Coppersmith Gordon Schermer & Brockelman PLC

eHI Connecting Communities for Drug Safety Collaboration

An Analysis of Legal Issues Related to the Use of Electronic Health Information in Pharmacovigilance Programs

Kristen Rosati
Kim Fatica
Roopali Desai
Coppersmith Gordon Schermer & Brockelman PLC*

Executive Summary

I. Introduction to the eHI Connecting Communities for Drug Safety Collaboration

The eHealth Initiative Foundation (eHI) Connecting Communities for Drug Safety Collaboration is a public-private sector effort designed to test new approaches and develop replicable tools for assessing the risks and the benefits of new drug treatments through the use of health information technology. The Drug Safety Collaboration is coordinated and led by eHI, a non-profit, multi-stakeholder organization whose mission is to improve the quality, safety and efficiency of health care through information and information technology. With guidance from eHI's multi-stakeholder Leadership Council, the Drug Safety Collaboration involves three leading pharmaceutical companies — Pfizer Inc., Johnson & Johnson, and Eli Lilly and Company—and two community-based healthcare organizations with advanced stage clinical information systems—Partners HealthCare System, Inc. in Massachusetts and the Indiana Network for Patient Care, run by the Regenstrief Institute.

The Drug Safety Collaboration is using three "use cases" to test and evaluate the value and utility of using electronic clinical and administrative health information to detect and evaluate drug safety signals: the use of cholesterol-lowering drugs and laboratory results related to liver failure, warfarin-related bleeding episodes, and adverse patient events commonly associated with medications, called "designated medical events." Lessons gathered from the "learning laboratories" in Boston and Indianapolis will be documented and converted into technical guides and tools that will be made widely available to the public to stimulate advancement of drug safety efforts.

The collaborators realized that the legal issues in a drug safety project are significant. The Drug Safety Collaboration thus commissioned the law firm of Coppersmith Gordon Schermer & Brockelman PLC to produce an extensive legal guidance to cover all of the major legal issues involved in drug safety collaborations involving Health Information Exchanges (HIE), health systems and pharmaceutical

* This work produced by Coppersmith Gordon Schermer & Brockelman PLC is intended as a general reference source and is not meant to provide legal advice to any person or entity that receives a copy of the work. This publication is provided with the understanding that the authors and eHealth Initiative are not engaged in rendering legal or other professional services, and readers should consult with competent counsel to determine applicable legal requirements for the specific fact situation.

companies, and two template agreements: an agreement between an HIE and its participants that would allow the HIE to utilize the information in the HIE for drug safety purposes, and an agreement between an HIE and a pharmaceutical company to govern the terms and conditions of a drug safety project, designed to ensure rigorous patient confidentiality and security. This document provides guidance to the numerous legal issues involved in drug safety surveillance (called "pharmacovigilance" throughout this report), utilizing electronic clinical information. The template agreements are published separately.

II. The Policy Background: Concern with "Secondary Uses" of Electronic Clinical Information

Using electronic clinical information promises to accelerate the timeliness, accuracy, and effectiveness of methods currently used to monitor drug safety and facilitate response by the health care system. The use of clinical information for a pharmacovigilance project, however, must be conducted with detailed attention to protecting the privacy and security of individual health information. Individual consumer trust is essential to build public support for using electronic health information for pharmacovigilance. Consumer trust is built through creating transparency about how health information is used, involving trusted parties such as health care providers and hospitals as collaborators in a pharmacovigilance program, and ensuring unwavering attention to the privacy and security of health information utilized in the program.

Building consumer trust in a pharmacovigilance program takes place in the context of growing public attention to "secondary uses" of health information—uses beyond the care and treatment of the individual. Many developing HIEs across the country are struggling with the policy decisions about whether, and under what conditions, the information in an HIE should be used for purposes beyond the care of the specific individual. While HIEs understand that use of health information for non-treatment purposes has the possibility of wide benefit to their communities—improvement of care at particular institutions, public health surveillance, research, and drug safety surveillance, among other important public goals—many policy makers involved in the creation of HIEs are wary of expanding the scope of the use of HIEs beyond treatment without a framework governing the parameters for these non-treatment activities.

This legal guidance is part of eHI's work to create such a framework. The eHI Connecting Communities for Drug Safety Collaboration will be an important step in establishing a national consensus for how to approach the technical, policy and legal issues involved in the use of electronic health information for pharmacovigilance programs. In addition, the National Committee on Vital and Health Statistics (NCVHS) released its report, "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data" on December 19, 2007, which addresses other non-treatment uses for health information. These resources will assist in building a national framework for appropriate use of health information for purposes other than treatment, hopefully increasing HIE comfort with harnessing the great wealth of information for public good, consistent with rigorous protection of individual privacy.

III. The Legal Analysis

A. Privacy

The use of health information for any purpose outside of the treatment of individual patients poses obvious concerns about the privacy of individual health information. In order for pharmacovigilance programs to be successful in the long run, consumers must trust that their health information will be treated confidentially and used appropriately.

