CCH Healthcare Compliance LETTER

Volume 6, Issue 1 www.cchgroup.com January 20, 2003

NCVHS: HIPAA "frustration, anxiety, fear and anger" persist

by Gordon R. Shea, J.D.

The National Committee on Vital and Health Statistics (NCVHS) is again warning Department of Health and Human Services (HHS) Secretary Tommy Thompson that Privacy Rule compliance is far from what it should be as the compliance date for the Rule draws ever closer. The warning is a follow-up on correspondence that the NCVHS sent to Thompson in September of last year concerning Privacy Rule readiness in the nation's healthcare system.

In a November 25, 2002 letter to Thompson on behalf of the NCVHS, Chairperson John R. Lumpkin warns that "[t]here is an extremely high level of confusion, misunderstanding, frustration, anxiety, fear, and anger as the April 14, 2003" date nears on which entities covered by the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) must begin following administrative mandates to protect the confidentiality of patient health information.

OCR "inadequate?" In the previous letter, NCVHS reported that, after a hearing in Boston — the first in a series of field hearings that the Committee was scheduled to conduct — testimony showed an "overall" lack of Privacy Rule readiness. Testimony also suggested "high levels of confusion and frustration" with the Privacy Rule, and a concomitant "likelihood of widespread disruption" in the nation's health care system. At that time, NCVHS reported that it was "so troubled by the Boston testimony" that it felt compelled to report the disruption to Thompson before continuing on with scheduled hearings in Baltimore and Salt Lake City.

Now that NCVHS has completed the Baltimore and Salt Lake City sessions, it reported that "[t]he tenor of the testimony at the two later hearings was virtually identical to that which we described in our letter after the Boston hearing."

That "tenor," NCVHS reports, includes considerable dissatisfaction with the role that the federal government has played in Privacy Rule implementation. While most organizations that presented testimony at the NCVHS's final field hearings reported that the Bush administration's August 2002 changes to the Privacy Rule were "viewed positively," the organizations also "widely viewed" HHS's Office of Civil Rights (OCR) as "not providing adequate guidance and technical assistance." OCR is the government entity responsible for upcoming HIPAA enforcement.

Specifically, according to the latest NCVHS letter, many "witnesses lamented the lack of model notices of privacy practices, acknowledgments, authorizations, and other forms. Many witnesses also complained that" the basic "general guidance" that most of them were being offered by swarms of high-priced consultants "was of limited value because of their special industry or professional circumstances. Witnesses conveyed a great sense of frustration that they could not obtain any clarifications from OCR or

Letters to the Editor

The CCH Healthcare Compliance team welcomes comments regarding articles published in the CCH Healthcare Compliance Letter. Send comments to Jeff Reinholtz, Managing Editor at reinholj@cch.com. For more information about the CCH Healthcare Compliance Portfolio visit our online store at http://health.cch.com.

answers to the questions they submitted via OCR's website."

"Let them catch me." HIPAA's preemption provisions — under which covered entities must determine whether or not state privacy laws are more strict than the federal Privacy Rule and must make this determination for each jurisdiction in which they operate — seem to be a particular sore spot. "A large number of witnesses," NCVHS reported, "said that issues of preemption made compliance" with the Privacy Rule "much more difficult, costly, and complicated." Several witnesses reported that the preemption analyses they were expected to complete "are often lengthy documents, expensive to research, highly technical, and not binding on any enforcement agency or the courts." NCVHS also warned of a lack of "national coordination on the issue of preemption."

Worse, NCVHS reports, "[s]everal witnesses estimated that well below half of all small providers had made any effort to comply with the Privacy Rule, and some have no intent to do so." One witness, according to the NCVHS letter, "reported that some rural providers have given up on compliance and adopted the position that 'I can't do this; let them catch me.'" Another witness, who represents an oncology provider, told the committee "that the difficulty and expense of HIPAA compliance had caused her practice to abandon the use of electronic billing and to go back to paper claims to avoid being a covered entity."

