

The Evolution of State-Based Medical Record Confidentiality

By Brian A. Bender and Alan M. Winchester

Causes of action in confidentiality, integrity and availability of electronic private health information.

The Missing Link in E-Privacy Litigation?

There are millions of documents associated with the development of a new drug. Many of them are created on a computer or scanned for electronic storage during the course of a clinical trial. More importantly, a large

percentage of clinical trial documents relate to the health of human subjects. Clinical trial sponsors and their researchers have always had an obligation to safeguard this information, but the penalties for non-compliance are likely to become more severe in the coming years.

People are becoming increasingly aware of the fact that their private information is one mouse click away from becoming public knowledge. Society is more computer literate than ever and headlines concerning “e-crimes” are now commonplace. There has been an exponential increase in the amount of private information maintained electronically by banks, businesses and governments, almost all of which lies outside the control of the individuals it identifies. Most private citizens now know that this data can be stolen from or disseminated to anywhere in the world. In sum, there are legions of people becoming seriously concerned about the security of their electronic personal data—and they are all potential plaintiffs.

As individuals become more aware of how public their private information may really be, there is going to be an associated increase in litigation concerning the wrongful dissemination of such data. Indeed, as justice systems continue to become more attuned to technology-related obligations, new statutes and doctrines will provide bases for innovative private causes of action. While it may be impossible to predict the success or failure of such lawsuits, it is reasonable to conclude that the plaintiffs’ bar will seek to create a new family of claims, some of which will take the form of class actions.

This is not idle prognostication. Today’s computers can store a staggering amount of data, and have virtually eliminated the need for hard copy documents. It has been estimated that approximately 20 exabytes of new data will be created in 2006. Igal Brightman, *United Kingdom: TMT Trends: Predictions, 2006—A Focus on the Technology Sector* (Feb. 2, 2006), at <http://www>.



■ Alan M. Winchester is a member of, and Brian A. Bender is a senior associate in, the New York City office of Harris Beach, PLLC. They are part of the firm’s Medical & Life Sciences Practice Group and have extensive experience defending product liability claims filed against members of the pharmaceutical and health care industries. Mr. Bender is also assigned to the firm’s E1Info practice, which is led by Mr. Winchester and provides technology-based legal services to corporations before, during and after litigation.

mondaq.com/i_article.asp_Q_articleid_E_37566. That is the electronic equivalent of two million Libraries of Congress, and less than 0.01 percent of that information will ever be reduced to paper. See John C. Tredennick, Jr., *There is a lot of data out there...*, ABA—Law Practice Today (Jan. 2004), at <http://www.abanet.org/lpm/lpt/articles/fwr01041.html>.

Thus, it is not surprising that there has been a recent rise in the number of privacy-related lawsuits. This increase will become more dramatic in the near future. Moderating factors such as the absence of private rights of action are beginning to give way to increased government enforcement activity, highly publicized “exploratory” claims, and recent state privacy statutes that provide a more defined avenue for relief or impose upon records custodians a duty to inform potential plaintiffs (or an entire class of potential plaintiffs) that their private information was improperly disseminated.

Under these circumstances, it is imperative that companies address their ability to secure any electronic personal information maintained on their computer systems. In addition to being the right thing to do, it will allow companies to proactively defend against impending privacy litigation. This article examines the risks associated with electronic medical information collected during a pharmaceutical clinical trial. However, it is important to note that many of the topics discussed will apply equally to other industries and scenarios.

Electronic Records in Clinical Trials

When a pharmaceutical company wants to conduct a clinical trial, it typically partners with health care providers at one or more medical facilities. Potential subjects are screened according to inclusion/exclusion criteria set forth in the study’s protocols. Qualified subjects must authorize the use of their private medical information prior to participating in the trial.

The exact type of information collected by researchers varies from study to study, but data such as family medical history, genetic testing, past/current medical conditions, use of the experimental drug, use of other medications, side effects, blood test results, diagnostic images, and various other outcome factors may be memorialized. This information is likely to be

associated with other data that identifies individual study subjects, even if it is not disclosed to all of the researchers. This data includes names, birth dates, addresses and social security numbers.

Much of the health information collected by researchers during a clinical trial is disclosed by the study’s sponsor. During the course of the study, the FDA will review the data to ensure ongoing compliance with federal regulations and study protocols. The study sponsor and its researchers also have a continuing obligation to report the occurrence of adverse events. Of course, the data may ultimately serve as scientifically valid proof that the experimental drug is ready for further testing or can be marketed to the general public.