The plethora of federal and state laws governing the confidentiality of health information complicates the analysis of privacy compliance in a pharmacovigilance program. The legal guidance discusses federal confidentiality laws, including the Health Insurance Portability and Accountability Act (HIPAA), the

federal alcohol and drug treatment program regulations, and the federal Privacy Act and Medicare Conditions of Participation, and then discusses various categories of confidentiality laws typically found at the state level. Each health system or HIE considering participating in a pharmacovigilance program should pay careful attention to how laws applicable in their individual jurisdictions will affect such a program.

1. HIPAA

HIPAA and its regulations present the most obvious privacy and confidentiality requirements that apply to the use of individual health information. The HIPAA compliance challenges and their resolution will depend on the source of the information for the pharmacovigilance program and the participants in the program. HIPAA applies to health plans, health care clearinghouses, and health care providers that engage in electronic standard transactions such as billing (called "HIPAA covered entities"). Health systems and other health care providers that participate in a pharmacovigilance program likely will be HIPAA covered entities. An HIE may or may not be a HIPAA covered entity, depending on its specific functions. If an HIE performs traditional billing functions on behalf of health care providers, it will be a health care clearinghouse; it is less clear under the regulations whether the processing of clinical data into a standard format (such as reformatting information into normalized clinical information for presentation in a clinical abstract or continuity of care record) meets the definition of a health care clearinghouse. In any event, most HIEs will be HIPAA business associates of the health care providers participating in the health information exchange and thus will be required to comply with many of the HIPAA requirements as a contractual matter. The pharmaceutical company partners in a pharmacovigilance program will not meet the definition of a HIPAA covered entity, and will only function as HIPAA business associates if they perform de-identification of the electronic health information that will be used for the project.

The HIPAA regulations protect all "individually identifiable health information" handled by a covered entity. If a covered entity "de-identifies" its information before utilizing it for a pharmacovigilance program, HIPAA would not apply to the use of that de-identified information, and many of the privacy concerns with a pharmacovigilance program would be removed. However, de-identification probably will not be a practical option for many pharmacovigilance programs. While pharmacovigilance programs generally will not need direct identifiers such as name, address, and social security number, the programs will need access to some HIPAA identifiers—particularly dates of service—to determine whether a particular drug potentially caused a particular safety event. If only partially de-identified information will accomplish the program's objectives, the parties may be able to conduct the program under a "Limited Data Set, as long as a "Data Use Agreement" is in place with any recipient of the information.

We assume that obtaining individual authorization to access medical records for a pharmacovigilance program will not be possible. Large health systems and HIEs maintain hundreds of thousands, if not millions, of records. The process of contacting these patients—many of whom may not be at the address of record—would be time consuming and entail substantial expense. If the information for a pharmacovigilance program cannot be de-identified or included in a Limited Data Set, we thus examine other feasible options for pharmacovigilance program HIPAA compliance.

First, the HIPAA Privacy Rule permits disclosures of health information for public health purposes, including two purposes relevant to pharmacovigilance programs. HIPAA permits a covered entity to release health information to a person or company subject to the FDA's jurisdiction to collect or report adverse events or for post-marketing drug safety surveillance. A pharmacovigilance program will meet this requirement. HIPAA also permits a covered entity to release health information to a public health authority such as the FDA, or to a person or entity acting under a grant of authority from a public health authority; this may be a feasible option if the FDA agrees to designate the participants in a pharmacovigilance program (or one of the participants) to act under a grant of authority from the FDA to collect post-marketing drug safety surveillance information.

Second, the HIPAA Privacy Rule permits use and disclosure of health information for research. Whether a particular pharmacovigilance program is a public health activity or "research" may be a difficult call, as the distinction between public health surveillance activities and research is sometimes a thin one. If the pharmacovigilance program is research, the program must meet at least one of the HIPAA Privacy Rule's requirements related to research. In this section of the report, we explore the circumstances under which an IRB could grant a request to waive HIPAA authorization. We conclude that, with appropriate confidentiality protections in place, many IRBs would approve waiver of HIPAA authorization for a pharmacovigilance program. Because these programs seek to evaluate all records held by a health system or HIE, the program is potentially examining huge numbers of patient records. Because it would be exceedingly difficult and expensive to contact all patients whose records are housed in a system's EHR or an HIE we believe that an IRB could conclude that the research could not practicably be conducted without a waiver of authorization. Of course, the researchers would also have to demonstrate to the IRB that they need individually identifiable information for the research and that they have a rigorous plan in place to protect the patient information from improper use and disclosure.

The final potential option for HIPAA compliance is to treat the collection and analysis of drug safety data for a pharmacovigilance program as "health care operations" under HIPAA, which include population-based activities relating to improving health. However, because the scope of these activities is unclear, and because the definition of health care operations excludes research activities, we do not recommend this route for HIPAA compliance.

