraging electronic prescribing (e.g., through enhancing formulary compliance), the safe harbor may be of most benefit to these groups.[21]

The MMA also authorizes the Department of Health and Human Services (DHHS) to make grants to physicians (with a 50% matching requirement) to cover the cost of devices, software, and training to implement electronic prescribing.[22] Finally, the MMA calls upon DHHS to establish a pay-for-performance demonstration program at four sites, in which physicians who agree to meet practice standards requirements for healthcare information technology would be eligible to receive a per-beneficiary payment if the physician meets performance standards for clinical quality and outcome.[23] This incentive is not limited to electronic prescribing, but rather is intended to encourage the use of email communication and other information technology to help coordinate care for Medicare beneficiaries with chronic conditions.

CMS's proposed rules for the Medicare Prescription Drug Benefit Program and the Medicare Advantage Program provide that an MA organization (but not a PDP sponsor) may offer differential payments to physicians to encourage use of e-prescribing.[24] MA organizations need not await the final e-prescribing standards, but could implement these incentives as early as January 1, 2006 under the voluntary standards. The preamble notes that differential payments could take into consideration the physician's cost of implementing e-prescribing, and could be increased to encourage:

- Formulary compliance where medically appropriate;
- Use of lower cost, therapeutically equivalent alternatives;
- Reductions in adverse drug interactions through appropriate use of drug interaction checking functions in the e-prescribing system; and
- Reduced administrative cost in filling and refilling prescriptions.[25]

CMS notes, however, that incentives must be in compliance with the Stark self-referral prohibition and the anti-kickback laws, and solicits comments on the application of these laws.[26]

The eHealth Initiative comments that third-party payors other than Medicare, and possibly employer groups, may adopt pay-for-performance plans to encourage use of health information technology, especially to improve management of chronic diseases. The report also speculates that if it can be demonstrated that electronic prescribing lowers malpractice costs, malpractice insurers may offer reductions to insureds who implement such systems.

IV. Conclusion

The eHealth Initiative report is a thoroughly documented case study of how to move from our current fragmented, paper-based system to an integrated electronic one, in the target area of electronic prescribing. As the eHealth Initiative asserts, the benefits of e-prescribing, while substantial on a freestanding basis, are multiplied when this function is one aspect of an integrated electronic medical record that crosses the continuum of care.

Endnotes

1 *Electronic Prescribing: Toward Maximum Value and Rapid Adoption*, a report of the Electronic Prescribing Initiative, 2004. The report can be found at www.ehealthinitiative.org/initiatives/erx/.

2 The aspects of e-prescribing identified are: usability; clinical design support, including formulary management; communication; vocabulary and standards; and implementation.

3 Pub. L. No. 108-173.

4 *Electronic Prescribing, supra* note 1, at p. 86.

5 Pub. L. No. 108-173, Sec. 101, creating Social Security Act Title XVIII, Sec. 1860D-4(e)(5); 117 Stat. 2090.

6 The joint explanatory statement on the MPDA describes the intent of this provision as allowing "for prescribing health care professionals to have ready access to neutral and unbiased information on the full range of covered outpatient drugs available." Joint explanatory statement on H.R. 1, p. 27 (available at http://waysandmeans.house.gov/media/pdf/hr1/hr1jexplstate.pdf).

7 Sec. 1860D-4(e)(2).

8 Since the disclosure of the information will be for treatment purposes, there should be no conflict between the electronic prescription program and the HIPAA Privacy Standards.

9 Joint explanatory statement, *supra* note 6, p. 27.

10 Sec. 1860D-4(e)(4)(B).

11 Sec. 1860D-4(e)(3)(A).

12 Sec. 1860D-4(e)(3)(C).

13 Sec. 1860D-4(e)(3)(D), (E).

14 Sec. 1860D-4(e)(1), (4).

5 69 Fed. Reg. 46631 (Aug. 3, 2004).

16 69 Fed. Reg. 46865 (Aug. 3, 2004).

17 42 C.F.R. § 423.159(a), at 69 Fed. Reg. 46821.

18 Pub. L. No. 108-173, Sec. 1012(a)(4).

19 The National Health Information Infrastructure Act, H.R. 2915, calls for development of a national health information infrastructure strategic plan, including developing recommendations to disseminate best practices in healthcare information technology. That bill was referred to the Subcommittee on Health on August 8, 2003. In the Senate, Senator Clinton introduced the Health Information for Quality Improvement Act, S. 2003, on December 9, 2003.

20 Sec. 1860D-4(e)(6).

21 The recently published Stark II interim final rule contained an exception for providing items or services of information technology to a physician to facilitate electronic health records as part of a community-wide health information system. *Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships (Phase II); Interim Final Rule,* 69 Fed. Reg. 16054 at 16142 (Mar. 26, 2004). Because this safe harbor applies only to community-wide health information systems that are available to all providers in the community, its applicability will be limited to those communities experimenting with community-wide systems.

22 Pub. L. No. 108-173, Sec. 108.

23 Pub. L. No. 108-173, Sec. 649.

24 42 C.F.R. § 423.159(b), at 69 Fed. Reg. 46821.

25 69 Fed. Reg. 46672.