"Dire" expertise shortage. "Even more troubling," the NCVHS letter continues, "are the potential adverse effects on the health care system. Some witnesses said that some Medicaid and other safety net providers may drop out of the system of providing care to indigent patients because they cannot afford to absorb the costs of complying with the Privacy Rule, and there is no way to pass along the costs." Concerns about large-scale breakdowns in the healthcare system resulting from poor Privacy Rule compliance, the Committee said, also extend to "the need for education and training" of healthcare workers. Although "millions of health care workers will need to be trained in the next few months" about the Privacy Rule, NCVHS says, "there is a dire shortage of expertise, materials, and funding. Overwhelmingly, witnesses said that generic training will not work; to be successful it must be customized by industry, entity, and job description." Some witnesses "reported that the fear of violating HIPAA already has resulted in negative health outcomes, including providers refusing to share patient medical information that would be helpful in treating another patient and a decline in mandatory or permissive reporting of essential health data to public health agencies, tumor registries, and other entities."

Interestingly, the NCVHS letter focuses on the perceptions of the covered entities from which it took testimony. It does not attempt to evaluate the reasonableness or rationality of the witness from whom it heard. At least some of the concerns raised by witnesses and communicated by the NCVHS seem somewhat at odds with HIPAA compliance measures that have already been announced.

For example, NCVHS reported that "[f]ears surrounding HIPAA...featured prominently in the testimony. Witnesses were very concerned about the possibility of overzealous enforcement by OCR as well as private lawsuits, both of which were viewed as costly to defend." Such fears seem contradicted by the government's actions thus far. For example, on October 15, 2002, HHS issued a news release stating that the agency's Centers for Medicare and Medicaid Services (CMS) will be responsible for HIPAA's transactions and code sets provisions. Rather than enforcing those provisions with an iron hand, CMS "will focus on obtaining voluntary compliance through technical assistance. The process will be primarily complaint driven and will consist of progressive steps that will provide opportunities to demonstrate compliance or submit a corrective action plan."

A copy of the NCVHS letter is available at http://ncvhs.hhs.gov/021125lt.htm. ■

CCH Chicago Bureau, Jan. 10, 2003

Where's the Security Rule?

Despite recent rumors that the Department of Health and Human Services would issue HIPAA's Security Rule for Federal Register publication on December 27, 2002, the Security Rule has not yet been released. When it is, the staff analysts at CCH INCORPORATED will bring you full coverage of the Rule and its impact.

CCH Healthcare Compliance Letter

Managing Editor
Jeff Reinholtz, J.D.

Coordinating Editors
Raio G. Krishnayya, J.D.
Gordon R. Shea, J.D.
Geraldine S. Stroka, J.D., R.N.
Judith A. Tichenor, J.D., LCSW

CCH Washington Bureau
HHS, CMS–Brendan Frost
DOJ, FTC–Peter Feltman
Capitol Hill–Catherine Hubbard, Jeff Carlson
White House–Paula Cruickshank

Developmental Editors
Patrick J. Osborne
Sharon Sofinski

Designer
Laila Gaidulis

Comments from readers are welcome and should be directed to Jeff Reinholtz at REINHOLJ@CCH.COM, Tel. 847-267-7316, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Healthcare Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Healthcare Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

OIG nets billions cracking down on fraud and waste

by Geraldine S. Stroka, J.D., R.N.

The Office of Inspector General's (OIG's) semiannual report to Congress is a must read for it not only highlights the many Department of Health and Human Services (HHS) program area achievements in 2002, but also discloses HHS's future focus. Although the majority of the report concerns its work alongside its sister agency, the Centers for Medicare and Medicaid Services (CMS), it also details other efforts in conjunction with other government agencies.

OIG's achievements. For fiscal year 2002, the OIG reported that it saved $21 billion dollars (with $19.9 billion due to better utilization of government funds), $426 million in audit disallowances and $1.49 billion in investigative receivables. In the next few months, OIG will issue a final compliance guidance for pharmaceutical manufacturers and it will be reporting on prescription drug costs and state rebate programs under the Medicaid program.

Safe harbor status. In Appendix G, OIG presented the status of the proposals it received as a result of its annual solicitation for modifying existing safe harbors. Appendix G also illustrates the OIG's rationale in accepting or denying these proposals. The OIG is developing a proposed rule for certain fee-for-service arrangements between federally qualified health centers and other providers. Also, new safe harbors being considered include: (1) a safe harbor similar to the self-referral exceptions created by CMS regulations, including compliance training, incidental benefits, and (2) a safe harbor for isolated transactions matching the exception in the physicians self-referral statute. Other new safe harbors as well as modifications to existing safe harbors are currently under review. ■

Office of Inspector General, Semiannual Report to Congress (April-September 2002), Dec. 11, 2002, ¶154,108

DHHS publishes regulatory agenda and seeks industry input

by Geraldine S. Stroka J. D., R.N.