A HIPAA covered entity participating in a pharmacovigilance program also must follow the HIPAA Security Rule in its handling of PHI. The Security Rule requires administrative, technical, and physical security safeguards to protect health information in electronic form.

2. Other Federal Laws

The federal regulations governing alcohol and drug abuse treatment information (the "Part 2" regulations) greatly restrict the ability to use information received from federally assisted alcohol or drug abuse programs for pharmacovigilance. If such information will be included, the only viable option to comply with the Part 2 regulations is to structure the pharmacovigilance program as a research protocol, which then will be subject to special research restrictions (such as approval by the substance abuse treatment program director).

Two other federal health information confidentiality laws—the Medicare Conditions of Participation and the federal Privacy Act—will not impose greater limitations on a pharmacovigilance program than the HIPAA Privacy Rule.

3. State Health Information Confidentiality Laws

A pharmacovigilance program involving patient information implicates state health information confidentiality laws, as well. Each health system or HIE contemplating such a program should look carefully at its state statutes and regulations to determine whether those state laws impose any additional restrictions on the conduct of the program beyond the federal law requirements discussed above.

Because it is beyond the scope of this legal guidance to cover the laws of all 50 states, we address typical *categories* of state laws that likely will limit health system and HIE use of information in a pharmacovigilance program—laws protecting particularly sensitive information such as genetic testing, mental health, and HIV/AIDS information—and examine different state laws as examples of the analysis that would be applied. We also provide a framework for evaluation of state laws' effect on a pharmacovigilance program, and suggest analysis of four discrete questions: (1) does the law apply to the proposed participants in the drug safety surveillance program; (2) does the law permit individual

information to be utilized in a pharmacovigilance program; (3) does the law apply only to external disclosure, or does it apply to internal uses, as well; and (4) do existing consent processes cover the pharmacovigilance program? We also provide resources that may be helpful for pharmacovigilance participants to locate their relevant state laws.

Based on the evaluation of example state laws in Arizona, Indiana, Massachusetts and Minnesota, it appears that, while some state laws have substantial restrictions on the disclosure of sensitive information, it may be a feasible option even under the most restrictive state laws to structure a pharmacovigilance program as a research protocol. Moreover, because many state laws apply only to disclosures to third parties, these state laws may not interfere with a health system accessing its own EHR for pharmacovigilance purposes and releasing only aggregated information to the pharmaceutical company participants.

B. Research Compliance Issues

As explored in the privacy compliance section, if a pharmacovigilance program is structured as a research protocol, it will meet the terms of most federal and state confidentiality laws. Of course, conducting research requires compliance with federal (and sometimes state) requirements relating to the protection of human subjects involved in the research.

Research involving human subjects regulated by federal law often requires review by an Institutional Review Board (IRB). The Federal Policy for the Protection of Human Subjects (also known as the "Common Rule"), applies to research involving the obtaining of identifiable private information, if that research (a) is not otherwise exempt, and (b) is conducted or supported by a federal department or agency that has adopted the Common Rule, or where the institution engaged in the research has agreed to apply the federal regulations under the institution's Federalwide Assurance to all non-exempt human subjects research regardless of the source of funding. The FDA regulations, which apply to all clinical investigations regulated by the FDA or that support marketing applications for FDA approval, also require IRB review. In addition, while some research is not covered by either the Common Rule or FDA regulations, many institutions have internal policies requiring IRB review of all research conducted at the institution.

In some circumstances, human subject research is exempt from the requirements of federal human subject protection regulations, including requirements related to IRB review. Under the Common Rule, research involving the collection or study of existing data, documents, or records (such as electronic medical records) would be exempt if researchers record the information so that individuals cannot be identified, either directly or through identifiers linked to the subjects. The FDA regulations' requirements, if applicable, have considerably stricter requirements for exemption. Moreover, even where research is exempt, an organization's policies may require review of research. So, it is unlikely that a pharmacovigilance research protocol will not be subject to IRB review. If the research protocol requires IRB review, it is possible that the protocol will be subject to expedited review by the IRB Chair or another IRB members designated by the IRB Chair, rather than full board review.

When an IRB reviews a research protocol, the IRB must determine that a number of criteria are met to approve the protocol. In a protocol involving access to electronic health records, where the research does not involve any individual therapeutic intervention, the issue of greatest interest to the IRB will be how the researchers will maintain the privacy and confidentiality of the information utilized in the project. It is likely that researchers will ask the IRB to waive the requirement of obtaining informed consent from the individuals whose information is accessed for a pharmacovigilance program. In an analysis similar to the IRB waiver of a HIPAA authorization, we expect that many IRBs would approve waiver of informed consent as long as rigorous confidentiality protections are in place.

