Protecting Medical Privacy In a Digital Age: Beyond Policies and Procedures, A Critical Role for Technology

BY

Bruce Merlin Fried, Esq.

Shaw Pittman, LLP

"Your information is confidential. We are dedicated to keeping your personal health information confidential. We take many precautions to make sure others can't pretend to be you and get your confidential information from this Web site."

- Kaiser Permanente Web Site Privacy Policy – prior to inadvertent release of hundreds of members' private information.[1]

Introduction: New Technologies, New Concerns

Two powerful forces, seemingly at odds, are sweeping through America's healthcare system: the accelerating implementation of digital and information technologies (IT) and society's demand that our personal medical information be protected from improper disclosure. Lawmakers in Congress, the Executive Branch and the states are struggling to develop public policies which strike the right balance between encouraging the use of healthcare IT and protecting the privacy of our personal health information.

The truth is that even the most thoughtful, carefully honed privacy policy, standing alone, will fail to prevent purposeful or inadvertent disclosures of protected healthcare information. Instances of digital health records being released through email or via the Internet due to human error, or worse, are regularly reported. Such events undermine the public's confidence not only in the company that releases the information but in America's private healthcare system. Understandably, patients are increasingly reluctant to share sensitive medical information with their clinicians for fear their secrets will become known by family, friends, neighbors, employers or even strangers.

The incentives to assure privacy protections have become even sharper as medical privacy laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), begin to be enforced. The civil and criminal penalties which may be levied under HIPAA and other federal and state laws, not to mention market consequences, should focus the attention of health insurers, providers, physicians, data companies and others on using strategies to keep personal health information private. Beyond the risk of governmentally imposed sanctions, lie platoons of trial attorneys who are sharpening their focus on this new area of liability.

Clearly, those charged with protecting health information from wrongful disclosure will need to implement new procedures and create within their organizations a culture which places the highest value in protecting their customers' medical secrets. But these necessary steps will not be sufficient. New technologies, designed to mitigate the risk of wrongful disclosures via email or the Internet, are our essential defense against privacy breaches, agency enforcement, and tort litigation.

The Healthcare IT Challenge: Improving Quality and Efficiency While Assuring Individual Privacy

Data in patient medical records are the information mother lode of the healthcare system. They are the institutional memory for clinicians and health care providers and provide the basis and justification for treatment and payment. For the patient, medical records are where their most intimate, potentially embarrassing and deepest personal secrets reside.

The end of the paper medical record is near. The ability of health professionals to effectively use paper medical records is limited. Paper records are cumbersome, requiring huge amounts of space. Moreover, they cannot be effectively searched for meaningful data. The information in a paper record cannot be easily shared with other clinicians or researchers. Paper medical records are static, isolated data sets designed more to defend against malpractice or financial fraud and abuse claims then to be analyzed for the advancement of medical or scientific knowledge.

Digitizing medical records has been a holy grail for the healthcare community for decades. Now, paper based medical records are quickly yielding to computer technology.[2] Electronic or digital medical records (DMRs) offer versatility and the prospect of more efficient, more effective, higher quality healthcare. Information contained in DMRs is used to coordinate billing, advise physicians, help compile comprehensive, longitudinal medical histories, enable utilization and quality review and permit the development of clinical practice profiles and patient drug profiles. With the growth of organized care systems, managed care plans and integrated delivery systems, an increasing number of entities are handling DMRs at any one time. Not only do doctors, labs, pharmacies, and hospitals have access to medical information about patients, but so do insurance companies, medical group administrators, drug companies, marketers, biomedical researchers, medical information bureaus, and oversight and accreditation bodies.

Increasing reliance on healthcare information technology (IT) – while advancing healthcare quality and efficiency – has also made it easier for personal medical information to be disseminated. The free and rapid flow of personal medical information, facilitated by healthcare IT, offers enormous benefits to clinicians and administrators, but not without risks to our privacy.