26 As described above, the MMA provides for additional safe harbors to encourage electronic prescribing. However, since the mandated new safe harbors cover nonmonetary incentives only, they would not apply to the payment differentials contemplated by CMS.

AMERICAN HEALTH LAWYERS ASSOCIATION

1025 Connecticut Ave, NW
Suite 600
Washington, DC 20036-5405
202-833-1100
202-833-1105 Fax

www.healthlawyers.org

PRACTICE GROUPS STAFF

Wayne Miller, CAE
Deputy Executive Vice President/COO
(202) 833-0775
wmiller@healthlawyers.org

Eileen M. Bantel
Associate Director of Practice Groups
(865) 458-0643
ebantel@healthlawyers.org

Laurie Garvey
Practice Groups Administrator
(202) 833-0783
lgarvey@healthlawyers.org

Sarah Muenzenmayer
Practice Groups Assistant
(202) 833-0765
smuenzenmayer@healthlawyers.org

Reconciling HIPAA Privacy and Security Compliance—A Brief Road Map Toward Security Rule Compliance

Kenneth Schuman, Esquire
Delta Dental Plans of Michigan, Ohio, and Indiana
Lansing, Michigan

I. Introduction

It might only seem like yesterday since health lawyers counseled healthcare organization[1] clients through the rigors of complying with the Health Insur-ance Portability and Account-ability Act (HIPAA) Privacy Rule[2] (Privacy Rule). However, instead of being able to sit back, relax, take a deep breath, and reflect on the fond memories of the Privacy Rule compliance road trip, it's time to pack up and head out on the road again for another compliance road trip. This time the destination is . . . the HIPAA Security Rule[3] (Security Rule). Fear not. This article will provide you with some valuable information and guidance for your road trip. In particular, this article will attempt to provide some reconciliation between the Privacy Rule compliance healthcare organizations have already completed with the Security Rule compliance journey it is about to embark on. Then, the article will provide a general road map toward Security Rule compliance.

II. Privacy Rule vs. Security Rule: Differences and Overlaps

Differences. Generally speaking, there are two major differences between the Standards within the Privacy Rule and the Security Rule. First, the Security Rule focuses on safeguarding electronic protected health information[4] (EPHI) from unauthorized access, modifications, deletions, and transmissions; whereas, the Privacy Rule focuses on managing uses and disclosures of protected health information and individual rights regarding protected health information. Second, as indicated above, the Security Rule is much more narrow in scope than the Privacy Rule in that it applies only to protected health information in electronic form and the Privacy Rule applies to protected health information[5] in any form.

Overlaps. The following are some examples of overlap in the policies and procedures that healthcare organizations developed to address the Privacy Rule and the policies and procedures that will be developed to address the Security Rule. Bear in mind that by and large, the Security Rule is designed to work with the Privacy Rule. The steps taken to comply with one Rule should promote compliance with the other Rule. But as you will notice each Rule has a slightly different focus.

- *Security Risk Assessment vs. Privacy Gap Analysis*. For complying with the Security Rule, a healthcare organization will be focusing on assessing its information systems when developing administrative, physical, and technical safeguards to protect EPHI.[6] For the Privacy Rule, a healthcare organization had to assess its entire organization.
- *Security Officer vs. Privacy Officer*. Similar to the Privacy Rule, a healthcare organization has to identify a Security Officer who is responsible for the development and implementation of the healthcare organization's security policies and procedures and the overall responsibility for the security of the EPHI.[7] The Security Officer can also be the Privacy Officer.[8] However, just like for the Privacy Officer, the Security Officer should be someone in the healthcare organization with higher-level decision-making authority.
- *Training*. Similar to the polices and procedures that address the Privacy Standards, employees, including management, must be trained on the healthcare organization's Security Rule policies and procedures.[9] The Security Rule suggests that training can be incorporated with Privacy Rule training and it can possibly be accomplished during employee orientation.[10]
- *Employee Sanctions*. A healthcare organization now has to develop a policy and procedure that will apply appropriate sanctions against employees who fail to comply with both its Security Rule and Privacy Rule policies and procedures.[11]
- *Documentation Requirements*. A healthcare organization has to maintain its policies and procedures in written or electronic form and a written record of any action required to be documented under the Security Rule.[12]
- *Hybrid Entity*. As a reminder, a hybrid entity is a healthcare organization whose business activities include both covered and non-covered functions and designates the covered functions as healthcare components so that only the healthcare components had to comply with the Privacy Rule.[13] Similar to the Privacy Rule, a healthcare organization's designated healthcare components must comply with the Security Rule, and protect against unauthorized access to EPHI with respect to the other components of the healthcare organization.[14]
- *Affiliated Covered Entities*. Similar to the Privacy Rule, legally separate healthcare organizations that are affiliated with each other can designate themselves as a single affiliated covered entity for compliance purposes.[15]
- *Business Associate Agreements*. The Security Rule requires additional provisions to be added to the Business Associate Agreements[16] if the Business Associate[17] will have access to EPHI. If the Business Associate will be handling EPHI for the healthcare organization, the Business Associate Agreement should have a provision in the Agreement that the Business Associate will implement administrative, physical, and technical safeguards to safeguard the confidentiality, integrity, and availability of EPHI that it creates, receives, or maintains on behalf of the healthcare organization.[18] In addition, there should be a provision in the Business Associate Agreement requiring the Business Associate to report any "security incident" of which it becomes aware.[19] A security incident is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[20]