Finally, if multiple institutions (health systems, hospitals, HIEs, and other providers) will be participating in a pharmacovigilance program, it is possible for those multiple institutions to designate one IRB as the reviewing IRB for the program. This makes a great deal of sense for pharmacovigilance programs involving multiple parties to reduce the cost of IRB reviews and to reduce the variability of IRB requirements across institutions.

C. FDA Reporting Obligations

Because the purpose of a pharmacovigilance project is to determine whether approved drugs are safe—essentially to create an "early-warning" system for drug safety—the participants in a pharmacovigilance project undoubtedly will learn about adverse drug experiences. Where a health system or HIE partners with drug manufacturers in a pharmacovigilance program, we believe information generated by the health system or HIE will be treated as a solicited source because it is an "organized data collection scheme," especially if the pharmacovigilance program is structured as a research protocol. A drug manufacturer, therefore, when learning of information about an adverse drug experience generated by the pharmacovigilance program, must determine if the adverse drug experience is both serious and unexpected and causally related to a drug. If these factors are present, then the manufacturer must make an expedited report to the FDA and later follow-up with a fifteen-day report, and then a periodic report. If, however, the manufacturer does not find these factors present, it need not make an expedited or periodic report to the FDA.

The holders of electronic health information—HIEs and health systems—do not have mandatory reporting obligations under FDA regulations. Rather, reporting is purely voluntary using the multiple adverse event reporting system called MedWatch.

D. The FDA Amendments Act of 2007

The Food and Drug Administration Amendments Act of 2007 (FDAAA) includes a number of provisions relating to drug safety, two of which may be particularly significant to pharmacovigilance programs. First, the law requires the FDA to develop a "postmarket risk identification and analysis system" by creating methods to obtain access to different data sources and validated methods to link data from various sources, yet which complies with HIPAA and does not disclose individually identifiable health information. The development of pharmacovigilance programs using HIE or health system data sources likely will be of great interest to the FDA, and the statute authorizes the FDA to enter into contracts with "qualified entities" to classify, analyze or aggregate data, and to investigate drug safety questions.

Second, the FDAAA authorizes the Secretary to require risk evaluation and mitigation strategies (REMS) by drug manufacturers when necessary to ensure that the benefits of a drug outweigh the risks, both for new applications and already-approved drugs and biologics. The data generated from a pharmacovigilance program may be a valuable data source for the FDA to utilize in evaluating drug risks after approval, and the participants should carefully monitor any regulations or guidance issued by the FDA to implement the REMS requirements.

E. Tort Liability under the Common Law

In assessing the risks associated with a pharmacovigilance program, each of the participants must evaluate whether it will have a common law duty to warn patients or physicians of potential drug risks that are identified through the program and whether a failure to do so can result in liability under a common law tort theory. We discuss the general state of the law relating to the common law duties and potential claims under strict product liability and negligence arising from a failure to warn of potential adverse side effects of FDA-approved drugs. However, because state law will govern common law liability, participants in a pharmacovigilance program should look carefully at how the law of the applicable jurisdiction will affect this analysis.

1. Manufacturers

Most strict product liability claims in the context of prescription drugs turn on the adequacy of the manufacturer's warnings of the risks associated with the drug. Failure to comply with FDA reporting requirements may render a product "defective" for inadequate instructions or warnings. On the other hand, compliance with FDA reporting requirements does not conclusively establish that a manufacturer has complied with its duty to warn of product dangers—such compliance is a factor to be considered in determining whether a product is defective, but is not determinative. Failure to warn may also result in a negligence claim against drug manufacturers. Like in a product liability claim, a manufacturer's compliance or failure to comply with FDA reporting requirements will be relevant to whether the manufacturer met its duty to warn.

Some courts have held that a manufacturer's duty to warn is not limited to reporting to the FDA and FDA-approved label changes, and have imposed upon manufacturers an obligation to send "Dear Doctor" letters or to enlist the assistance of the manufacturer's sales force to alert physicians to particular risks. So, when a pharmacovigilance program indicates a new risk not included in the FDA-approval label for the drug, manufacturers should consider disseminating that information to prescribing physicians.

The FDA does not impose a duty to warn consumers directly. Moreover, most courts have adopted the "learned intermediary doctrine," which holds that a manufacturer of prescription drugs satisfies its duty to give notice of potential drug dangers by notifying the physicians who will prescribe the drugs. The rationale behind the learned intermediary doctrine is that only health care professionals are in a position to understand the significance of the risks involved and to assess the relative advantages and disadvantages of the prescription drug at issue. Once adequate warnings are provided to the physician, it becomes the duty of the physician to provide such information to the physician's patients to allow the patients to make informed decisions. There are, however, limitations to the learned intermediary doctrine that have eroded protections offered to manufacturers and the continued application of the learned intermediary doctrine in the context of a pharmacovigilance effort may be challenged.