Prior to the Internet, email, and other IT advances, a provider would need to have a patient's medical record photocopied before it could be shared. Now, with a mere click of the mouse, that same provider can electronically transmit a patient's entire medical record. When an entire record is sent or the wrong information is distributed or, worse, information is sent to an unauthorized recipient, potential violations of health privacy regulations begin to mount. Whether inadvertent or not, in the blink of an eye, an entire medical record can be sent to the wrong person. And just as fast, the organization that wrongfully sent the record has become vulnerable to legal and market liabilities.

Problems and Anxieties

As noted in health law and policy journals, industry papers, and in major media, anxieties about the use (and misuse) of personal health information are increasing. Some recent statistics, provided in literature from the Health Privacy Project at Georgetown University, include:

- Only one-third of U.S. adults say that they trust health plans and government programs to maintain confidentiality all or most of the time.
- One in five American adults believe that a healthcare provider, insurance plan, government agency, or employer has improperly disclosed personal medical information.
- Only 38% of Fortune 500 companies say that they *do not* use or disclose employee health information for employment decisions.
- One in six American adults say they have done something out of the ordinary to keep medical information confidential.
- It is estimated that around 150 people have access to a patient's medical record during the course of a typical hospitalization.
- The Association of American Physicians and Surgeons reports that *78%* of its members report withholding information *from a patient's medical record* due to the *physician or surgeon's privacy concerns.*

The last statistic may be the most shocking. Not only are patients fearful of how their personal medical information is being used but, their doctors are similarly concerned – so concerned, in fact, that some are withholding potential essential information from medical

charts to eliminate the risk of improper disclosure.

Improper Disclosures – Reports from the Field

Anxieties about improper release of patient medical information are well founded. There have been numerous instances of personal medical information being used improperly. For example, a banker who sat on a county health board gained access to patients' medical records, identified several people with cancer, and called in their mortgages.[3] As previously noted, the increase in technological sophistication has caused other problems. Thousands of University of Michigan health system patients had personal and medical information released over the Internet without knowing it. Records were online and available to the public for at least two months. It was not until a student stumbled on to them trying to help a friend find a doctor that the problem was corrected.

An increasing amount of information is being disseminated through internal and external emails. As the general public has become comfortable with, even dependant on email, there is a growing call for email communications between physicians and patients. While this new mode of communicating makes great sense, it is not risk free. For instance, patients who email their physicians from their workplace cannot be assured of confidentiality and may inadvertently expose sensitive details of illness or social circumstances to their employer.[4] Patients who use family email accounts at home may lack privacy from their spouses, children, or parents.

Administrative errors can permit or cause the release, misclassification or loss of information or compromise data accuracy which threatens medical privacy.[5] Human error, misuse by users, and uncontrolled access to the digital medical record may be even a greater threat. As digital medical records become more prevalent, researchers are capturing, storing, aggregating and analyzing the data in those records for various scientific and marketing purposes. This process of data warehousing and data mining offers enormous benefits: we learn why certain drugs are effective for some people but not others; we learn why some physicians have superior results as compared to others; and medicine becomes more evidenced based and less a matter of art. But here again, society must be concerned that data which is intended to be securely warehoused is not susceptible to improper disclosure. A misdirected email can reveal not just a discrete amount of data, but a virtual warehouse of personal medical information. [6]

With deadlines for complying with new healthcare privacy regulations like HIPAA looming and the potential for liability resulting from negligent breaches of confidentiality, healthcare entities must be proactive in preventing wrongful disclosures such as those which occurred

in the following cases:

University of Montana – Children's Mental Health Records Posted on Web

Detailed psychological records of 62 children and teenagers were accidentally posted on the University of Montana's Web site beginning October 29, 2001.[7] The over 400 pages of documents that were posted "describe patient visits and offer diagnoses by therapists of mental retardation, depression, schizophrenia and other serious conditions" and in most cases listed patients' names, dates of birth, addresses and schools attended.[8]