The Department of Health and Human Services (DHHS) has published its semiannual regulatory agenda. As part of this publication, DHHS has requested members of the healthcare industry to submit input into the rulemaking process. The agenda and request is directed with the intended result to issue advance notices of proposed rulemaking and final rules within the next 12 months.

"For fiscal year 2002, the OIG reported that it saved $21 billion dollars (with $19.9 billion due to better utilization of government funds)"

Fraud and abuse. Although much of the activities of The Centers for Medicare and Medicaid Services (CMS) is of interest to all compliance officers, there are several rules, in different stages of drafting that require industry input. According to the agenda, CMS has developed a proposed rule for a safe harbor arrangement involving federally qualified health centers and providers. Final rules under development include: (1) the shared risk exception to safe harbor provisions, (2) Stark II-Phase II or as it is officially known, "Physicians' Referrals to Health Care Entities with Which They have Financial Relationships- Phase II", and (3) The Emergency Medical Treatment and Labor Act.

Importance. The agenda is an excellent source for the following information about each of the rules presented: (1) priority, (2) legal authority, (3) citation, (4) legal deadline, and (5) an abstract of the rule. In addition, it lists any actions taken on the rule, the dates of these actions and their citations, as well as the agency contact for each rule. ■

HHS-Semiannual Regulatory Agenda, 67 FR 74492, Dec. 9, 2002, ¶362,028

Maintaining Compliance While Promoting Medical and Clinical Research: Conflict of Interest Issues

by Theodore J. Sanford Jr., MD; Leslie H. Kamil MS, JD; and Edward B. Goldman, JD

The recent federal suspension of medical research programs at several well-known academic medical centers has caused many institutions to review, revise, or create compliance policies for their research programs. Most of the more recent issues centered on informed consent or authorization of research participants. Institutions cannot afford the risk of losing public confidence, a tarnished research reputation, or suspension of their research efforts.

Conflict of Interest. COI refers to situations in which a researcher may compromise or appear to compromise his or her objectivity while conducting research. This lack of objectivity frequently, but not always, involves a financial interest for the researcher. A researcher's impartiality can extend to the protocol, design, data collection, analysis, interpretation, and reporting as well as the hiring of staff and acquisition of equipment and materials. A COI can also result from the various "hats" a faculty/researcher wears within an integrated health system. In addition to financial conflicts there is always the potential for conflict between the investigator role as a physician and his role as a researcher. A physician/researcher can also receive financial incentives as a network provider in the health system's HMO while conducting research on a participant who is a member of that HMO. In addition to the individual conflict, this situation also creates conflicts for the health system.

Research participants should be comfortable that the medical school will manage COI, that they will be notified in writing of investigator COI, and that investigator(s) of a study in which they are enrolled comply with the federal guidelines[1,2,3] for participants in clinical trials and also guidelines from the Association of American Medical Colleges (AAMC),[4] International Committee of Medical Journal Editors (ICMJE),[5] and the Declaration of Helsinki,[6] and that these researchers do not have a COI with the industry sponsor.

The problem of non-compliance of medical researchers was delineated in a recent article that looked at the compliance of research investigators at 108 academic medical centers with regard to investigator participation in guidelines from the ICMJE (2002) concerning study design, access to all trial data, and control over publication of industry sponsored research.[7] Of the 108 medical centers participating in multi-center trials, only one percent of the agreements between researchers and the sponsoring organization adhered to the ICMJE guidelines on investigator access to all data; ten percent were in compliance with guidelines for study design and data collections; and only sixteen percent reported that IRBs routinely reviewed agreements between investigators and industry sponsors. This study concluded that academic institutions "rarely ensure that their investigators" have full and unimpeded access to all trial data, have a right to publish their own findings, or even have input into the study design of protocols.

The Public Health Service requires that grantee institutions have COI policies in place.[8] The statement says, "(E)ach institution receiving financial support must have written policy guidelines on COI and the avoidance thereof." It should be noted that perceived conflicts are as important to identify and manage as are the real conflicts. Public opinion of the community and the granting agencies can impact future funding.