Because manufacturers of prescription drugs are heavily regulated by the FDA, we discuss whether state law tort claims may be preempted by the federal regulations. We conclude that the FDA regulations for prescription drug manufacturing, advertising, and distribution will not preempt state law tort claims related to strict product liability and negligence for failure to warn.

2. Health Systems and HIEs

Health systems and HIEs likely would not be held liable under strict product liability. Even if health system employees distribute pharmaceuticals (either in the hospital, outpatient setting, or retail pharmacy), courts generally have refused to hold nonmanufacturing retail sellers of prescription drugs liable under strict product liability. Moreover, an HIE is not in the retail or distribution chain of the pharmaceutical product and thus could not be held liable under strict product liability.

Health systems and HIEs also likely would not be held liable under a negligence theory for failure to warn of a drug risk discovered in a pharmacovigilance program. Absent a doctor-patient relationship, courts generally have been reluctant to impose a duty to warn patients of potential dangers of drugs. Courts thus have not imposed a duty to warn unless an entity voluntarily assumes a duty to notify patients and the patients have a reasonable expectation that the entity will do so. The risk of such a claim can be minimized by health systems and HIEs if any communications related to the pharmacovigilance program explain that the purpose of the project is to gather data to be analyzed by the drug manufacturers and that information about drug risks will be reported to the FDA in accordance with regulatory requirements and not directly to patients or their physicians.

IV. Conclusion

The legal issues for HIEs, health systems and pharmaceutical companies engaging in pharmacovigilance programs are quite complicated, but we believe the legal risk is not high as long as the program is carefully constructed. The program must include a rigorous plan to protect the privacy and security of the health information evaluated and should minimize the use of individually identifiable health information to the extent possible. Moreover, the pharmaceutical company participants must follow FDA reporting obligations and communicate significant new findings of risk to health care providers. Of course, these issues have not yet been examined by courts in the context of pharmacovigilance programs, so we urge HIEs, health systems and pharmaceutical companies participating in pharmacovigilance programs to track the progress of issues noted in this guidance and closely evaluate the applicable laws in their jurisdictions.

An Analysis of Legal Issues Related to the Use of Electronic Health Information in Pharmacovigilance Programs

Table of Contents

I. Introduction 1

A. The eHI Connecting Communities for Drug Safety Collaboration 1

B. The Policy Background: Concern with "Secondary Uses" of Electronic Clinical Information 1

C. What This Legal Guidance Covers 2

II. Privacy Compliance Issues 3

A. The Health Insurance Portability and Accountability Act (HIPAA) 4

1. HIPAA's Application to a Pharmacovigilance Program: Participants as HIPAA Covered Entities or Business Associates 4

2. Pharmacovigilance Program Utilization of Protected Health Information 6

3. Use and Disclosure of Protected Health Information in a Pharmacovigilance Program 9

a. Use and Disclosure for Public Health Purposes 10

b. Use and Disclosure for Research 11

(1) Public Health Surveillance Versus Research 11

(2) Use and Disclosure of PHI for Research 12

c. Use and Disclosure for Health Care Operations 15

4. Compliance with the HIPAA Security Rule 16

B. Federal Alcohol and Drug Abuse Treatment Program Regulations 17

C. Other Federal Laws 19

D. State Health Information Confidentiality Laws 19

1. Genetic Testing Information 20

2. Mental Health Information 23

3. HIV/AIDS 27

4. General Health Information Laws 28

III. Research Compliance Issues 31

A. Definition of "Research" 32

B. Review by an Institutional Review Board 32

1. "Human Subject Research" 32

2. Research Exempt from IRB Review 33

3. Research Subject to Expedited Review 33

4. Criteria for IRB Approval 34

5. Waiver of Informed Consent 35

C. Whose IRB May Conduct the Review? 36

IV. FDA Reporting Obligations 37

A. Drug Manufacturer Obligations 37

1. Expedited Safety Reporting (15-Day Alert Reporting) 38

a. Spontaneous Source 38

b. Solicited Source 39

c. Timing of Report 40

d. Proposal for Expedited Reporting of All Adverse Drug Experiences 40

2. Periodic Safety Reporting Requirements 41

3. Application to a Pharmacovigilance Project 41

B. Health System and HIE Obligations 42

1. Voluntary Reporting to MedWatch 42

2. Proposal for Expedited Reporting by Contractors 42

V. The FDA Amendments Act of 2007 43

A. Active Postmarket Risk Identification and Analysis 43

B. Risk Evaluation and Mitigation Strategies (REMS) 44

VI. Tort Liability under the Common Law 45

A. Manufacturers 45

1. Strict Product Liability 45

2. Negligence 47

3. Content, Timing, Target and Methods of Warnings 48

4. Preemption by FDA Regulation 52

B. Health Systems and HIEs 53

1. Strict Product Liability 53

2. Negligence 54

VII. Conclusion 56

An Analysis of Legal Issues Related to the Use of Electronic Health Information in Pharmacovigilance Programs