It is unclear how these records made it onto the Internet, but a University official said that a student or technical employee may have accidentally posted the records, which were discovered only after a local paper reported that the information was online.[9] The former president of the American Psychological Association, Daniel Borenstein, commented on the disclosure saying, "That's the danger with having all these electronic records…If you push the wrong button or put something in the wrong spot on your Web site, it [can mean] immediate distribution of a massive amount of private medical information."[10]

Eli Lilly – Medi-Messenger Email Service Goes Awry

Eli Lilly & Co. developed "Medi-Messenger", an email service which reminded people to take their medications.[11] One could sign up for the Medi-Messenger service through Eli Lilly's "Prozac.com" Internet site which is geared towards users of Lilly's anti-depressant, Prozac. The automated system was supposed to send messages anonymously. The email's "To:" line was to be blank, while the email address of the recipient was to be entered in the "bcc" line (which permits the message to be sent to the bcc recipient without revealing the names and/or email addresses that had been entered into this "blind" field). The Medi-Messenger system was fully functional for two years. On June 27, 2001, Lilly sent an email to notify users it was discontinuing the service[12] and, in a much-publicized debacle, human error caused all the email addresses of all Medi-Messenger recipients to be included in the "To:" line.[13] As a result, the names and/or email addresses of all the other Prozac users on the mailing list became public.

By all accounts, Eli Lilly's response was good, but it was time consuming. According to Lilly all emails to patients were stopped while the problem was being corrected.[14] Lilly responded individually to every complaint, sent a separate message, and apologized to all Medi-Messenger users.[15] In addition, a new code-review procedure was instituted to block all outgoing messages with more than one name in the "To:" field.[16]

The problems did not end there for Lilly, however. In response to consumer complaints, the American Civil Liberties Union (ACLU) sent a letter to the Federal Trade Commission (FTC) accusing Lilly of negligence, deceptive trade practices and violations of Lilly's own published privacy policy. In the letter to the FTC, the ACLU wrote, "The events have set a dangerous precedent. Eli Lilly had a duty of care and a duty under the Federal Trade laws to protect the confidentiality of the medical consumers who use (its) product." Citing Lilly's stated promise of confidentiality, the ACLU asserted that their actions constituted unfair trade practices. "Eli Lilly had led John Doe and the hundreds of other users of its Medi-messenger service to believe that their identities would be protected. Its apparently negligent dissemination of his identity was made without his knowledge or consent. By divulging his identity as a user of anti-depressants, Eli Lilly's actions have caused him substantial injury, and are likely to cause substantial injury to him in the future – injuries they cannot reasonably avoid and are not outweighed by countervailing benefits to him or competition."

Although Lilly said the release was a human programming error, ACLU responded, "Whether they did it inadvertently or not, they did it." [17]

Kaiser Permanente – Bulk Emails Sent to Wrong People

In August 2000, Kaiser Permanente – one of the nation's largest health insurers – inadvertently sent the private correspondence of over 850 of its members to approximately 19 people. Some of the customers' misdirected emails contained hundreds of messages.[18] The error occurred through "KP Online," a website through which Kaiser members can gain access to health information, participate in discussion groups, make appointments, request advice from a nurse or ask questions of a pharmacist. Some of these emails contained sensitive personal medical advice (e.g., response to member's questions about sexually transmitted diseases) as well as home phone numbers and medical account numbers.[19]

Kaiser officials attributed the misdirected correspondence to "human error" and a "technological glitch" which occurred when a technician was upgrading the Web site. The problem was caught by the technician after noticing that a lot of the emails being sent were very large. According to Kaiser, "This is not a security breach of our Internet service . . . . This is accidentally sending emails to the wrong people. All of us have sent emails to the wrong persons . . . ."

Fixing the Kaiser problem was not easy, either. Company officials attempted to phone each of the members whose emails were misdirected and also tried to apologize to every person. To fix the problem, the email sending protocol had to be changed.