Conflicts are not necessarily bad, but the lack of policies that provide guidance on identification, disclosure, sanctions, and management of conflicts can create significant liability for both the researcher and the institution. Management of conflicts includes monitoring, limiting activity, cessation of the project or discontinuation of a faculty's/researcher's involvement frequently through the substitution of non-conflicted personnel.

Implementation of the federal COI policies creates a challenging opportunity for the institutional compliance officer. First, he or she is charged with overseeing the faculty and satisfying all applicable laws and regulations. This is an enormous cost to the institution in terms of money as well as faculty morale. Compliance with these requirements requires additional faculty and staff to satisfy the paperwork and monitoring requirements specified in the laws, regulations, and resultant institutional policies. Compliance officers cannot make institutions compliant. It is the responsibility of each faculty member, researcher, and their related staff.

Recommendations. We make the following recommendations:

1. Develop and implement detailed research compliance programs. Although physician and researcher auditing and monitoring of the privacy regulations can be conducted as part of the institutional process, a separate process of auditing and monitoring must be established for COI issues.

2. The IRB or other regulatory body responsible for identifying and managing COI should consider assigning a study coordinator to each research project. Each coordinator can be assigned either full-time with one study or part-time with more than one study. Determine:

- if the principal investigator should be allowed to hire a study coordinator or if there should be a pool of study coordinators, independently hired and supervised by a disinterested party, that are assigned to project.
- the method of funding for and the allocation of expense for the independent study coordinator; if funding is central and not allocated to a specific research project, the likelihood of a COI will be reduced.

3. Educate and train:

- Administrative staff in the research office(s) should be well trained in the laws and regulations and who (and how) to contact for guidance. Training may require bringing in an outside consultant or sending the administrators to an appropriate course(s). Extensive education and training is imperative.
- Study coordinators should be educated in specific agency regulations. Training can be done by existing administrative staff or outside staff. The end goal is that extensive education and training must be achieved. Staff must be able to answer their constituents correctly.
- Researchers training is available from the Office of Human Research Protection (OHRP). The institution must make these training sessions convenient to the researchers and provide the researcher with accessibility to a designated person for more detailed training if desired.

4. Appoint a research representative to the institutional privacy committee.

5. Consider designating a Research Compliance/Privacy Officer specific to research. This position would be the primary contact for privacy and research questions.

6. Develop policies that assist researchers in identifying conflicts and privacy issues. The COI policies must provide a mechanism for annual disclosure and retrieval of disclosed conflict issues; specific guidance on the types of and limits on outside activities that are permitted; sanctions for breach of policies; and establishment of a committee to review each conflict and provide guidelines on management. The privacy policies must specify access, authentication, minimum necessary, use and disclosure guidelines and sanctions for breach of the policies.

7. Make sure all researchers, whether clinical or laboratory, understand that they must provide full and complete disclosure of any perceived and actual conflicts to the institution and to participants, such as industry sponsored research. Consider incorporating COI disclosure into the IRB process.

8. Consider conducting an initial assessment of research efforts about to commence to establish a benchmark for improvement. If one decides to engage an outside company or to internally assess current research compliance, discuss this with your attorney prior to initiating the assessment.

9. Establish an effective communication mechanism for the timely and accurate dissemination of information to all faculty, researchers, and staff involved in research. Consider development of a website for dissemination of information and for publishing resources available for researchers. For example, the FDA's website can be found at www.fda.gov/oc/gcp/ or the National Institutes of Health (NIH) can be found at www.grants1.nih.gov/grants/guide/notice-files/NOT-OD-01-053.html.

10. Establish a website for easy access to laws, regulations and internal policies.

11. Establish a committee on COI that is part of the Medical and Clinical Research entity. This committee should have contact with the facility IRB so that any identified conflicts involving research can be sent to the IRB to be sure that the research informed consent process and documentation include the appropriate COI disclosures.

12. Researchers should review and comply with federal regulations on COI and not have inappropriate equity position in any company sponsoring trials, or buy, sell, or hold stock in those companies as defined in the federal regulations.

13. Institutions should reassess, review, and implement the guidelines from the AAMC and ICMJE, FDA, Public Health Service (PHS), NIH, and National Science Foundation (NSF).

Theodore J. Sanford Jr., MD, is the Compliance Officer for University of Michigan Health System; Leslie H. Kamil MS, JD, is the Deputy Compliance Officer and Privacy Officer, University of Michigan Health System; and Edward B. Goldman, JD, is Assistant General Counsel, Office of the General Counsel, University of Michigan.