This would arguably include any suspected misuse of data.[21]

- *Group Health Plan Documents*. Similar to the Privacy Rule, if EPHI other than enrollment and disenrollment information or summary health information[22] for purposes described in the Privacy Rule, or as authorized by a Privacy Rule authorization, will be disclosed to the plan sponsor by the group health plan[23] or the health insurance issuer/ health maintenance organization[24] with respect to the group health plan, the plan documents should be amended. The amendments should focus on the group health plan ensuring that the plan sponsor will reasonably and appropriately safeguard EPHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.[25]

III. A Brief Road Map Toward Compliance

Now that you understand the path your healthcare organization client had to take to reach its Privacy Rule compliance destination, here is a roadmap to aid your client as it travels toward its new destination . . . Security Rule compliance. Please keep in mind that the following information is geared more toward larger healthcare organizations. Of course, a relatively small healthcare organization (e.g., a solo provider office with a couple of employees) will more than likely not have to take their compliance efforts to these levels. However, the following information should still provide some general guidance for these healthcare organizations on the road trip toward Security Rule compliance.

- *Understanding the Security Rule*. Of course, as with any compliance effort, it is essential that someone within the healthcare organization have a thorough understanding of the Security Rule. This more than likely will fall on the shoulders of in-house counsel and/or other compliance leaders within the healthcare organization.
- *Develop a Compliance Team*. This team should be made of a cross-section of employees from appropriate departments. The "appropriate departments" are healthcare organization specific, but more than likely they will include employees from information systems and services, corporate audit, corporate communications, human resources, and legal. The Compliance Team should have some input on selecting the Security Officer.
- *Security Gap Assessment*. With a through understanding of the Security Rule and the Compliance Team in place, the next logical step is to have the Compliance Team conduct a thorough gap assessment of its information system. An information system normally includes hardware, software, information, data, applications, communications, and human resources (e.g., people). Generally speaking, the first step in a security gap assessment will involve identifying electronic media that maintain or transmit EPHI and evaluating how current computer policies and procedures address EPHI. For larger healthcare organizations, this can possibly be accomplished by having your Security Officer send a questionnaire via email to department heads requesting that they capture all EPHI that is stored and/or transmitted in their department. The email should be easy to complete. Perhaps this can also be accomplished by, and/or in conjunction with, face-to-face meetings between department heads and the Compliance Team. Email is of course preferable because it would be easier to document. The gap assessment should also include a review of any sort of health data sharing arrangement in terms of affiliated covered entities, hybrid entities, and group health plans. In addition, the gap assessment should involve a review of Business Associate Agreements to see if they need any sort of modification to incorporate provisions addressing EPHI.
- *Gap Analysis*. The gap analysis should begin as the gap assessment is being performed, in that as the Compliance Team starts to receive feedback from the questionnaire, they should start to identify areas in the information system with deficient security controls and weaknesses against the Security Standards. Once the security weaknesses have been identified and documented, the Compliance Team should document how they can be addressed in relation to the Security Standards. For example, if computer sessions are terminated after a lengthy period of inactivity, the healthcare organization should consider if it is reasonable, within its corporate environment, to develop a mechanism and procedure to terminate the electronic session after a shorter period of time. In addition, the recently published "An Introductory Resource Guide for Imple-menting the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" by the National Institute of Standards and Technology provides a great deal of useful information for guiding a healthcare organization through its gap assessment and gap analysis.[26]
- *Training*. Once the policies and procedures have been documented in written or electronic form, the Compliance Team needs to develop a strategy for having the healthcare organization's current employees and management trained on them by the compliance date. Also, a strategy needs to be formulated for training employees after the compliance date.
- *Continual Assessment*. The Security Rule indicates that a healthcare organization has a duty of continual assessment. To comply with this duty, the Com-pliance Team should establish a procedure for periodically performing security evaluations of the healthcare organization's information systems, which would include both internal and external audits. Having the Compliance Team periodically review the healthcare organization's Security Rule polices and procedures to see if they need any refinement will also help the healthcare organization comply with the continual assessment duty.

Continued on page 14

Continued from page 13

IV. Attorney-Client Privilege for Security Rule Compliance Efforts

The gap assessment might reveal sensitive corporate information in regard to information systems. Therefore, it is essential to have legal counsel involved as early as possible to enable any gap assessment communications to be protected under attorney-client privilege. The attorney-client privilege can be very important to your entire Security Rule compliance efforts by making it possible to investigate potential legal liabilities that may otherwise become undetected (e.g., a privileged audit of computer security risks). In essence, the attorney-client privilege protects a communication between a licensed attorney and an individual or corporate client. While the communication is protected, the underlying facts are not. Also, the attorney must be acting as a lawyer, not as a business advisor of some sort. In addition, the communication must be made in confidence and for the purpose of receiving legal advice.