The California Department of Managed Healthcare conducted an investigation of the incident resulting in an "administrative penalty" of $25,000 being levied against Kaiser.[20] Kaiser also acted promptly to mitigate any harm and implemented corrective measures to reduce the likelihood of such an event happening again. As a result, "[t]he amount of the fine is less than that which the Department would have otherwise sought had [Kaiser] not been forthcoming about the incident, and had it not taken steps to remedy the problems resulting from the error." [21]

DHHS – Government Website Reveals Personal Online Requests

Even the government has problems. A government health information Web site exposed information about thousands of people who asked for pamphlets and brochures about drug and alcohol addiction. Because of a software flaw, consumers who visited the site and requested titles such as "Moving Forward With Your Life, Leaving Alcohol and Other Drugs Behind" had their names, emails and addresses revealed on an Internet page.[22] The site, Health.org is maintained by a private subcontractor for the Department of Health and Human Services' Substance Abuse and Mental Health Services Administration. Other titles on the site include "Learning to Live Drug Free," "Heroin Information for Adolescents," and "Marijuana, Facts Parents Need to Know." Although schools, hospitals and health agencies most frequently request the information, some individuals do so as well. The technical flaw in the software was so widespread and easy to use that the FBI, through its National Infrastructure Protection Center, issued a warning about it on April 6, 2001 instructing users to install a software patch to fix the problem.

New Technologies, New Laws

With new technologies come new opportunities for their use, as well as for abuse. Inevitably, public policies follow. Such is the case with the growth of healthcare IT. Initially, large insurers and governmental agencies employed mainframe computers to process the millions of claims for coverage and payment being received each day. It did not take long before those computers were linked to achieve operational efficiencies. Encouraging healthcare providers to electronically submit their claims followed shortly. The healthcare system was well on its way to being wired, at least for financial transactions.

But roadblocks emerged to the healthcare information superhighway. In many instances, computers could not talk to each other: there were no standards for data, language, forms or the myriad of other documentation requirements in the healthcare industry. To overcome these obstacles, the insurance industry created the Workgroup on Electronic Data Interchange

("WEDI"). While WEDI made good progress in developing standards, it became clear that those standards would not be uniformly implemented without a regulatory obligation.

The Health Insurance Portability and Accountability Act of 1996

Tagging on to a health insurance reform law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress enacted so-called "Administrative Simplification" provisions to create by regulation new standards for electronic transactions, data security, unique identification numbers, and privacy of individually identifiable health information. Collectively, the HIPAA standards are intended to foster the electronic exchange of health information.

The HIPAA final privacy regulations were published on December 28, 2000, and became effective on April 14, 2001.[23] Covered entities must be in compliance with the privacy regulation by April 14, 2003.

Sections 261-265 of HIPAA: "Administrative Simplification"

HIPAA's Administrative Simplification provisions were enacted to accomplish three things:

1. to "*facilitate efficiencies* and cost savings for the healthcare industry that the increasing use of electronic technology affords."
2. Direct the Department of Health and Human Services (HHS) to *issue standards* to facilitate *electronic exchange of information* with respect to financial and administrative transactions.
3. Direct HHS to *develop standards* to protect the *security*, including the *confidentiality* and *integrity*, of health information.

Section 264(b) required the Secretary of HHS to develop and submit to Congress recommendations for:

- The *rights* that an individual who is the subject of individually identifiable health information should have.
- The *procedures* that should be established for the exercise of those *rights*.
- The *uses* and *disclosures* of such information that should be *authorized* or *required*.

Which are the "Covered Entities"?[24]

HIPAA's Administrative Simplification provisions directly affect three distinct categories of "covered entities" with varying rules applicable for each.

- Health Plans – any individual or group health insurance plan, both private and public, that provides or pays for medical care (some exclusions).
- Healthcare Clearinghouses – organizations that translate health information into standard electronic format (as required by other HIPAA provisions).
- Healthcare Providers – including persons (physicians to homeopaths, etc.), entities (hospitals, clinics, etc.) and providers of supplies (pharmacists, medical equipment distributors, etc.). It does not include blood, sperm, or organ donor banks.

The regulation applies to health plans, healthcare clearinghouses, and healthcare providers *who transmit health information in electronic form* in connection with specified financial and administrative transactions, such as claims for payment.