[1] Public Health Service: 42 CFR Section 50.601, 45 CFR Section 94.1, 45 CFR 680: October 1, 1995.

[2] National Institutes of Heath: Developing Sponsored Research Agreements. Considerations for Recipients of NIH grants and Contracts. 59 FR 55673. November 8, 1994.

[3] FDA: Conflicts of Interest Regulations. 21 CFR Part 54. February 2, 1999.

[4] AAMC Guidelines for Dealing with Faculty Conflicts of Commitment and Conflicts of Interest in Research, February 22, 1990.

[5] International Committee of Medical Journal Editors. Sponsorship, authorship and accountability. N Engl J Med 2002:346:290-92.

[6] Declaration of Helsinki – Ethical Principles for Medical research Involving Human Subjects. June 1964. www.wma.net.

[7] A National Survey of Provisions in Clinical-Trial Agreements between Medical Schools and Industry Sponsors. N Engl J Med 2002: 347:1335-41.

[8] National Science Foundation Investigator Financial Disclosure Policy. 60 FR 35820. October 1, 1995.

[9] Taskforce on Financial Conflicts of Interest in Clinical Research. Protecting subjects, preserving trust, promoting progress-policy and guidelines for the oversight of individual financial interests in human subjects research. Washington, D.C.: Association of American Medical Colleges, December 2001.

For security's sake: homeland security trumps HIPAA protections

by Raio G. Krishnayya, J.D.

After President Bush signed the Homeland Security Act of 2002 into law on November 25, 2002, a major crossover occurred between homeland security and medical privacy—an otherwise unlikely pairing—resulting in controversy. Specifically, the Homeland Security Act has paved the way for "data-mining," which if implemented would test historical protections of privacy, including notions of medical privacy. Furthermore, the Act allows healthcare and biotechnology entities to become prominent players in homeland security by obtaining federal grant money for research into technologies designed for counter terrorist measures, including bioterrorism.

The threat. The issue of bioterrorism gained prominent public concern after the anthrax attacks hit the United States in early October 2001. Prior to the highly publicized anthrax attacks, the U.S. government had always been concerned with bioterrorist attacks, the emphasis was primarily in developing a responsive plan to such attacks.

The events of 2001, however, coupled with the fact that no criminal prosecution has yet occurred after the anthrax attacks sparked public demands that the government do more to protect its citizens from future attacks. A consensus was drawn at the highest levels of government that the United States had to take preemptive measures to detect and foil future attacks. In part, the Homeland Security Act of 2002 is the vehicle for such measures.

As a practical matter, a change in policy is reflected by a change in methodology. Therefore, how would an entity charged with preventing future attacks be able to obtain information in a timely fashion to do just that? Enter data-mining.

Data-mining. The premise of data-mining is that the electronic world contains trillions of bits of information; organizations that maintain electronic records keep this data in data warehouses to protect and maintain the information. However, the vast amount of data makes analysis of the data for statistical trends virtually impossible without data-mining techniques.

Data-mining experts are quick to caution that while data-mining results can provide statistical predictions about relationships, it cannot identify a causal connection between the events quantified and the predicted outcomes.

Nevertheless, the power of data-mining makes the government's interest and subsequent codification for its use obvious. With regard to bioterrorism, those same Department analysts could search for trends in medical treatment data to determine the statistical probability that a bioterrorism attack has occurred. In theory, analysts could target potential hot spots that indicate a high probability of an attack. Subsequently the Department analysts could dispatch Centers for Disease Control and Prevention investigators to verify whether an attack has occurred and coordinate with public health agencies to quickly isolate the problem. Although this is a powerful method for detecting and deterring such an attack, the data-mining measure has been strongly criticized.

The language of the Homeland Security Act that governs data-mining appears to be vague. Under Title II of the Act, entitled "Information Analysis and Infrastructure Protection," the following are listed as some of the main objectives regarding information analysis:

> (1) To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—
> (A) identify and assess the nature and scope of terrorist threats to the homeland;
> (B) detect and identify threats of terrorism against the United States; and
> (C) understand such threats in light of actual and potential vulnerabilities of the homeland.