Medical information collected during a clinical trial is frequently maintained in computer databases. Medical records are recognized as confidential information, so the databases are typically protected by electronic, administrative and physical safeguards. In addition, any data disclosed to the FDA or the study sponsor may have to be “de-identified” so that it cannot be associated with any particular individual.

But what happens if the drug company’s firewall fails, allowing an unauthorized individual to gain access to the subjects’ files? What happens if the sponsor’s security software is functional but one of its employees intentionally or accidentally discloses all of the subjects’ confidential information? The answer is that regulatory penalties may apply, and the company is likely to face a series of defensible—but contentious—lawsuits. These lawsuits will be driven by evolving state laws and will draw heavily on the duties and concepts expressed in federal regulations such as HIPAA.

HIPAA Privacy Rule

The United States Department of Health and Human Services (“HHS”) has adopted minimum national standards for the protection of “individually identifiable health information” (also known as “protected health information” or “PHI”). The standards, which are commonly referred to as the “Privacy Rule,” are codified at 45 C.F.R. §§160 and 164. The Privacy Rule defines PHI as any information: a) created or received by a health care provider, health plan or health care clearinghouse; b) which

relates to an individual’s past, present or future medical history; and c) identifies or may reasonably be expected to identify that individual. 45 C.F.R. §160.103.

The Privacy Rule standards pertaining to the security of electronic PHI are codified in Subpart C of 45 C.F.R. §164. They generally require that entities subject to HIPAA: a) ensure the confidentiality of all

Covered entities of all sizes are free to design computer record systems that accommodate their particular needs.

electronic PHI they create, receive, maintain or transmit; b) protect against any reasonably anticipated threats or hazards to the security of such information; c) protect against any reasonably anticipated uses or disclosures of such information that are not authorized by the Privacy Rule; and d) ensure that their workforce complies with the standards. 45 C.F.R. §164.306(a). “Covered entities” are health plans, health care clearinghouses, and health care providers who transmit health information in electronic form for insurance administration or other payment-related purposes. 45 C.F.R. §160.103.

While certain clinical study sponsors (e.g., private drug companies) are not covered entities under the Privacy Rule, they may still be affected by its provisions. For example, if a pharmaceutical company partners with physicians at a large teaching hospital to conduct a clinical trial, the physicians and the hospital are likely to be covered entities under the Privacy Rule. Thus, the Privacy Rule will affect how the researchers provide PHI to the sponsor. Moreover, if a sponsor chooses to become a “business associate” of a “covered” research facility in order to assist in the data compilation process, it may be deemed covered under the Privacy Rule.

45 C.F.R. §164 sets forth administrative, physical, technical and organizational

standards for securing electronic PHI. Each standard calls for the implementation of policies, procedures and other safeguards pertaining to a given security topic. For example, 45 C.F.R. §164.308(a)(1)(i) requires the implementation of policies and procedures to prevent, detect, contain and correct security violations. 45 C.F.R. §164.312(e)(1) requires the imple-

Absent new federal legislation, state laws will be the driving force behind tomorrow's "e-privacy" actions.

mentation of technical security measures to guard against unauthorized access to electronic PHI, and 45 C.F.R. §164.310(c) calls for the implementation of physical safeguards for all workstations that access electronic PHI.

Many of the standards promulgated by 45 C.F.R. §164 are accompanied by "implementation specifications." Implementation specifications provide covered entities with additional information about the types of policies, procedures and safeguards contemplated by HHS. For instance, 45 C.F.R. §164.308(a)(1)(i) (requiring the implementation of policies and procedures to prevent, detect, contain and correct security violations) is accompanied by the following implementation specifications:

- Conduct an "accurate and thorough" assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI;
- Implement security measures sufficient to reduce risks and vulnerabilities to "a reasonable and appropriate level;"
- Apply "appropriate sanctions" against workforce members who fail to comply with security policies and procedures; and
- Implement procedures to "regularly review" records of information

system activity, such as audit logs, access reports, and security incident tracking reports.

See 45 C.F.R. §164.308(a)(1)(ii)(A)-(D).

Implementation specifications burden covered entities with the responsibility for determining what satisfies the Privacy Rule security standards. The standards and their specifications were purposefully drafted to be scalable and technology-neutral. See Health Insurance Reform: Security Standards; Final Rule, 68 Fed. Reg. 8335 (Feb. 20, 2003). As such, covered entities of all sizes are free to design computer record systems that accommodate their particular needs. However, they may also have to document their decision-making process. See 45 C.F.R. §164.306(d)(3).