The corporate attorney-client privilege only protects the corporation, not its employees, officers, or directors. On the other hand, since the company can only act through individuals, the issue then becomes which corporate communications are privileged. *Upjohn v. United States*[27] is the definitive case for providing guidance on this issue. In *Upjohn*, the U.S. Supreme Court held that communications with low level employees, as well as with officers and directors, could be protected, provided: (1) the communication was made at the direction of corporate officials to obtain legal advice; (2) the matters communicated fell within the scope of the employee's duties and were not available from upper level employees; (3) employees were aware that the purpose of the inquiry was to help in obtaining legal advice; and (4) the communications were intended to be kept confidential.[28]

In order for a gap assessment communication to qualify for the attorney-client privilege, and to prevent the attorney-client privilege from being inadvertently waived, there must be an initial intention to keep the communication confidential. Therefore, the communication should not be disclosed to third parties (e.g., auditors, public officials, vendors). Also, if the communication is oral, it should be commenced outside the presence of third parties. In addition, when circulated internally, the communication should be limited to employees on a "need to know" basis. Of course, it makes good practical sense to label any documents associated with Security Rule compliance efforts "Confidential, Attorney–Client Privilege" to avoid putting them in your organization's company files that are easily accessible.

V. Conclusion

I am sure most healthcare organizations are not thinking like Willie Nelson in that they "just can't wait to get on the road again"[29] in terms of Security Rule compliance. Nevertheless, it is extremely important not to delay this road trip. The compliance date for covered entities, except for small health plans, is April 21, 2005.[30] Even worse than receiving a penalty from the Department of Health and Human Services for non-compliance, would be the bad press associated with a security breach. In the mean time, there is lot of work to be done. However, the work that has already been accomplished by a healthcare organization in reaching its previous destination, Privacy Rule compliance, should help tremendously in enabling the healthcare organization to reach its brand new destination . . . Security Rule compliance.

Endnotes

1 "Healthcare organization" refers to an organization with one or more healthcare providers considered to be a covered entity [as defined in 45 C.F.R. § 160.103] required to comply with the Administrative Simplification portions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

2 45 C.F.R. pts. 160 and 164.

3 45 C.F.R. pts. 160 and 164.

4 45 C.F.R. § 160.103 (defining *electronic protected health information*).

5 45 C.F.R. § 160.103 (defining *protected health information*).

6 As defined in 45 C.F.R. § 164.304, an "*Information system*" means an interconnected set of information resources under the same direct management control that shares a common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

7 45 C.F.R. § 164.308(a)(2).

8 68 Fed. Reg. 8347 (Feb. 20, 2003).

9 45 C.F.R. § 164.308 (a)(5).

10 68 Fed. Reg. 8350 (Feb. 20, 2003).

11 45 C.F.R. § 164.308(a)(1)(ii)(c).

12 45 C.F.R. § 164.316(b)(1).

13 45 C.F.R. § 164.103 (defining *hybrid entity*).

14 45 C.F.R. § 164.105(a).

15 45 C.F.R. § 164.105(b).

16 A "Business Associate Agreement" is an agreement between a covered entity [as defined in 45 C.F.R. § 160.103] and a business associate [as defined in 45 C.F.R. § 160.103] in which a business associate provides satisfactory assurances to a covered entity that it will appropriately safeguard protected health information [as defined in 45 C.F.R. § 160.103] it creates, receives, or maintains on behalf of the covered entity. 45 C.F.R. § 164.504(e)(1) provides the minimum requirements for a business associate agreement.

17 45 C.F.R. § 160.103 (defining *business associate*).

18 45 C.F.R. § 164.314(a).

19 *Id.*

20 45 C.F.R. § 164.304 (defining *security incident*).

21 68 Fed. Reg. 8351 (Feb. 20, 2003).

22 45 C.F.R. § 164.504(a) (defining *summary health information*).

23 45 C.F.R. § 160.103 (defining *group health plan*).

24 *Id.* (defining *health insurance issuer* and *health maintenance organization*).

25 45 C.F.R. § 164.314(b).

26 "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) of 1996," National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, NIST Special Publication 800-66.

27 *Upjohn Co.* v. *United States,* 449 U.S. 383 (1981).

28 *Id.*

29 "*On the Road Again*" words and music by Willie Nelson, Willie Nelson Music Incorporated, 1979.

30 45 C.F.R. § 164.318

Chair Report: *Riding the Health Information Technology Tidal Wave*

Marilyn Lamar, Esquire
McDermott Will & Emery LLP
Chicago, Illinois

Health information technology continues to attract high-level attention in Washington, with a renewed focus on its potential for increasing patient safety and cost savings. Legal issues are also receiving fresh consideration as government and industry try to increase the adoption rate.

The HIT Practice Group is committed to providing its members timely information on what many expect will become a tidal wave of HIPAA–like proportions. In addition to the usual high caliber legal analysis from AHLA members, we plan to focus on practical advice and negotiating strategies for the contracts our clients will enter into for additional technology. Our activities in the 2004-05 year will include ongoing listserve discussions, teleconferences and publications, as well as a "think tank" to be held in Chicago (details below).