Thus, with such broad objectives, the Act has provided the Department of Homeland Security the ability to conduct data-mining among its arsenal of intelligence capabilities. The data-mining provision simply states that the Department must:

> (14) (E)stablish and utilize, in conjunction with the chief information officer of the Department, a secure communications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

The language of paragraph one coupled with paragraph fourteen has sparked criticism by civil rights advocacy groups.

Privacy concerns. Opponents of the data-mining provisions of the Act have argued that this provision is the successor to a line of statutory enactments designed to erode privacy. Most notably, the Center for Democracy & Technology (CDT) has published a statement addressing the data-mining aspects of the Homeland Security Act.

The CDT's statement outlines the historical devolution of privacy, culminating with the Homeland Security Act. Beginning with the USA Patriot Act, the CDT's privacy analysis states that under the Patriot Act, law enforcement was entitled to gain access to electronic data, such as e-mails and other electronic records, without court order if the custodian of the electronic data reasonably believed that an emergency situation existed, resulting in imminent threat of harm. The CDT's statement continues by asserting that the Homeland Security Act removes the "imminent threat" requirement, allowing unfettered access to electronic data without court review.

Furthermore, the CDT detailed other data-mining initiatives by other governmental agencies, including the Defense

Advanced Research Projects Agency (DARPA). President Reagan's National Security Advisor, John M. Poindexter who initially introduced DARPA, has become its head and chief spokesperson. The aim of DARPA is to develop systems that would provide information about travel to high-risk areas, suspicious e-mails, nefarious financial transactions, and medical activities. The Homeland Security Act not only allows the Department access to technologies such as those developed by DARPA, but also requires the Department to pursue and utilize such technologies. See John Markoff, Pentagon Plans a Computer System That Would Peek at Personal Data of Americans, N.Y. Times, Nov. 9, 2002 at http://www.nytimes.com.

HIPAA. Many of the concerns voiced by opponents to the Homeland Security Act address not just general privacy concerns but specifically challenge the protections under the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule. The Privacy Rule prohibits uses and disclosures of protected health information to third parties without notice to the patient of his or her privacy rights and equally, importantly, the provider's privacy practices. The Rule further requires providers to make a "good faith" effort to procure a patient's written acknowledgement of the privacy rights and practices.

While many healthcare and medical research entities are well aware of HIPAA, what is less known is the impact that provisions like the data-mining clause have on an entity's efforts at HIPAA compliance. Consider, based on the previously described scenario, what if the Department could accew otherwise protected information? What would be the HIPAA liability to a healthcare or research entity? Furthermore, what requirements does such a scheme impose on entities in terms of providing notice about privacy rights and practices?

Recall that violations of the Privacy Rule could result in an entity facing severe penalties depending on the level of intent associated with the privacy breach. For example, if an entity intended to sell or transfer the data for commercial gain or to cause malicious harm, the attached penalty could be up to ten years in prison or a fine of up to $250,000. But that is unlikely to be the case with regard to the scenario just illustrated.

In the scenario above, and absent any notice that a patient's medical treatment information could be data-mined, an entity could face a penalty of up to one year of imprisonment or up to $50,000 per incident. In the above-described scenario, data-mining would not only encompass retrieval of one record but of thousands of records, each carrying the possibility of separate, consecutive violations.

Privacy safety nets. Although the scenario detailed above seems bleak, proponents of the data-mining provision would argue that both HIPAA and the Homeland Security Act provide safeguards to prevent the catastrophe that could occur. Three separate provisions between the two statutes would seem most relevant.

The Homeland Security Act creates a new position, the privacy officer. The Act assigns five major responsibilities to the privacy officer. The responsibilities mainly consist of "assuring" that the technologies employed by the Department do not "erode privacy protections relating to use, collection, and disclosure of personal information." Furthermore, the Act requires the privacy officer to maintain departmental compliance with the Privacy Act of 1974. The privacy officer is also required to conduct a privacy assessment, which is to include the type of personal information collected and the number of people affected. The last provision requires the privacy officer to submit an annual report to Congress detailing the Department's privacy practices, including information about privacy complaints. The duties of the privacy officer seem routine and reassuring that breaches in privacy protections will not occur.

However, as is often the case, what is not said is equally as important as what was said. Interestingly, the Act makes no mention of exactly how the privacy officer is to "assure" that Department practices do not "erode privacy protections." Also absent are any provisions that grant the privacy officer the power to suspend or terminate any practices that are found to "erode privacy protections." In other words, the Act is unclear about what specific enforcement options the privacy officer has to guarantee such assurances.