What about "Business Associates"?

While the HIPAA statute applies directly to only covered entities, the regulation extends HIPAA's reach by requiring covered entities to compel HIPAA compliance by their business associates through the use of contracts and other written agreements. Whenever a covered entity discloses Protected Health Information ("PHI") to an agent, subcontractor or other business associate to provide a service for the entity – whether by email or any other method - an appropriate business associate agreement is required. Business associates may not use or disclose PHI for any purpose beyond that which is required to complete the work requested by the covered entity.

What is "Protected Health Information"?[25]

Information that is protected under HIPAA is health information that is "individually identifiable" and is created or received by a covered entity. This PHI can include not only that which is in electronic form, but any oral or recorded information relating to past, present or future physical or mental healthcare or payments (e.g., medical records, notes, billing). Information that is "individually identifiable" is health information that identifies or reasonably can be used to identify the individual.[26]

Minimum Necessary Standard[27] – Identifying Access Groups and Implementing Restrictions

One important privacy protection, which specifically addresses some of the concerns with the increasing computerization and resulting ease of dissemination of medical records, is the "minimum necessary standard."[28] This standard requires the covered entity to take reasonable efforts to limit information used or disclosed to the "minimum amount necessary to accomplish the intended purpose of the use or disclosure."[29]

Except when used for treatment purposes, covered entities must limit their use and disclosure of PHI to the "minimum necessary" amount. The final rule – and its "minimum necessary" standard – requires a complex "mapping" of personnel to the specific categories

of PHI that they are allowed to access to perform their job functions. Moreover, the covered entity must implement policies and procedures to limit access only to the identified person and the identified PHI necessary. Although a review of each request or disclosure – when routine – is not required, the policies must identify the types of PHI to be disclosed, the types of persons who would receive the PHI, and the conditions that would apply to such access.

The preamble to the final privacy rule acknowledges that one of the largest ongoing costs to covered entities will arise from compliance with the minimum necessary standard. The rule allows the use of standard policies for routine activities and requires a covered entity to make "reasonable efforts" in limiting PHI to what is minimally necessary; however, there will still be significant administrative burdens and costs associated with making individualized determinations for non-routine uses and disclosures of PHI. Technologies that cheaply and efficiently satisfy many of these requirements will be a necessary component of HIPAA compliance.

Consent and Authorization

Similar to the mapping involved in complying with the minimum necessary standard, covered entities will need to find ways in order to verify that the entities have obtained the necessary written permission from patients for the use or disclosure of their PHI. "Consent" is required for use or disclosure of PHI for treatment, payment, and the entity's own operations. When an individual's health information is to be used or disclosed for certain specific purposes *other than* treatment, payment, or healthcare operations, "authorization" is required.

Compliance and Enforcement

Compliance is not going to be cheap. Estimates of the cost of HIPAA compliance for the health care system range from $18 to $40 billion dollars.[30] HIPAA is enforced by HHS' Office of Civil Rights. Other federal agencies, including the Office of the Inspector General, the Centers for Medicare and Medicaid Services, and the Department of Justice are expected to also be involved in HIPAA enforcement. The law provides for the imposition of civil and criminal penalties. Civil penalties can add up quickly: at $100 per person per violation (with a cap of $25,000 each year for each standard violated). A person who "uses or causes to be used a unique health identifier," discloses individually identifiable health information to another person, or obtains individually identifiable health information relating to an indi-

vidual, is subjected to a number of penalties. The criminal penalties include a fine up to $50,000 and/or imprisonment of up to 1 year. If the offense is with the intent to use individually identifiable information for commercial advantage, personal gain, or malicious harm, the fine can be up to $250,000 and/or imprisonment up to 10 years.

As the details for determining compliance and applying penalties is not yet finalized, there is some flexibility in the law. What will be most important, therefore, is whether the entity can demonstrate a good faith effort to understand the rules and to achieve compliance. Without a doubt, a more expensive fine is guaranteed for wrongful disclosure of patient information when no compliance effort is made.