A covered entity that is found to have violated a Privacy Rule security standard may be subject to civil penalties of up to \$25,000 per violation type per year. See 45 C.F.R. §§160.402 to 160.408. In addition, while the Privacy Rule does not create a private cause of action, it does permit private causes of action that are properly brought pursuant to other statutes (e.g., those available under state law). 45 C.F.R. §160.418.

FDA Guidance Documents

On March 20, 1997, HHS issued 21 C.F.R. Part 11 ("Part 11"), which establishes the conditions under which electronic records submitted to the FDA will be considered trustworthy duplicates of their paper counterparts. Part 11 is not a privacy statute, but its conditions overlap with many of the concepts discussed in the HIPAA Privacy Rule. As a result, the FDA's interpretation of Part 11 may provide insight into what a covered entity may be required to do under the broadly worded standards and specifications set forth by 45 U.S.C. §164.

One particularly relevant area of overlap is electronic records security. Part 11 recognizes that secure computer systems produce reliable electronic records. Although this concept does not address security from a privacy perspective (and the Rule's only penalty provision is the potential for the FDA to reject electronic record submissions), the FDA has interpreted it in a manner that could be useful for covered entities engaged in clinical trials.

For example, *Guidance for Industry: Computerized Systems Used in Clinical Tri-*

als (U.S. Food and Drug Administration; September, 2004 draft, rev. 1) ("Part 11 Guidance") sets forth various recommendations on how to construct a computer system that is secure enough to generate reliable electronic documents. These recommendations may be used to clarify a "covered entity's" obligations under the Privacy Rule. For instance, the Part 11 Guidance recommends that the following internal and external safeguards be put in place to ensure that access to the computer system is restricted to authorized personnel:

- Operational system checks;
- Authority checks;
- Device checks;
- Written policies that hold users accountable for actions initiated under their names;
- Methods for maintaining a cumulative record of data flow (e.g., via audit trails);
- Protection against unauthorized and/or external browsing or querying of system data; and
- Procedures to prevent, detect and mitigate the effects of computer viruses, worms or other potentially harmful software code.

Part 11 Guidance, at pp. 8-9.

Part 11 is currently under review and will soon be re-drafted by the FDA. During this process, the FDA will be exercising a certain amount of enforcement discretion. However, the current version of Part 11 remains in effect and its guidance documents continue to provide useful information concerning the government's thinking with respect to electronic record security.

State Legislation

The HIPAA Privacy Rule contains a general preemption provision, but it permits state law claims if they are based upon a statute that does not conflict with or is more stringent than the Privacy Rule. See 45 C.F.R. §160.203. As a result, many states have enacted their own privacy laws. Private organizations have also studied the issue and drafted a model privacy rule that could help standardize state statutes.

Absent new federal legislation, state laws will be the driving force behind tomorrow's "e-privacy" actions. Unlike §164 of the HIPAA Privacy Rule, the state statutes are

not necessarily limited to electronic medical information and create private rights of action that allow plaintiffs to recover statutory as well as actual damages. These damages may be awarded in addition to penalties imposed under HIPAA.

Model Rule

In the mid-1990s, the Centers for Disease Control and Prevention, Council of State and Territorial Epidemiologists, Association of State and Territorial Health Officials, National Conference of State Legislatures, and Georgetown University Law Center sponsored a program to develop a model state public health privacy act. See <http://www.critpath.org/msphpa/modellaw5.pdf> ("Model Rule").

The Model Rule provides substantial remedies to individuals whose private health information was negligently or intentionally disclosed. For instance, §7-103 (Civil Remedies) provides that a private cause of action may be maintained by any person aggrieved by:

- the failure to impose and maintain adequate safeguards for the confidentiality and security of protected health information;
- the failure to supervise persons responsible for the acquisition, use, disclosure, or storage of protected health information;
- the disclosure of protected health information in violation of the Model Rule; or
- any other violation of the Model Rule.

The Model Rule also provides for damages beyond those articulated in HIPAA. §7-104(C) allows an aggrieved person to recover damages equal to the greater of his/her actual damages or liquidated damages of \$1,000 for each violation (not to exceed \$10,000 for any particular claim). Notably, the Model Rule also contemplates the assessment of punitive damages and attorney fees in appropriate circumstances.

The Model Rule provides for a substantial amount of damages over and above the federal statutory fines. This would be particularly true in the case of an improper large-scale disclosure of PHI during a late-stage clinical trial. For instance, a Phase III study might involve thousands of human subjects, each of whom would have a right to sue for damages under the Model Rule.