The privacy assessment, while designed to provide an accounting of the Department's privacy practices, includes no guarantee that any discovery of violations would result in review or investigation or any such redress. Clearly, the delineated enforcement power of the privacy officer under this scheme is the ability to report violations to Congress. However, by the time the annual report is submitted and Congress would have an opportunity to act, the privacy violation would have already occurred and the damage done.

The other provision of the Homeland Security Act that comes into play appears just before the clause establishing the privacy officer. That provision, Section 221, imposes four requirements regarding sharing of information.

- To limit the redissemination of information to ensure that it is not used for an unauthorized purpose;
- Secure and maintain confidentiality of information;
- Maintain data integrity by removing obsolete or erroneous names and information in a timely manner; and
- Protecting individuals' constitutional and statutory rights.

This begs the question, however, of what are the constitutional and statutory rights that bind the Department's privacy practices? Returning to the HIPAA Privacy Rule for an answer, consider the protective provision for treatment information. The main requirements of the final Privacy Rule issued in August 2002 although universally known contains less noted exceptions that may ultimately answer the question.

Pursuant to §164.512 of the Privacy Rule, entitled "Uses and disclosures for which an authorization or opportunity to agree or object is not required," the healthcare entity that would provide the treatment information for data-mining purposes would presumably have safe haven from liability. Paragraph "(f)(3)" allows an entity to disclose otherwise

protected information in order to identify individuals suspected to be victims of crimes. Paragraph "(f)(3)," however, requires that the disclosure either occur upon assent by the individual suspected of being the victim or if the person is incapacitated or an emergency condition exists, then three conditions must be satisfied.

First, the law enforcement agency conducting the investigation must establish that the crime investigated was committed by someone other than the victim and that the treatment information would not be used against the victim. Second, law enforcement would be required to demonstrate that the investigation would be materially and adversely affected by waiting for the individual's assent. Third, the healthcare entity must determine that disclosure is within the best interests of the individual.

Relating this back to the Department practice of data-mining for potential bioterrorism events, the Department (clearly a bioterrorist attack would constitute a criminal act for §164.512 purposes) would be required to establish all three requirements before conducting the data-mining. On the other hand, the Department could argue that it could not identify whether a treated patient was a victim of a bioterrorist attack without first analyzing the data — a cart and horse problem.

However, recall that the primary purpose of conducting data-mining analyses is to develop statistical models to identify the probability of a terrorist event such as a bioterrorist attack. In other words, the *modus operandi* is to gather *intelligence* and §164.512 paves the way for this type of operation.

Under subparagraph "(k)" of §164.512, there is a clause entitled, "National security and intelligence activities." The clause reads: "[a] covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. § 401, *et seq.*) and implementing authority."

The National Security Act has become the key to open otherwise locked doors in the name of national security. Section 442(b) of the National Sec urity Act, which authorizes intelligence gathering activities by "an appropriate official of the United States Government, acting within the scope of official duties... and in compliance with Federal law," would provide the healthcare entity, participating in a Department of Homeland Security data-mining survey, a possible exemption from HIPAA liability because arguably, the purpose of such data-mining is to gather intelligence. Thus both the Department and the entity would be free from HIPAA reprisal.

Conclusion. The concept of active data-mining treatment records for the existence of "unusual medical activity" may seem Orwellian. However, the existence of current surveillance programs such as the Federal Bureau of Investigation's Carnivore program and the research and development programs such as DARPA indicate that a picture of a world, dominated by a need for safety over privacy, are coming together. But the evolution of actual cases formed under such schemes will truly dictate how protected medical privacy is or just how wide-reaching the national security argument is.

Complete text of the Homeland Security Act may be found at http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.5005.enr:. A copy of President Bush's remarks at the signing of the Homeland Security Act may be found at http://www.whitehouse.gov/news/releases/2002/11/print/20021125-6.html. Information about data-mining can be found at the Two Crows Corporation by downloading their Free Data Mining Tutorial Booklet at http://www.twocrows.com/intro-dm.pdf. A copy of the Center For Democracy and Technology's statement regarding the Homeland Security Act can be found at http://www.cdt.org/security/homelandsecuritydept/021210cdt.shtml. A copy of the HIPAA Privacy Rule can be found at ¶100,915. ■

CCH Chicago Bureau, Jan. 9, 2003