Beyond the imposition of statutory fines is the potential harm to an organization's reputation. Respect and trust by patients and customers, standing in the community and years of good will can all evaporate should a patient's healthcare secrets be wrongfully disclosed. These "marketplace penalties" may be even more compelling than the prospect of government enforcement actions.

Other Laws

While HIPAA may be the newest and most comprehensive federal law to protect the privacy of medical information, it does not stand alone. Indeed the number of federal laws creating protections for personal health information are too numerous to list completely. For example, compliance with the Americans with Disabilities Act (ADA)[31] makes it essential that employee medical records be segregated from other employee records and never used for employment decisions. On a global level, the European Commission's Directive on Data Privacy went into effect in October 1998. This Directive prohibits the transfer of personal information to non-European Union countries that do not meet the stringent European standards for privacy protection.

State statutes and common law remedies offer patients a remedy when medical records are exposed. For example, breach of confidentiality, invasion of privacy, breach of contract, and breach of fiduciary relationship form the bases for legal action against practitioners who unreasonably publicize information. Many states have enacted specific privacy provisions for medical information. Among such laws are those that require HMOs to hold medical information confidential, to provide for the confidentiality of hospital patients' medical records, and to protect medical information from general public exposure.

Physicians and other healthcare providers often have a legal obligation to protect medical information from unnecessary and unauthorized disclosure. Legal standards often emanate from prevailing ethics codes, whether the case is brought under an implied contract, fiduciary duty or invasion of privacy theory. The American Medical Association, for example, explicitly delineates elements of a physicians' obligation to provide a confidential relationship, absent a legal or therapeutic directive to disclose information to a third party.[32] The AMA interprets the physician's duty to uphold patient confidentiality broadly, asserting that "information disclosed to a physician during the course of a relationship between physician and patient is confidential to the greatest degree. The physician should not reveal confidential communications or information without the express consent of the patient."[33] Because of the duty to protect patient confidences, individual physicians will be required to insulate their patients' emails from public view. To protect patient data generally, and email specifically, a physician's duty to guard confidentiality must involve more than a pro forma awareness.[34] Rather, physicians and other healthcare professionals should take precautions to secure patient-related email both through enhanced technological security and clearly defined and observed office practices.

Best Technology Practices in Protecting Medical Privacy – The Role for Email Filtering Technology in a HIPAA Compliance Strategy

Achieving the level of privacy protection required by HIPAA and other federal and state laws will require new policies, procedures, employee training, consents, authorizations and other steps mandated by law and regulation. But those steps alone will not be sufficient to mitigate the risk of purposeful or inadvertent disclosures of PHI. Technology advances have led to the current privacy challenges and technology must now be used to help provide privacy protections.

A comprehensive strategy for securing patient privacy should include email content management software. Such technology from a trusted provider is an essential component of HIPAA compliance. Email filtering can significantly mitigate the possibility of PHI being inadvertently or willfully released to unauthorized parties through email.

America's growing comfort with and use of information technology can lead to disastrous

results in violation of new and existing law:

- A well-intentioned employee making a simple mistake can release large volumes of PHI to the general public;
- A key-stroke error can result in sensitive health information being emailed nearly simultaneously to a great many unauthorized recipients; and
- A disgruntled or unstable employee could knowingly disclose PHI for a variety of personal reasons.

So, the question is, what positive steps can covered entities take to avoid wrongful disclosures? HIPAA-covered entities that deploy best technology practices should familiarize themselves with secure content technology that can guard against the wrongful disclosure of PHI and help covered entities comply with the new "minimum necessary standard."

Organizations can employ technology to control who is permitted to email information to specific designated recipients. Sophisticated email content management tools using advanced email filtering technology allow organizations to give authorization rights to *designated* employees to email *particular* information to *intended* recipients. Perhaps more importantly, rules enforced by filtering technology can prevent emails containing PHI from being sent by unauthorized employees to unintended recipients.