As background, most of you are aware this spring the Bush administration increased its focus on health information technology with the stated goal of having electronic health records (EHR) available for most Americans within the next ten years. Early steps in this initiative included the appointment of Dr. David Brailer to the new position of National Health Information Technology Coordinator. On July 21, 2004, Dr. Brailer issued an overall framework for strategic action to promote health information technology, with further activity expected in the fall.

The Government Accountability Office (GAO) has now weighed in with a Congressional briefing dated August 13, 2004 regarding DHHS's efforts to promote health information technology and legal barriers to its adoption. (The GAO report is available on its website at *www.gao.gov*.) The report identified six legal issues (in addition to privacy and security) that present barriers to the adoption of health information technology: (1) fraud and abuse, (2) antitrust, (3) tax, (4) intellectual property, (5) malpractice and (6) state licensing. The GAO indicated that DHHS efforts to address some of these barriers have not been sufficient and that other federal agencies have not acted to reduce these barriers.

As one of our activities in response to these developments, the HIT Practice Group is sponsoring a "think tank" for advanced practitioners in Chicago on November 11-12. This meeting will be held prior to the HIT Practice Group lunch on November 12. The discussion will focus on the policy and legal implications of the Electronic Health Record initiative and the development of the National Health Information Infrastructure (NHII). This "think tank" and networking opportunity is designed to be an interactive discussion for experienced practitioners in the health information and technology field. Participants will discuss cutting-edge issues related to the EHR initiative and the NHII, including:

- the standardization of electronic health record development: the standards setting process, and how HIT lawyers might contribute to these efforts
- potential legal barriers and issues in developing and using shared electronic health record systems: fraud and abuse/Stark, malpractice, privacy/security, antitrust concerns, and others
- practical contracting issues related to shared electronic health record systems

Representatives from EHR standards-setting organizations and key government officials involved in the NHII will be invited to participate, providing a unique opportunity to hear from policymakers and provide them with additional information to consider when developing the EHR and NHII.

To facilitate an advanced and interactive discussion, moderators will provide background materials on an important EHR or NHII topic, introduce that topic, and facilitate a problem-solving discussion among the participants. Due to the think tank, round-table format, enrollment will be limited to 40 people who are members of both the AHLA and its HIT Practice Group, and who have been practicing health information and technology law for a minimum of five years or have other substantial experience with health information technology.

For those members of the HIT Practice Group who cannot attend, we expect this will result in practical guidance that will be shared with the entire HIT Practice Group through teleconferences, publication of the outcome of the discussions, the drafting of detailed member briefings, or similar materials.

The sessions will begin on Thursday, November 11th and will end just before the annual HIT Practice Group luncheon at the Fundamentals Program on Friday, November 12th. The "think tank" has been structured to keep the cost of attendance at a minimum and we are pleased to offer this educational and networking opportunity to HIT Practice Group members for only $295. Watch your email and the Health Lawyers' web site for more details. Attendance will be limited to facilitate discussion, so if you are interested, please register on-line as soon as it is available.

I would like to thank Gordon Apple, Kristen Rosati, and Robyn Meinhardt for co-chairing the "think tank". I would also like to extend a warm welcome to Robert Q. Wilson, who joins Gordon, Kristen, and Ed Shay as Vice Chairs of the HIT Practice Group for the 2004-05 year. Finally, I would also like to express my appreciation to Alan Goldberg, who continues as the wonderful Moderator of our listserve. We all benefit from the enormous energy that these talented lawyers bring to HIT activities and publications.

We look forward to seeing many of you in Chicago and to having you join us electronically throughout the year. If you have any thoughts or questions about HIT Practice Group activities throughout the year, please feel free to contact me at mlamar@mwe.com.

Year-in-Review 2003-2004

Edward F. Shay, Esquire
Post & Schell PC
Philadelphia, Pennsylvania

Progress on Electronic Health Records

On July 1, 2003, the College of American Pathologists announced that it had signed a $32.4 million, five-year sole source contract with the National Library of Medicine (NLM) to license English and Spanish language editions of SNOMED Clinical Terms®. The agreement is of major significance for three reasons. First, SNOMED's uniform terminology is believed to be fundamental to developing a standardized electronic health record. Second, the agreement is widely perceived as an outgrowth of the President's support for an improved healthcare information infrastructure. Third, the agreement demonstrates the role the government can play in both adopting and disseminating standards for the development of healthcare information infrastructure.

Starting in January, 2004, free-of-charge access to SNOMED CT core content and all version updates will be available through the NLM's Unified Medical Language System (UMLS) Metathesaurus, a knowledge source containing biomedical concepts and terms from many controlled vocabularies and classifications.

CMS Issues Enforcement Guidance for Transactions and Code Sets

On July 24, 2003, the Centers for Medicare and Medicaid Services (CMS) held an audio-conference to describe simultaneously released enforcement guidance for post-October 16th noncompliance with the Health Insurance Portability and Accountability Act's (HIPAA) transaction and code set regulations. The guidance is significant in at least two ways. First, it documents an underlying reality that the healthcare industry is largely unprepared for the transition from legacy transaction formats to HIPAA-mandated formats. Second, it largely puts to rest any expectations for a regulatory or legislative extension to the October 16 deadline for compliance.

