Medical Privacy: At What Cost?

NEW PRIVACY REGULATIONS REQUIRE DOCTORS TO GET APPROVAL FROM PATIENTS FOR THE USE OF THEIR PERSONAL HEALTHCARE DATA.

Dr. Joe Fortuna

By Denise Myshko

WHILE QUESTIONS REMAIN ABOUT WHAT THIS ULTIMATELY WILL MEAN FOR CLINICAL RESEARCH AND THE INDUSTRY'S ACCESS TO DATA, ONE THING IS CERTAIN: AN EXTRA LAYER OF ADMINISTRATION HAS BEEN ADDED FOR EVERYONE.

Privacy has become a political hot potato in the healthcare industry as advances in technology have fueled fierce debate over medical record confidentiality. Earlier this year, after much political wrangling, a wide-ranging regulation to ensure confidentiality of personal health information was enacted. Even now huge differences in opinion exist, with some calling the regulation long overdue, while others consider it unworkable.

The Health Insurance Portability and Accountability Act (HIPAA) became law in August 1996. The primary intent of the legislation was to create portable health benefits — to protect individuals and family health benefits in the case of a job loss or change. HIPAA instructed Congress to enact legislation that would create standards protecting an individual's personal health information.

On the surface, the privacy protection rule is a step forward in patient rights. The regulation, however, is expected to make the research of new medicines more complex. The rule will require an additional layer of administration during clinical trials, and its impact could reach even further since virtually all the research necessary to demonstrate safety and efficacy of new medicines depends on data obtained from patients and providers.

Almost from the start, the privacy provision was controversial. When Congress failed to enact legislation by the deadline, the Department of Health and Human Services was charged with developing the privacy standards.

What HHS came up with — and what former president Bill Clinton approved just before leaving office last December — was a set of sweeping standards that require disclosure and patient consent for all paper-based, oral, and electronic health records — including routine use of healthcare information — where a person's identity can be known. The measure also established criminal and civil sanctions for the improper use or disclosure of personal health information.

After a short delay, President George W. Bush decided to allow the regulations to go forward. Although the final rule took affect April 13, 2001, organizations have until April 14, 2003, to comply (April 14, 2004, for small health plans).

When it comes to personal information that moves across hospitals, doctors' offices, insurers or third-party payers, and state lines, the country has relied on a patchwork of federal and state laws. Under pre-existing laws, personal health information could be distributed — without either notice or consent — for reasons that have nothing to do with a patient's medical treatment or healthcare reimbursement. Patient information held by a health plan may be passed on to a lender who may then deny the patient's application for a home mortgage or a credit card — or to an

employer who may use it in personnel decisions. The Privacy Rule establishes a federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new federal privacy standards.

The privacy regulation requires providers to get written consent before the collection, use, or disclosure of patient information for treatment, payment, or healthcare operations. The regulation also requires providers to get an individual's authorization before patient information can be disclosed for purposes other than treatment, payment, or healthcare operations.

Healthcare providers have a strong tradition of safeguarding private health information. But in today's world, the old system of paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the rule provides clear standards for all parties regarding protection of personal health information.

Consumer groups applaud the new regulation, however physician and industry organizations decry it as restrictive and unworkable. Trade groups such as the Health Care Leadership Council, the National Association of Health Underwriters, and the Health Insurance Association of America indicated that the measure could be disruptive and limit even routine communications with patients, as well as increase administrative costs.

Officials with HHS say the healthcare delivery system will actually experience a net savings. HHS projects that costs to comply with the privacy regulation will be $17.6 billion. The electronic claims regulation law of August 2000 has a 10-year projected savings of $29.9 billion. That law, also required by HIPAA, established standard formats for data content and for submitting electronic claims and other administrative health transactions.

But an analysis released in April 2001 by the Robert E. Nolan Company and sponsored by the Blue Cross Blue Shield Association found that HHS significantly understates the actual cost of the regulation. Nolan concludes that HHS failed to conduct a complete estimate of several significant cost elements and underestimated the impact of many others. The final privacy regulation is expected to cost more than $42.9 billion over five years to implement, according to this analysis. And the American Hospital Association estimates that hospitals alone may spend up to $20 billion over five years on information systems changes and upgrades.

IMPACT ON RESEARCH

The HHS regulation also sets standards for the use of medical information for research. The regulation requires that before using identifiable health information, the research study must be approved by an Institutional Review Board (IRB) and participants must give their informed consent.