The sheer volume of plaintiffs, accompanied by the potential for a punitive damages and/or attorney's fees award, would almost certainly result in an attempt to certify a class action.

State Statutes

There has been a marked increase in the scope and specificity of state-based privacy laws in the past few years. In addition, many of these new laws have enacted notification procedures that entities must adhere to when there has been a breach of security. As of 2003, only a few states had such statutes. However, several additional states passed laws in 2004, followed by 30 others in 2005. For the year 2006, there have so far that been 16 states that have passed new notification laws relating to security breaches for private information. Today, every state and many other nations have enacted laws requiring notification in the event of a security breach and each year the obligations have become more refined. The various state laws bear some resemblance to the Model Rule, but individual lobbying efforts have created tremendous diversity in approach and implementation on the state level.

For example, New York has enacted a regulatory scheme that imposes a duty upon health care providers (very broadly defined by N.Y. Pub. Health Law §18(1)(b)-(d)) to enclose either a copy of the patient's written consent or the name and address of the third party with a note explaining the purpose of the disclosure with any medical records being disclosed. See N.Y. Pub. Health Law §18(6). New York also has additional regulations for certain types of entities. Under N.Y. Pub. Health Law §4408(2), an HMO enrollee has the right to demand to see the procedure used by the HMO to protect the confidentiality of medical records. Similarly, N.Y. Ins. Law §3217(c) prevents an insurance company from disclosing health information to any third party without the patient's consent. There are also special laws relating to hospitals (N.Y. Ins. Law §4324(b)); on-site occupational health service facilities (N.Y. Lab. Law §201-e); and state government (N.Y. Pub. Off. Law §87 and 96).

New York also has enacted condition-specific laws that provide heightened protection for certain types of medical records.

This list includes birth defects (N.Y. Pub. Health Law §2733); cancer (N.Y. Pub. Health Law §2402); genetic information (N.Y. Civ. R. Law §79-1(2)(d)); HIV/AIDS (N.Y. Pub. Health Law §2781(1)); and mental illness (N.Y. Mental Hyg. Law §33.13).

New York has one of the most complex sets of health privacy laws, but most other states have enacted various provisions that differentiate between types of providers and different diseases. In virtually every case, the laws are more threatening than HIPAA. This is because they provide for private rights of action and larger monetary awards. Plaintiffs have also been successful in using state statutes as springboards for recovery for damages arising out of other common law causes of action. In some cases, this is made possible by using the statutory violation to prove a breach of duty.

For example, in Michigan, a private right of action exists for people whose HIV status is released without authorization. See Mich. Comp. Laws §333.5131. This provision has been used by plaintiffs to access the courthouse and recover on multiple theories. In *Doe v. Am. Med. Pharmacies, Inc.*, 2002 WL 857766 (Mich. App. May 3, 2002), a pharmacy employee loudly disclosed a patient's HIV status in a crowded waiting room, resulting in a \$100,000 sustained verdict for slander, invasion of privacy and intentional infliction of emotional distress.

Similarly, a Palm Beach County Health Department statistician and epidemiologist recently attached a list identifying 6,000 HIV/AIDS patients to an e-mail received by hundreds of the department's employees. See *HIVE-Mail Leads to Changes*, Palm Beach Post, February 23, 2005. In addition, the fines for breaching this information can be quite steep. Florida Stat. Ann. §381.004(6)(a) makes it a misdemeanor to disclose HIV information and imposes a maximum penalty of one year in jail and \$1,000 in fines. If HIV information is disclosed maliciously or for monetary gain, the penalties jump to five years in jail and a \$5,000 fine. Under both circumstances, the aggrieved party may recover attorney fees and the greater of actual or liquidated damages in a separate private lawsuit.

In sum, state privacy regulations are fertile ground for "e-privacy" claims. The statutory schemes may cross various areas

of practice, and implicate both traditional and non-traditional theories of liability. It is important for pharmaceutical manufacturers to familiarize themselves with these laws prior to engaging in a clinical trial. Indeed, it makes good sense to adhere to the standards of the most privacy-conscious state or nation in which the study may be performed.

The Model Rule provides for a substantial amount of damages over and above the federal statutory fines.

Potential Claims and Defenses

Plaintiffs whose electronic PHI is wrongfully disclosed during a clinical trial will rely on state privacy statutes to file private causes of action. They will pair those claims with other theories of recovery (e.g., negligence, slander, libel, emotional distress). The essence of most matters will be that a study sponsor or researcher failed to take appropriate steps to safeguard PHI or train its staff members. Creative plaintiffs' attorneys will use the HIPAA Privacy Rule and the Part 11 Guidance to demonstrate the existence of a duty, particularly when there has been a violation of those provisions. They will demand copies of all documentation required under those standards, particularly those concerning the security system decision-making process (which are mandated pursuant to 45 CFR Part 164.306(d)(3)).