Grounding its enforcement policy on §1176(b) of the Social Security Act, CMS has formulated a flexible policy that is based on the facts and circumstances of each covered entity. Although the policy reaffirms the October 16 deadline and the legal duty to comply, CMS also stated that its enforcement process will be complaint-driven. The policy is designed to motivate health plans to build not only a track record of technical compliance but also one of outreach and testing with provider trading partners. If CMS receives a complaint, it will expect a showing of:

- Compliance, or
- Good faith efforts to comply, and
- A corrective action plan.

Good faith efforts will vary by setting. Indicators will include awareness outreach, testing and contingency planning. Health plans that have engaged vigorous outreach and testing will not be penalized if they operate legacy payment systems after October 16, 2003, that accept and process noncompliant claims. CMS will excuse these noncompliant systems as a form of contingency planning. Overall, pre-October 16 efforts will greatly outweigh the value of post-October 16 efforts. After October 16, 2003, CMS will expect noncompliant covered entities to submit corrective actions plans that remediate noncompliance in a time satisfactory to the Secretary.

Long Quest for Universal Electronic Health Record Took a Few More Steps Forward

On April 27, 2004, President Bush signed an executive order creating a National Health Information Technology Coordinator at the sub-cabinet level. The position will report directly to the Secretary of Health and Human Services. The National Coordinator will direct a plan to move the nation towards an interoperable, secure health information system that will reduce medical errors, improve healthcare quality, and produce greater value for healthcare expenditures. The executive order outlines a ten-year plan intended to:

- Advance development and adoption of health information standards;
- Address key technical, scientific, economic and other issues;
- Evaluate and assess benefits and costs of interoperable health information technologies;
- Address privacy and security related concerns with interoperable systems and recommend methods to insure authorization, authentication, and encryption;
- Not rely on additional federal spending;
- Include measurable outcome goals.

The plan will continue to build on ongoing initiatives to standardize health information and records. It will also attempt to leverage the purchasing power of federal healthcare programs to move standards closer to implementation.

I. LEGISLATION

Congress Enacts Medicare Prescription Drug, Improvement and Modernization Act

The Medicare Prescription Drug, Improvement and Modernization Act of 2003, P.L. 108-173 (Act), includes a broad array of provisions touching on health information technology. The Act will:

- Establish standards for electronic prescribing (e-scribing), including development of a safe harbor and Stark exception to enable physicians to receive e-scribing hardware, software and training used solely to receive and transmit information in the Medicare e-scribing program.
- Authorize Medicare Advantage Plans to promote e-scribing by participating physicians by offering differential payment to those who adhere to e-scribing standards.
- Establish matching (50/50) grants to enable physicians to acquire e-scribing hardware, software, etc.

- Create a Commission on Systemic Interoperability to develop a comprehensive strategy for adoption and implementation of healthcare information technology standards.
- Extending the duration and scope of the Telemedicine Demonstration Project begun under the Balanced Budget Act of 1997.
- Authorize a study and a report on skilled nursing facilities as originating sites of telehealth demonstrations.
- Impose upon Medicare contractors the obligation to develop and implement contractor-wide information security programs that will be subject to audit by independent auditors.
- Require Medicare, and Medicare contractors, to establish Web sites to make relevant information available to Medicare beneficiaries via the Internet.

Medicare Prescription Drug, Improvement and Mod-ernization Act of 2003, Pub. L. 108-173, 117 Stat 2066 (2003).

II. LITIGATION

US Court in Arizona Dismisses Claim of Negligent Security Based on Lack of Evidence of Damages to Plaintiffs Whose Personal Information Was Stolen

A federal US District Court in Phoenix, Arizona, dismissed most, but not all, of the complaint in a case involving the theft of a laptop computer containing personal information (e.g., names, social security numbers) on 500,000 military personnel from the offices of TriWest Healthcare Alliance Corp., a large contractor for the Department of Defense TRICARE program. Although the plaintiff class alleged negligent security, the court held that there was no showing of damages to the plaintiffs; and, absent damages, an allegation of negligence alone would not survive a motion to dismiss. The case is significant because in testimony on April 3, 2003, before the US House of Representatives Subcommittee on Financial Institutions and Consumer Credit, TriWest testified at length about its mitigation efforts (e.g., contacting every beneficiary, contacting the media, establishing a web site, etc.) following discovery of the break-in. The ruling of the court suggests that TriWest's mitigation efforts may have been sufficiently successful to blunt the initial theory of the lawsuit. An amended complaint remains an option.

Stollenwerk v. TriWest Health Care Alliance Corp., No. 2:03cv00185, 2003 WL 22399295 (D. Ariz. Oct. 21, 2003).

The court's dismissal suggests that the insurer's effort to mitigate damages to individuals after their information was stolen may have successfully blunted the initial theory of the lawsuit.

U.S. Court in Florida Approves Settlements Between Health Insurers and Physicians

In the ongoing litigation between a class of roughly 700,000 physicians and most of the large commercial health insurers, the class physicians reached settlements approved by the court with CIGNA on September 4, 2003, and with AETNA on October 24, 2003. The settlements are significant with respect to health information technology and the law because both settlements obligate the defendant insurers to make substantial investments in the information technology infrastructure and to use electronic information systems (e.g., e-mail, Web sites) to make their business processes more accessible to participating physicians. For example, in its settlement, CIGNA agrees to make substantial investments in Internet and clearinghouse connectivity to enable physicians to electronically pre-certify, submit claims, and check member eligibility. CIGNA also agrees to establish an email address to enable class members to inquire about CIGNA's claims administration policies and issues relating to coverage.