The law also contains specific rules allowing for disclosure of patient information for medical research without consent or authorization, says John Bentivoglio, an attorney with the law firm of Arnold & Porter. Generally, the rules require approval by an IRB or privacy board, with detailed administrative and record-keeping requirements.

Mr. Bentivoglio says a healthcare provider, i.e., physician, hospital, etc., may not disclose information for research unless: (a) the individual provides written authorization for such disclosures; or (b) the disclosure fits in the narrowly crafted research provisions of the rule. Under the letter provisions, approval by an IRB or IRB-like entity is required and detailed administrative and record-keeping requirements must be followed.

All this will mean more security bells and whistles for the industry, says Natasha Leskovsek, an attorney in the law firm of Heller Ehrman. "Companies need to be more cautious about the type of disclosures, who has access, keeping a log of who has been able to see data that are not anonymous, limiting that access, and developing new language for informed consent."

The full impact of the new regulations, however, is not yet known, says Ms. Leskovsek, who before becoming a lawyer was a registered nurse. "The hospitals and the research clinics are just now beginning to do their audit to determine what they need to do for compliance."

According to industry experts, from a clinical research point of view, the regulations are going to have a fairly wide-ranging effect.

"The investigators are going to have to do their jobs very carefully," says Dr. Joe Fortuna, medical director at Dorland Sweeney Jones. "They are going to have to know the rules and pay attention to the rules at the beginning of the game and not afterwards. They are going to have to inform the patient and get opt-in information, and so forth."

Making matters even more confusing for the industry is that HHS could make changes to the final rule. An HHS guidance document issued in July 2001 suggested that changes might be made to help eliminate uncertainties. Changes that are likely to be made will allow physicians to call in prescriptions to pharmacies; permit providers to schedule appointments and surgery before obtaining consent for access to records; allow for communication with patients' families; and

Natasha Leskovsek

COMPANIES NEED TO BE MORE CAUTIOUS ABOUT THE TYPE OF DISCLOSURES, WHO HAS ACCESS, KEEPING A LOG OF WHO HAS BEEN ABLE TO SEE DATA THAT ARE NOT ANONYMOUS, LIMITING THAT ACCESS, AND DEVELOPING NEW LANGUAGE FOR INFORMED CONSENT.

exempt medical charts at hospital beds. So far, no changes have been suggested in terms of the privacy rule and its impact on research.

Healthcare industry groups, such as the Healthcare Leadership Council, a Washington-based organization that represents healthcare companies, have urged HHS to assess the rule and make any changes as quickly as possible. In a letter to HHS Secretary Tommy Thompson signed by healthcare companies and industry groups — the Pharmaceutical Research and Manufacturers Association of America (PhRMA) is among them — says: "Organizations impacted by the rule are poised to devote considerable resources to comply with the rule. It would be unfortunate if these resources were expended before organizations knew what modifications were to be made."

WHO CARRIES THE BURDEN?

IRBs have long been charged under the Common Rule — what the body of federal regulations governing the protection of human subjects in research is called — to protect the privacy of those who participate in clinical trials.

But with the advent of the HIPAA privacy rule, IRBs must bear burdens relating to patient privacy that are more onerous and more complicated than under the Common Rule, says Jean Paul Gagnon, Ph.D., director, public policy, at Aventis Pharmaceuticals. "HIPAA regulations will mandate extensive consideration, with detailed criteria and formal requirements, of privacy issues. It will take years for the clinical community and its attorneys to fully understand the implications. The challenge is that every research compliance officer, every IRB member, and every clinician must begin to reshape the processes and protocols to comply with the new law.

"The HIPAA rule requires a type of analysis never before conducted in a sustained and focused way by IRBs or similar bodies, and IRBs and their institutions must be prepared to undertake methods of analysis with which they may have little familiarity or competence," Dr. Gagnon says.

He says that research practices must be examined thoroughly, and ultimately on a clinical trial-by-clinical-trial basis, to identify the necessary protected health-information uses and informed consent forms. To comply with HIPAA, a full review will be needed of research practices of each research institution, of each IRB, and of each physician researcher; and policies, procedures and forms will need to be revised to comply with these detailed requirements. In the meantime, even in advance of a complete HIPAA compliance review, IRBs and researchers should consider carefully the transition provisions in the HIPAA regulations that will govern research studies already under way as of the HIPAA compliance date.

The burden of the privacy regulations also is on the individual physicians and the sites, says Dr. John Schrogie, VP, peri-approval research services, at Omnicare Clinical Research.