I. Introduction

A. The eHI Connecting Communities for Drug Safety Collaboration

The eHealth Initiative Foundation (eHI) Connecting Communities for Drug Safety Collaboration is a public-private sector effort designed to test new approaches and develop replicable tools for assessing the risks and the benefits of new drug treatments through the use of health information technology. The Drug Safety Collaboration is coordinated and led by eHI, a non-profit, multi-stakeholder organization whose mission is to improve the quality, safety and efficiency of health care through information and information technology. With guidance from eHI's multi-stakeholder Leadership Council, the Drug Safety Collaboration involves three leading pharmaceutical companies — Pfizer Inc., Johnson & Johnson, and Eli Lilly and Company—and two community-based healthcare organizations with advanced stage clinical information systems—Partners HealthCare System, Inc. in Massachusetts and the Indiana Network for Patient Care, run by the Regenstrief Institute.

The Drug Safety Collaboration is using three "use cases" to test and evaluate the value and utility of using electronic clinical and administrative health information to detect and evaluate drug safety signals: the use of cholesterol-lowering drugs and laboratory results related to liver failure, warfarin-related bleeding episodes, and adverse patient events commonly associated with medications, called "designated medical events." Lessons gathered from the "learning laboratories" in Boston and Indianapolis will be documented and converted into technical guides and tools that will be made widely available to the public to stimulate advancement of drug safety efforts.

The collaborators realized that the legal issues in a drug safety project are significant. The Drug Safety Collaboration thus commissioned the law firm of Coppersmith Gordon Schermer & Brockelman PLC to produce an extensive legal guidance to cover all of the major legal issues involved in drug safety collaborations involving Health Information Exchanges (HIE), health systems and pharmaceutical companies, and two template agreements: an agreement between an HIE and its participants that would allow the HIE to utilize the information in the HIE for drug safety purposes, and an agreement between an HIE and a pharmaceutical company to govern the terms and conditions of a drug safety project, designed to ensure rigorous patient confidentiality and security. This document provides guidance to the numerous legal issues involved in drug safety surveillance (called "pharmacovigilance" throughout this report), utilizing electronic clinical information. The template agreements are published in separately documents.

The eHI Connecting Communities for Drug Safety Collaboration is intended to contribute to the creation of an active drug safety surveillance system in the U.S., which is a key provision of the recent Food and Drug Administration Amendments Act (FDAAA) of 2007. The Collaboration expects the findings from its learning laboratories to contribute to and build off of the efforts of the Reagan-Udall Foundation, a new private and independent non-profit organization established by Congress under the FDAAA. The mission of the Foundation is to identify and help to address the unmet scientific needs in the development, manufacture, and evaluation of the safety and effectiveness of FDA-regulated products.

B. The Policy Background: Concern with "Secondary Uses" of Electronic Clinical Information

Using electronic clinical information promises to accelerate the timeliness, accuracy, and effectiveness of methods currently used to monitor drug safety and facilitate response by the health care system. The use of clinical information for a pharmacovigilance project, however, must be conducted with detailed

attention to protecting the privacy and security of individual health information. Individual consumer trust is essential to build public support for using electronic health information for pharmacovigilance. Consumer trust is built through creating transparency about how health information is used, involving trusted parties such as health care providers and hospitals as collaborators in a pharmacovigilance program, and ensuring unwavering attention to the privacy and security of health information utilized in the program.

Building consumer trust in a pharmacovigilance program takes place in the context of growing public attention to "secondary uses" of health information—uses beyond the care and treatment of the individual. Many developing HIEs across the country are struggling with the policy decisions about whether, and under what conditions, the information in an HIE should be used for purposes beyond the care of the specific individual. While HIEs understand that use of health information for non-treatment purposes has the possibility of wide benefit to their communities—improvement of care at particular institutions, public health surveillance, research, and drug safety surveillance, among other important public goals—many policy makers involved in the creation of HIEs are wary of expanding the scope of the use of HIEs beyond treatment without a framework governing the parameters for these non-treatment activities.

This legal guidance is part of eHI's work to create such a framework. The eHI Connecting Communities for Drug Safety Collaboration will be an important step in establishing a national consensus for how to approach the technical, policy and legal issues involved in the use of electronic health information for pharmacovigilance programs.

In addition, the National Committee on Vital and Health Statistics (NCVHS) released its report, "Enhanced Protections for Uses of Health Data: A Stewardship Framework for 'Secondary Uses' of Electronically Collected and Transmitted Health Data" on December 19, 2007, which addresses other non-treatment uses for health information.[1] The Office of the National Coordinator for Health Information Technology (ONC) asked NCVHS to develop a policy framework that would "balance the benefits, sensitivities, obligations, and protections" of secondary uses. ONC recognized that a framework for secondary use of health data "increases in importance as health care moves from paper to electronic and from point-to-point data exchange to the vision of a nationwide health information network (NHIN)." The NCVHS recommendations were presented to the American Health Information Community at its November 13, 2007 meeting. [2] In its report, NCVHS makes specific recommendations about a national framework for secondary uses of electronic health information. Some of these recommendations, if adopted by HHS, would result in significant changes in the national privacy landscape. For example, NCVHS cites an increasing need to adopt data stewardship principles by all entities with access to health data, independent of whether entities are presently "covered entities" under HIPAA. NCVHS also recommends that HHS restrict the allowable uses of data that are "de-identified" under HIPAA.