In re Managed Care Litig., No. 00-MD-1334 (S.D. Fla.).

The settlements are significant because they obligate insurers to invest in the information technology infrastructure and to use electronic information systems to make their processes more accessible to physicians.

US Court in Illinois Holds That HIPAA Privacy Standards Elevate State's More Stringent Medical Privacy Act and Incorporate It into Federal Law

The effect of HIPAA's pre-emption provision was challenged in the maelstrom of abortion litigation surrounding challenges to the Partial Birth Abortion Ban Act of 2003. The case is significant because it will result in a better understanding of whether more stringent state laws have a role in privacy litigation in federal court, or whether the Privacy Standards alone control the use and disclosure of PHI in that forum. The US Department of Justice argued that medical records subpoenaed by the Department could not be protected by more stringent Illinois law because the Supremacy Clause and Federal Rules of Evidence control what law applies in a federal forum. Nonparty hospitals objected to the government's discovery of their medical records citing Illinois statutory and decisional law prohibiting disclosure of records even when identifying information had been redacted. The Court held that the Privacy Standards elevate Illinois' more stringent Medical Privacy Act and incorporate it into federal law, making it applicable in a federal case. Clearly headed for appeal, the case has the potential to define for the federal courts what role will be played in federal court litigation by more stringent state law.

National Abortion Fed. v. Ashcroft, No. 04 C 55, 2004 WL 292079 (N.D. Ill. Feb. 6, 2004).

This case is significant because it will result in a better understanding of whether more stringent state laws have a role in privacy litigation in federal court, or whether the Privacy Standards alone control the use and disclosure of PHI in that forum.

US Court in Illinois Says It Has Authority to Order Plaintiffs to Sign HIPAA Authorizations

The Privacy Standards again came into play in the context of a pharmacy malpractice suit. Defendants sought plaintiff's prior men-

Continued on page 18

Continued from page 17

tal health records, and the court ordered them disclosed pursuant to an authorization that plaintiff was ordered to sign. Plaintiff challenged the order and claimed that the court lacked authority to order plaintiff to sign an authorization. In what may be a first in the jurisprudence of HIPAA authorizations, the court held that "we clearly have the authority to require plaintiffs to sign the authorizations." Plaintiffs cannot bring a subject's "mental health into issue and then refuse access by the defendants to relevant information."

Happel v. Wal-Mart, No. 02 C 7771, 2004 WL 755581 (N.D. Ill. Feb. 3, 2004).

This case is significant mainly because it asks and answers the question of whether a court can order a party to sign a HIPAA privacy authorization in litigation.

Texas Appeals Court Declines to Entirely Dismiss Pre-HIPAA Privacy Case Because Existence of Hospital Privacy Policies Did Not Prove Policies' Enforcement

One year after covered entity providers everywhere adopted numerous new policies, this case looks at liability founded on whether a Texas hospital adequately enforced similar policies adopted in accordance with state law. The facts involved a teenage girl, J.L., who was allegedly beaten by her boyfriend. Her mother took her to the local hospital, where she was x-rayed and treated for injuries. An employee of the hospital removed J.L.'s medical records from the hospital and showed them to the boyfriend. Sued for invasion of privacy and violation of Texas statutory law, the hospital sought to dismiss the action, arguing that it had adopted privacy policies and trained the employee on the policies and that in removing them, the employee clearly acted beyond the scope of employment. The hospital's motion to dismiss was accompanied by a copy of its policies, an acknowledgment that the employee had received them, and a confidentiality statement signed by the employee. Notwith-standing this documentation, the Court held that the case could not be dismissed entirely because the existence of policies did not prove that they were actively enforced. Holding that the mere fact that the records had been removed from the hospital gave rise to a genuine issue as to whether the policies were adequately enforced, the court declined to dismiss the claim for negligent supervision of its wayward employee.

Foster ex rel. J.L. v. Hillcrest Baptist Med. Ctr., No. 10-02-143-CV, 2004 WL 254713 (Tex.App.-Waco Feb. 11, 2004).

In the policy and paper driven post-HIPAA world, this case nicely illustrates that enforcement of privacy policies will play a pivotal role in future privacy litigation.

Seventh Circuit Quashes Subpoena After Finding Records Sought Lacked Sufficient Probative Value to Outweigh Privacy Interest

The Seventh Circuit quashed a subpoena for medical records on dilation and extractions performed at Northwestern Hospital in Chicago. The decision is important because the appeals court stepped back from the lower court's ruling that the federal privacy regulations incorporated more stringent state protections and made them applicable in federal court on federal question cases. Instead, the appeals court disposed of the case on the narrower and more fact specific basis that the records sought lacked probative value sufficient to outweigh the loss of privacy that would accompany the disclosure of the records.

Northwestern Mem'l Hosp. v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).