"From a trial perspective, as part of the informed consent process, patients are told that information is being collected as part of the study and a variety of people are going to have access to it," Dr. Schrogie says.

He adds that the privacy regulations could be one more obstacle for investigators to have to overcome, especially those in individual physician practices. Pharmaceutical sponsors and contract research companies like Omnicare, he says, will have to provide guidance and a template to help the sites and physician offices to maintain privacy.

"For us, this would be a one-time cost," Dr. Schrogie says. "We have to send out a package of information anyway with the regulatory documents, contractual agreements with the sites, etc. Potentially, part of the site qualification process that we go through might have one more step, namely evaluating whether the site has its HIPAA policy and procedure in place."

IS ACCESS TO DATA COMPROMISED?

A larger issue involves not informed consent in clinical trials, but the use of data, says Heidi Wagner, director of government affairs, at Genentech Inc.

Informed consent is important for clinical trials, she says. But real the question — to which no one yet has the answer — is what the disclosure requirements will mean in terms of access to data? The industry uses and reviews clinical trial data often retrospectively, for example, for epidemiologic studies, health outcomes, and other studies that look for trends in diseases and treatments, etc. Those in the industry are concerned that providers (hospitals and doctors), because of high administrative costs and liability concerns, will not want to disclose this information for research purposes. In these cases, it is not always possible to get informed consent.

"We're very supportive of ensuring confidentiality of the data in research," Ms. Wagner says. "We take confidentiality of patient information incredibly seriously. But also of importance, is that data, and information forms so much of the basis of our early stages of research that we do need access to fulfill our mission of researching and developing life-saving technologies."

Ms. Wagner continues: "When it comes to the HHS rule, we can certainly meet the various requirements. But the way that the rule is written creates several concerns. The primary concern is that the rule imposes most of the obligations and the burdens when it comes to disclosure of

Dr. Jean Paul Gagnon

IT WILL TAKE YEARS FOR THE CLINICAL COMMUNITY AND ITS ATTORNEYS TO FULLY UNDERSTAND THE IMPLICATIONS. THE CHALLENGE IS THAT EVERY RESEARCH COMPLIANCE OFFICER, EVERY IRB MEMBER, AND EVERY CLINICIAN MUST BEGIN TO RESHAPE THE PROCESSES AND PROTOCOLS TO COMPLY WITH THE NEW LAW.

patient health information on providers. Hospitals, doctors offices, and health plans are often the sources of our information. They are the ones who have information about patients, to whom we have to have access to pursue our research. The way the rule is written may provide a disincentive for them to continue partnering with us. It's not that we can't meet the letter of the rule. It's that we think the incentives have been misplaced."

Access to data was a concern expressed by PhRMA before the privacy regulation became law. In a February 2000 letter to the HHS, PhRMA officials expressed concern that the proposed regulations would have an adverse impact on the industry's efforts to discover and research new medicines. At that time, PhRMA officials said in a statement that the regulations are likely to reduce the willingness of health plans and providers to participate in research because of the civil and criminal penalties involved. A spokeswoman for PhRMA would not comment for this story.

Dr. Schrogie says the burden again is on the site. "If a site is participating in an electronic data

Bonnie Brescia

PEOPLE ARE VERY CONCERNED ABOUT THEIR HEALTH AND INSURANCE INFORMATION GETTING OUT. THEY CARE MORE ABOUT THAT THAN THEY DO ABOUT THEIR CREDIT CARD INFORMATION.

GETTING PERSONAL

PERSONAL HEALTH INFORMATION OF CONCERN. Survey after survey of patients and consumers revealed that there is concern about the use of personal health information. In fact, lack of privacy significantly diminishes access to quality healthcare, say officials with the Health Privacy Project, Institute for Health Care Research and Policy, at Georgetown University. Many worry that the disclosure of medical records could result in the denial of insurance or loss of employment and, as a result, some patients withhold information from their doctors or avoid care altogether.

During the past 10 years, surveys indicate that consumers show increasing concern about the confidentiality of medical records. For example, a Gallup survey for MedicAlert Foundation in November 2000 found that 55% of respondents would not trust an insurance company or managed-care organization to keep personal information secure. Another survey by Princeton Survey Research Associates for the California HealthCare Foundation in January 1999 found that one in five adults believes that providers, insurers, or employers have improperly disclosed medical information. And that, one in seven adults has done something out of the ordinary — withhold information from doctors, provide inaccurate information, doctor hop, or pay out of pocket — to keep personal medical information confidential.