Email filtering software can be used to recognize specific email content — including particular file types and/or certain key words — and then delay a message from being sent until it is reviewed by an authorized manager. Individuals authorized to email certain types of health information could do so unhindered, while emails that trigger a content restriction rule would be stopped.

Using secure email content tools is a best technology practice for avoiding legal liability from the accidental – or purposeful – release of protected patient records or other kinds of confidential health data. It is possible that a covered entity, a hospital for example, that releases PHI to an unauthorized recipient could be found negligent if it did not have email filtering in place that could have prevented the release. Similarly, for business associate relationships, if a covered entity knows that its partner has a pattern of activity that results in a material breach of information and has not taken steps to stop it (e.g. implemented available email filtering technology), business contracts must be terminated, if feasible. Or, the entity must report the errant business associate to the Secretary of Health and Human Services.

Compliance will require covered entities to examine every aspect of their information practices, including:

- Revising contracts with business associates and modifying contracting procedures;
- Drafting new medical information policies and procedures, authorizations, notice and consent forms; and
- Establishing new administrative procedures that govern how they use and disclose individually identified health information.
- Establishing best technology practices to implement the new policies and procedures.

Mandatory compliance deadlines are not far away, and the complexity of the rule is such that all covered entities should begin to take immediate steps towards compliance.

Does your company comply with the regulations and assure responsible information handling?

- Are procedures in place for preventing former employees from gaining access to computer files?
- Are files secured and available only to qualified persons?
- Have you taken extra precautions to guard against leakage of information?
- When providing copies of medical records to others, do employees make sure that nonessential information is removed? Is personally identifiable information that has no relevance removed?
- Does your email system allow you to control who is authorized to send or receive certain types of confidential files, such as a medical record?

The Politics of the Policy Process: The Future of HIPAA

Since its first drafting, HIPAA's privacy provisions have been under constant assault by many interested parties including hospitals, insurance companies, privacy advocates and patient groups. The debate has swirled around operational complexities of the new standards and competing perspectives of the regulation's stringency or laxity. For now, the status of HIPAA has apparently settled. When the regulations became effective on April 14, 2001 the public (and the industry) was admonished that there would be some changes to the Rule before the April 14, 2003 compliance date. Indeed, the Administration issued "guidance" to interpretation of the Rule in August 2001. While doing little more than clarifying ambiguities and resolving internal conflicts, the Administration indicated more fundamental reforms could be expected in a forthcoming modification to the Rule. Such a modification is expected by early 2002.

It goes without saying that the terrorist attacks of September 11th have profoundly changed the nation in many ways, including the development of public policy. The implications for the HIPAA privacy rule are uncertain. As published, the Rule permitted PHI to be used or disclosed without authorization or consent for law enforcement and national security purposes. As policy makers shift their focus to international matters and issues of domestic security, it is unlikely that major domestic policy initiatives will be advanced. Major reforms to existing medical privacy laws, which would likely result in partisan conflict, are unlikely. That being the case, insurers, hospitals, other covered entities and others effected by the Rule should proceed with their efforts to become compliant.

- **Bruce Merlin Fried** is a partner in the Health Law Group at Shaw Pittman, LLP. Mr. Fried has counseled many organizations on HIPAA and health privacy policies including health insurers, managed care organizations, contract research organizations, hospitals, health data companies and physician groups. Previously, Mr. Fried was the Director of the Center for Health Plans and Providers at the Health Care Financing Administration where he was responsible for Medicare policy and operations. Shaw Pittman is an international law firm based in Washington, DC. Mr. Fried can be reached at Bruce.Fried@ShawPittman.com.

This White Paper was commissioned by SurfControl, the number one Internet filtering company in the global security market. SurfControl is the maker of SuperScout Email Filter, a simple solution to preventing an employee from accidentally releasing private medical records containing personally identifiable information. The email filter also is the only technology that allows designated managers to review email remotely before it is sent to determine if it potentially violates privacy rules. For more information about the SuperScout Email Filter, visit Web site www.surfcontrol.com/hipaa.