This case is important because the court quashed a subpoena on a fact-specific basis that the records sought lacked sufficient probative value to outweigh the loss of privacy.

US Court in Pennsylvania Dismisses Challenge to HIPAA Privacy Standards

The US Court for the Eastern District of Pennsylvania dismissed on summary judgment a challenge by a privacy advocacy group to the Privacy Standards. The case is significant in that it represents the last of the first generation of challenges to the Privacy Standards. Plaintiffs had focused particularly in this case on the repeal of the original rule requiring an individual's consent. Dismissing the contention that the Secretary of Health and Human Services had exceeded his authority by eliminating the consent requirement, the court held that § 264 of HIPAA permitted the Secretary to balance privacy protections against efficiency of the healthcare system.

Citizens for Health v. Thompson, No. Civ.A. 03-2267, 2004 WL 765356 (E.D. Pa. Apr. 2, 2004).

This case emphasizes the Secretary's authority under HIPAA to balance privacy protections against the efficiency of the healthcare system.

III. REGULATIONS

CMS Issues Final Regulations Mandating Electronic Claims Submission to Medicare

Implementing the Administrative Simplification Compliance Act, CMS published final regulations requiring all but the smallest Medicare providers and practitioners to submit electronic claims to Medicare. The impact of the rules will be threefold. First, the rules will reduce greatly Medicare's volume of 139 million paper claims each year. Second, the required electronic submission will subject all but the smallest providers to compliance with HIPAA's other rules on privacy and security. Third, CMS expects that once committed to electronic transactions for Medicare claims that providers will carry that commitment forward to all other types of transactions both with Medicare and non-governmental payors. Borrowing heavily from related HIPAA Administrative Simplification regulations, these regulations define a claim as one defined under the Standards for Electronic Transactions.

Medicare Program; Electronic Submission of Medicare Claims, 68 Fed. Reg. 48805 (Dep't of Health and Human Servs. Ctrs. for Medicare & Medicaid Servs. Interim Final Rule Aug. 15, 2003).

FDA Adopts Final Rules Requiring Bar Codes on Prescription Drugs and FDA-Regulated OTC Drug Products

The Food and Drug Administration (FDA) adopted final rules that require all manufacturers, repackers, relabelers, and private label distributors of human prescription drugs or over-the-counter drug products regulated by the FDA to add a linear bar code to the label of their products. The bar code rules are a further step towards a less error prone environment in healthcare and a demonstration of the belief that technology can play a major role to establish that environment.

The bar code must contain only the National Drug Code for the drug. The stated purpose of the bar code requirement is to reduce the number of medication errors. The FDA envisions the bar codes as an essential element of a wider effort that will involve hospitals installing bar code scanners that will feed bar code data into computer maintained databases of patient medication regimes. When a healthcare professional administers the drug in question, it will be scanned against the label bar code and a wristband with patient identifying bar code information.

The FDA was clear in stating that it did not regulate hospitals or their technological choices. For this reason, the FDA adopted the most prevalent and inexpensive form of technology (e.g., linear bar codes) rather than more sophisticated but less proven methods such as radio frequency identification chips. In addition, the FDA chose not to include lot and expiration data in the initial bar code content requirements. The FDA has stated that its objective is to establish for hospitals a reliable "technological floor" and monitor the need for other requirements. The bar code rules will take effect for newly approved drugs not later than sixty days following their approval and two years following the effective date of the rules for all existing drugs.

Bar Code Label Requirement for Human Drug Products and Biological Products, 69 Fed. Reg. 9120 (Dep't of Health and Human Servs. Food & Drug Admin. Final Rule Feb. 26, 2004).

CMS Adopts Requirements for Unique Health Identifier for Healthcare Providers

The Secretary of Health and Human Services adopted final rules for a standard for unique health identifiers for healthcare providers. Adding yet another piece of the overall system of standards for administrative simplification, the national provider identifier (NPI) will consist of a ten-digit, numeric identifier with no embedded intelligence. The NPI must be used in all standard transactions. The compliance date for use of the NPI is May 23, 2007, for all but small health plans. NPIs will be issued to any healthcare provider, and sub-parts of providers. Providers seeking an NPI must apply to the National Provider System, which will conduct enumeration of providers for the government.

HIPAA Administrative Simplification: Standard Unique Health Identifier for Health Care Providers, 69 Fed. Reg. 3434 (Dep't of Health and Human Servs. Ctrs. for Medicare & Medicaid Final Rule Jan. 23, 2004).

AMERICAN HEALTH LAWYERS ASSOCIATION

1025 Connecticut Avenue, NW, Suite 600
Washington, DC 20036-5405
Phone: (202) 833-1100
Fax: (202) 833-1105
healthlawyers.org

Save these Dates!

HIPAA Privacy in Clinical Research: Issues, Approaches, and Solutions Teleconference

Co-sponsored by Health Information and Technology and Teaching Hospitals and Academic Medical Centers Practice Groups

Wednesday, October 13, 2004 • 1:00 - 2:30 pm Eastern

HIT Practice Group Mid-Year Luncheon

Friday, November 12, 2004

Fundamentals of Health Law Program • Chicago, IL • November 10-12, 2004

HIT News

Summer 2004 (August)
Volume 7
Issue 2