TECHNOLOGY FUELS THE PRIVACY DEBATE. Technology, especially the Internet, and genetic research have helped to fuel concerns. Managed care and integrated health systems have led to the development of large databases of personal health information that can be linked. A November 2000 survey by Pew Internet and America Life Project found that 85% of respondents fear that insurance companies might change coverage after online information was accessed. A September 2000 survey by the California HealthCare Foundation and the Internet Healthcare Coalition found that 76% of online users in good health are concerned that their health insurers will use personal health information to limit or affect coverage. And 60% are concerned that their employer will use health information provided online to limit job opportunities or affect job status.

CONSUMER FEARS, NOT UNFOUNDED. While these results may appear to be extreme, consumer fears are not completely unfounded. Life insurance and healthcare companies generally use personal health information in underwriting. In February 2001, the Equal Employment Opportunity Commission filed its first lawsuit challenging the use of genetic testing by employers. The suit charged Burlington Northern and Santa Fe Railway with conducting genetic testing — secretly and without consent — on employees who filed workers' compensation claims for carpal tunnel syndrome. Some studies have purported a genetic predisposition for carpal tunnel syndrome. This would have given the employer support to deny benefits, claiming the injury as not work-related. The company quickly responded, saying it would stop such testing.

PROTECTING PATIENT'S PRIVACY

Each time a patient sees a doctor, is admitted to a hospital, goes to a pharmacist, or sends a claim to a health plan, a record is made of their confidential health information. In the past, family doctors and other healthcare providers protected the confidentiality of those records by sealing them away in file cabinets and refusing to reveal them to anyone else. Today, the use and disclosure of this information is protected by a patchwork of state laws, leaving gaps in the protection of patients' privacy and confidentiality.

Congress recognized the need for national patient record privacy standards in 1996 when it enacted the Health Insurance Portability and Accountability Act (HIPAA). The law included provisions designed to save money for healthcare businesses by encouraging electronic transactions, but it also required new safeguards to protect the security and confidentiality of that information. The law gave Congress until August 21, 1999, to pass comprehensive health privacy legislation. When Congress did not enact such legislation after three years, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

In November 1999, HHS published proposed regulations to guarantee patients new rights and protections against the misuse or disclosure of their health records. During an extended comment period, HHS received more than 52,000 communications from the public. In December 2000, HHS issued a final rule that made significant changes to address issues raised by the comments. President George W. Bush allowed the rule to take effect April 14, 2001, as scheduled, and make appropriate changes during the next year to clarify the requirements and correct potential problems that could threaten access to or quality of care. On July 6, 2001, HHS issued its first set of guidance to answer common questions and clarify confusion about the final rule's provisions.

COMPLIANCE SCHEDULE. The final rule took effect April 14, 2001. As required by the HIPAA law, most covered entities have two full years — until April 14, 2003 — to comply with the final rule's provisions. The law gives HHS the authority to make appropriate changes to the rule prior to the compliance date.

As required by HIPAA, the final regulation covers health plans, healthcare clearinghouses, and those healthcare providers who conduct certain financial and administrative transactions (i.e., billing and funds transfers) electronically. All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

PATIENT RIGHTS. Under the final rule, patients have significant new rights to understand and control how their health information is used.

- PATIENT EDUCATION ON PRIVACY PROTECTIONS. Providers and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information.
- ENSURING PATIENT ACCESS TO THEIR MEDICAL RECORDS. Patients will be able to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients.
- RECEIVING PATIENT CONSENT BEFORE DATA ARE RELEASED. Healthcare providers who see patients will be required to obtain patient consent before sharing their information for treatment, payment, and healthcare operations. In addition, separate patient authorization must be obtained for non-routine disclosures and most non-healthcare purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.
- PROVIDING RECOURSE IF PRIVACY PROTECTIONS ARE VIOLATED. People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule.

BOUNDARIES ON MEDICAL RECORD USE AND RELEASE. With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes.

- ENSURING THAT HEALTH INFORMATION IS NOT USED FOR NON-HEALTH PURPOSES. Health information covered by the rule generally may not be used for purposes not related to healthcare — such as disclosures to employers to make personnel decisions, or to financial institutions — without explicit authorization from the individual.
- PROVIDING THE MINIMUM AMOUNT OF INFORMATION NECESSARY. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes.