Because so called "secondary uses" of electronic health information are under considerable scrutiny and there are legitimate and forceful arguments supporting different policy outcomes, the participants in a pharmacovigilance program should pay close attention to the developing policy in this area.

C. What This Legal Guidance Covers

We examine a number of legal issues applicable to health systems, HIEs and pharmaceutical companies conducting a pharmacovigilance program with electronic health information.

---

[1] *See* http://www.ncvhs.dhhs.gov/071221lt.pdf.

[2] *See* http://www.os.dhhs.gov/healthit/community/meetings/m20071113.html.

- Privacy: We examine how numerous privacy laws affect a pharmacovigilance program, including HIPAA, federal alcohol and substance abuse treatment program regulations, the Privacy Act, Medicare Conditions of Participation, and categories of state health information confidentiality statutes, including those protecting genetic testing, mental health, HIV/AIDS information.

- Human Subject Research Compliance: We discuss a variety of issues that arise if the pharmacovigilance program is structured as a research protocol, including whether it is "human subject research" under the Common Rule, whether it would be exempt from IRB review, whether it would be subject to expedited review by the Chair, the criteria applied for IRB approval, guidance on the elements to consider in waiving informed consent, and when institutions may designate an outside IRB to review a pharmacovigilance protocol.

- Food and Drug Administration (FDA) Reporting Obligations: We discuss drug manufacturers' obligations to report adverse drug experience information to the FDA for "solicited sources" and "spontaneous sources," and discuss voluntary reporting by HIEs and health systems.

- Food and Drug Act Administration Amendments Act of 2007 (FDAAA): We discuss the FDAAA and its potential impact on pharmacovigilance programs.

- Tort Liability: We discuss manufacturer, HIEs and health system potential liability for failure to warn of drug risks uncovered during a pharmacovigilance program.

The legal issues for HIEs, health systems and pharmaceutical companies engaging in pharmacovigilance programs are quite complicated, but we believe the legal risk is not high as long as the program is carefully constructed. The program must include a rigorous plan to protect the privacy and security of the health information evaluated and must minimize the use of individually identifiable health information to the extent possible. Moreover, the pharmaceutical company participants must follow FDA reporting obligations and communicate significant new findings of risk to health care providers. Of course, these issues have yet not been examined by courts in the context of pharmacovigilance programs, so we urge HIEs, health systems and pharmaceutical companies participating in pharmacovigilance programs to track the progress of issues noted in this guidance and closely evaluate the applicable laws in their jurisdictions.

II. Privacy Compliance Issues

The use of health information for any purpose outside of the treatment of individual patients poses obvious concerns about the privacy and confidentiality of individual health information. In order for pharmacovigilance programs to be successful in the long run, consumers must trust that their health information will be treated confidentially and used appropriately. The public perceives the "increasing use of interconnected electronic information systems as one of the greatest threats to medical privacy."[3] Rigorous confidentiality protection for the health information handled by health systems and HIEs is therefore essential. As the federal Department of Health and Human Services (HHS) has stated, "the entire health delivery system is built upon the willingness of individuals to share the most intimate details of their lives with their health providers."[4] In enacting the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Congress recognized that adequate protection of the privacy and security of health information is a "*sine qua non* of the increased efficiency…brought about by the

[3] 65 Fed. Reg. 82,465.
[4] 65 Fed. Reg. 82,467 (Dec. 28, 2000).

electronic revolution,"[5] and the protection of medical privacy is essential for access to "effective, high quality health care."[6]

The plethora of federal and state laws governing the confidentiality of health information complicates the analysis of privacy compliance in a pharmacovigilance program. This section discusses federal confidentiality laws, including HIPAA, the federal alcohol and drug treatment program regulations, and the federal Privacy Act and Medicare Conditions of Participation, and then discusses various *categories* of confidentiality laws typically found at the state level. Each health system or HIE considering participating in a pharmacovigilance program should pay careful attention to how laws applicable in their individual jurisdictions will affect such a program.

A. The Health Insurance Portability and Accountability Act (HIPAA)[7]

1. HIPAA's Application to a Pharmacovigilance Program: Participants as HIPAA Covered Entities or Business Associates

HIPAA and its regulations present the most obvious privacy and confidentiality requirements that apply to the use of individual health information. The HIPAA compliance challenges and their resolution will depend on the source of the information for the pharmacovigilance program and the participants in the program. HIPAA applies to health plans, health care clearinghouses, and health care providers that engage in electronic standard transactions such as billing (called "HIPAA covered entities").[8] The federal regulations that implement HIPAA—the HIPAA Privacy Rule[9] and the HIPAA Security Rule[10]—create detailed rules for how HIPAA covered entities may use and disclose health information and how they must protect that information.