SurfControl, Inc.
100 Enterprise Way, Suite A110
Scotts Valley, California 95066, USA
Tel: 1-831-431-1300 Fax: 1-831-431-1800
Email: surfsales@surfcontrol.com

[1] Bill Brubaker, "'Sensitive' Kaiser Emails Go Astray," *Washington Post*, Aug. 10, 2000, p. E01.
[2] "Legal implications of electronic transmission of patients' records in the managed care pharmacy industry," *Compensation & Benefits Management,* Winter 2000, Vol. 16, No. 1, pp. 33-45.
[3] 65 Fed. Reg. 82468.
[4] Kenneth D. Mandl, Isaac S. Kohane, & Allan M. Brandt, "Electronic Patient-Physician Communication: Problems and Promise," *Annals of Internal Medicine,* Sept. 15, 1998, Vol 129, pp. 495-500.
[5] Smith, supra note 4.
[6] Mandl et al., supra note 5.
[7] Charles Piller, "Web Mishap: Kids' Psychological Files Posted," *LA Times*, November 7, 2001.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] Frank Hayes, "Damage Control," *Computerworld*, July 16, 2001.
[12] "Inside the Industry – Eli Lilly: 'Inadvertently' Lists Prozac Patient's Email," *American Health Line*, July 5, 2001.
[13] Hayes, supra note 9.
[14] *American Health Line,* supra note 10.
[15] Hayes, supra note 9.
[16] *Id.*
[17] *Technology*, Friday, July 6, 200 (available at www.canoe.ca/MoneyNewsTechnology/jul6_lillyprivacy-ap.html).
[18] *Id.*
[19] Brubaker, supra note 1.
[20] Letter from James Novello, Staff Counsel, Department of Managed Healthcare to Ellen Leonard, Senior Counsel, Kaiser Foundation Health Plan, Inc. (Dec. 27, 2000) (available at http://www.dmhc.ca.gov/library/enforcements/kaiserinc/001227.pdf)
[21] *Id.*
[22] Bob Sullivan, "Health site exposed customer info," MSNBC.com, May 25, 2001 (available at http://www.msnbc.com/news/578476.asp)
[23] In addition to the rule on privacy of medical records, a final rule has been issued setting standards for electronic healthcare transactions and for the codes to be used in those transactions. Proposed regulations have been published regarding standards for data security and e-signatures and for the assignment of unique identification numbers for plans, providers and others. Proposed regulations relating to other HIPAA mandated standards are in development.
[24] *See* HIPAA §§ 160.102 (General Administrative Requirements - General Provisions – Applicability); 164.501 (Security and Privacy – Privacy of Individually Identifiable Health Information – Definitions).
[25] *See* HIPAA § 164.501 (Security and Privacy – Privacy of Individually Identifiable Health Information – Definitions).
[26] A covered entity may, however, de-identify the information in order to use it. PHI is considered de-identified if it does not identify the individual to whom the information relates and if there is no reasonable basis to believe that the information can be used to identify the individual.
[27] *See* HIPAA §§ 164.502(b) (Security and Privacy – Privacy of Individually Identifiable Health Information –Uses and disclosures of protected health information); 164.514(d) (Security and Privacy – Privacy of Individually Identifiable Health Information – Other requirements relating to uses and disclosures of protected health information).
[28] *See* HIPAA §§ 164.502(b) (Security and Privacy – Privacy of Individually Identifiable Health Information –Uses and disclosures of protected health information); 164.514(d) (Security and Privacy – Privacy of Individually Identifiable Health Information – Other requirements relating to uses and disclosures of protected health information).
[29] *Id.*
[30] "Privacy Rule will Force Major Changes in Handling of Patient Information," *American Health Lawyer's News*, Vol. 5, No. 2 (Feb. 2001), p. 9.
[31] Pub. L. 101-336, 42 U.S.C. § 12101.
[32] American Medical Association, Code of Medical Ethics: Current Opinions with Annotations Opinions 5.04-.07 (1998)
[33] AMA Code, Opinion 5.05.
[34] AMA Code, Opinion 5.07.