SECURITY STANDARDS. The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. Covered entities generally will have to:

- ADOPT WRITTEN PRIVACY PROCEDURES. These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed.
- TRAIN EMPLOYEES AND DESIGNATE A PRIVACY OFFICER. Entities will need to train their employees in privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

Information about the regulations is available at hhs.gov/-ocr/hipaa.

capture program, patients need to be notified that they are participating in the program and that their data will be aggregated for other purposes. Patients need to know that their data will be part of a pool and they need to agree or disagree to that."

Officials with HHS don't believe that medical research will be hindered by the rule, saying the rule provides patients participating in research more protection and therefore, more incentive to participate. They concede that some providers might decide to limit access to personal health information because of the disclosure requirements, but they believe few will do so.

The disclosure requirements will not only impact access to historic patient data, but could also affect access to such things as tissue samples, tumor samples, DNA information, says Bonnie Brescia, president of BBK Healthcare Inc.

She says this could lead to a subset of the industry that will create registries and databanks of people who are willing to have their information available for use.

"We saw it with stem cells and cord blood," Ms. Brescia says. "We've seen it with tumor registries where there are databanks of people who have full awareness that science needs their input and who are interested in contributing in some way. To these patients, this is a much less onerous way of making a contribution than participating in a clinical trial."

Dr. Schrogie says in addition, the privacy regulations are likely to affect patient recruitment efforts in clinical trials. Patients' records, he says, are sometimes reviewed to determine if a patient has a particular diagnosis and if he or she is a potential candidate for studies. "It is possible that more people in the office get to look at those files," Dr. Schrogie says.

The privacy rule also is likely to impact postmarketing efforts, says John Mack, president of the Internet Healthcare Coalition. "There are a lot of gray areas where the pharmaceutical industry may be affected. For example, sales representatives working with doctors will want to review patient records to see if a patient should be switched to another dosage form. Some things the reps are doing may get into patient-care issues, which may not be condoned by the pharmaceutical company."

To comply with HIPAA, he says, the pharmaceutical sales representatives will have to be trained in the new rule. "Pharmaceutical companies need to be aware of what their people in the field are doing. In addition, this is important depending on how much a pharmaceutical company is involved in disease management and care with physicians. The more they are involved, the more they have to make sure they have proper training and awareness."

But none of this should be a surprise to the pharmaceutical industry, Ms. Leskovsek says. "The clinical research industry has been on notice for some time. This has been an issue in the past, not just in terms of privacy, but also in terms of intellectual property. If a tissue sample is taken in a clinical trial, and that tissue is provided to a sponsor of a marketable product, that person is entitled to some type of royalty."✦

PharmaVoice welcomes comments about this article. E-mail us at feedback@pharmalinx.com.

Experts on this topic

JOHN BENTIVOGLIO. Attorney, Arnold & Porter, Washington, D.C.; Arnold & Porter is a law firm

BONNIE BRESCIA. President, BBK Healthcare Inc., Newton, Mass.; BBK is a healthcare communications agency

DR. JOE FORTUNA. Medical director at Dorland Sweeney Jones, Philadelphia; Dorland Sweeney Jones is a healthcare communications agency

JEAN PAUL GAGNON, PH.D. Director, public policy, Aventis Pharmaceuticals Inc., Bridgewater, N.J.; Aventis is a global pharmaceutical company

NATASHA LESKOVSEK. Attorney, Heller Ehrman, Washington, D.C.; Heller Ehrman is a law firm

JOHN MACK. President, Internet Healthcare Coalition, Washington, D.C.; the Internet Healthcare Coalition is an international, non-partisan, non-profit organization dedicated to identifying and promoting quality healthcare resources on the Internet

DR. JOHN SCHROGIE. VP, peri-approval research services, Omnicare Clinical Research, Fort Washington, Pa.; Omnicare Clinical Research is a contract research organization and a division of Omnicare Inc., Covington, K.Y.

HEIDI WAGNER. Director of government affairs, Genentech Inc., Washington, D.C.; Genentech is a biotechnology company with headquarters in South San Francisco, Calif.

John Mack

THERE ARE A LOT OF GRAY AREAS WHERE THE PHARMACEUTICAL INDUSTRY MAY BE AFFECTED. FOR EXAMPLE, SALES REPRESENTATIVES WORKING WITH DOCTORS WILL WANT TO REVIEW PATIENT RECORDS TO SEE IF A PATIENT SHOULD BE SWITCHED TO ANOTHER DOSAGE FORM. SOME THINGS THE REPS ARE DOING MAY GET INTO PATIENT-CARE ISSUES, WHICH MAY NOT BE CONDONED BY THE PHARMACEUTICAL COMPANY.