Though feasible, these actions are defensible. In fact, many defenses draw on identity theft litigation. For instance, in *Smith v. Chase Manhattan Bank*, 741 N.Y.S.2d 100 (App. Div. 2d. 2002), the defendant promised its customers that it would not sell their personal information to third parties. Plaintiffs filed a class action alleging that the bank sold customer lists to third parties, including a telemarketing firm. The court dismissed the complaint, finding that the alleged "harm" was that class members were offered products and services they were free to decline. Moreover, the

complaint did not allege a single instance where a specific class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail.

Depending on the medical information released for patients in a clinical trial, this defense may succeed. For one thing, many human subjects are healthy. In any event, even sick plaintiffs may be hard-pressed to show that they actually knew of, or were harmed by, the wrongful disclosure of their study records (e.g., loss of a job, emotional distress). However, this defense will not necessarily avoid any applicable liquidated damages, and if the number of patients whose records were disclosed is sufficiently large, this could represent a daunting sum.

It can also be argued that the disclosure of plaintiffs' PHI was not the proximate cause of their alleged damages. In cases where the plaintiff maintains copies of his own medical records, or where he has made public the fact that he was in a clinical trial, it will be hard for him to prove that it was the disclosure of the PHI (as opposed to something he did) that caused him injury. In identity theft cases, this usually involves someone rummaging through plaintiff's unshredded trash. As with the damages defense, however, the proximate cause argument does not avoid statutory fines for the mere act of disclosure.

There are, of course, other defenses available (e.g., those provided in HIPAA, adherence to industry standards). However, the best arguments are simply that: a) the PHI was never disclosed; and b) if it was disclosed, it was not due to unreasonable acts or omissions by the defendant. Unfortunately, there is no black letter rule for making sure these defenses apply to a specific situation. Study sponsors and their researchers must be sure to use materials like the HIPAA Privacy Rule standards and the Part 11 Guidance to make the best choices they can for their particular situation. This should be done in consultation with an attorney who can provide advice about the sufficiency of all clinical trial documentation and make sure those materials do not contain potentially harmful admissions.

Conclusion

The time is right for a surge in "e-privacy"

litigation, and health care records may be part of its leading edge. Public knowledge of the risks associated with electronic information is at an all-time high, and our reliance on digital media is steadily growing. Computerized medical records are of particular interest because of their sensitive nature, and pharmaceutical clinical trials generate tremendous amounts of such information.

HIPAA addresses electronic medical records security, but leaves to each covered entity the task of determining what particular measures it must take to comply with the statute. The Part 11 Guidance provides some further guidance, but it is collateral at best. Moreover, covered entities may be required to create harmful admissions regarding the security choices they made to comply with the regulation.

Since HIPAA only provides for limited monetary penalties, plaintiffs will look to evolving state laws for private rights of action. Many state statutes provide for more severe penalties than HIPAA, and in certain cases may be the impetus for an attempt at class action certification. Plaintiffs will also attempt to file more traditional causes of action based upon a disclosure of PHI, some of which could result in additional damages.

The best defense to a claim concerning the disclosure of PHI is conscientious adherence to HIPAA and any state laws that specifically govern the security of electronic medical records. Documents such as the Part 11 Guidance are helpful in this regard, because adherence to their provisions may deprive plaintiff of a means by which to establish the violation of a legal duty underlying a state law claim.

Pharmaceutical companies should work closely with their attorneys to ensure that the documents concerning their clinical trial computer systems cannot be construed as allowing for punitive damages (e.g., stating that economics, not privacy concerns, drove the decision-making process). Attorneys may also help drug companies assemble task forces comprised of IT, medical and legal personnel who will bring diverse experience to the regulatory compliance effort. This may ultimately serve as additional proof of reasonability.

In closing, it must be recognized that "e-privacy" is an evolving area of law. The

number and diversity of standards promulgated by federal and state governments to secure health information generally, and computer information specifically, makes the subject dynamic and very complex.

There is no single solution to all electronic problems. However, a full understanding of federal law and regulations will guide companies towards compliance with their duties under unique state privacy laws.

This, in turn, will help study sponsors select the best legal venues for their clinical trials and, most importantly, keep their subjects' PHI as secure as possible. 