One category of anticipated participants in a pharmacovigilance program likely will be HIPAA covered entities—health systems, hospitals and other health care providers that have treatment relationships with individuals—as most providers engage in electronic transactions such as billing. Any use or disclosure of health information by health care providers participating in a pharmacovigilance program likely must comply with the HIPAA Privacy Rule and Security Rule.

An HIE may or may not be a HIPAA covered entity, depending on its specific functions. HIE clinical data exchange functions will not make the HIE a health plan (defined as an individual or group health plan that pays the cost of medical care) or a health care provider (defined as someone furnishing, billing or being paid for health or medical services in the normal course of business).[11] However, it is possible that an HIE will meet the definition of a health care clearinghouse, depending on its specific functions.

HIPAA defines a health care clearinghouse as

---

[5] 65 Fed. Reg. 82,474.
[6] 65 Fed. Reg. 82,467; *see also Jaffee v. Redmond*, 116 S. Ct. 1923, 1928 (1996).
[7] HIPAA, Pub. L. No. 104-191 (Aug. 21, 1996), §§ 261-264, enacting Social Security Act §§ 1171-1179, codified at 42 U.S.C. § 1320d-2 *et seq*.
[8] 45 C.F.R. § 160.102 ("(a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this sub-chapter."); § 160.103 (defining "covered entity"). *See also* the HIPAA covered entity decision analysis tool published by the Centers for Medicare and Medicaid Services, at http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/CoveredEntitycharts.pdf.
[9] 45 C.F.R. Part 160 and Part 164, Subpart E.
[10] 45 C.F.R. Part 160 and Part 164, Subpart C.
[11] 45 C.F.R. § 160.103.

> a public or private entity, including a billing service, repricing company, *community health management information system or community health information system,* and "value-added" networks and switches, that does either of the following functions:
>
> (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
>
> (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information [in the standard transaction] into nonstandard format or nonstandard data content for the receiving entity.[12]

Some HIEs are acting as traditional clearinghouses and providing billing functions for health care providers, processing claims into the required "standard transaction" formats for transmission to health plans. Those functions would make such HIEs "covered entities" under HIPAA.

It is less clear whether the processing of clinical data into a standard format for purposes other than billing (or other electronic financial and administrative transactions under HIPAA) would render an HIE a HIPAA covered entity. For example, some HIEs may take non-standard information from providers and reformat that information into normalized clinical information for presentation in a clinical abstract or continuity of care record. That *may* meet the definition in section (1) above (processing or facilitating the processing "of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.") In its covered entity decision tool, the Centers for Medicare and Medicaid Services (CMS) explains that a "'standard transaction,' for purpose of this definition, is a transaction that complies with the standard for that transaction that the Secretary adopted in 45 CFR Part 162. See 45 CFR 162.103. " So, CMS has clarified reformatting of clinical data would not be a "standard transaction" under HIPAA. It has not explained, however, whether the reformatting of clinical data would be processing "nonstandard data content into standard data elements," which is not defined in the regulations.

"HHS's inclusion of 'community health management information system' and 'community health information system' as examples in the definition could lend weight to the conclusion that an entity performing HIE functions might be considered a health care clearinghouse if the functions described above were performed or facilitated" by the HIE.[13] On the other hand, the purpose of the HIPAA Transactions and Code Set regulations (45 C.F.R. Part 162) was to establish rules for the electronic transmission of the common financial and administrative business in the health care industry, such as billing, payments, referrals, etc. So, we think it unlikely that HHS would treat the reformatting of clinical data as a health care clearinghouse function, but that conclusion remains uncertain.

In any event, most HIEs will be HIPAA business associates of the health care providers participating in the health information exchange and thus will be required to comply with many of the HIPAA requirements as a contractual matter. The HIPAA regulations define a "business associate" as

---

[12] 45 C.F.R. § 160.103 (emphasis added).

[13] *See, The Quest for Interoperable Electronic Health Records: A Guide to Legal Issues in Establishing Health Information Networks* (American Health Lawyers Association, 2006) ("Although these terms were part of the original definition of health care clearinghouse in the November 3, 1999 Notice of Proposed Rulemaking for the Privacy Rule, HHS has not explained their meaning in depth. *See* 64 Fed. Reg. at 59,227 and 59,930 (Nov. 3, 1999); 65 Fed. Reg. at 82,477 and 82,572 (Dec. 28, 2000).).

a person who:

(i) On behalf of [the covered entity] … performs, or assists in the performance of:
  (A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
  (B) Any other function or activity regulated by this sub-chapter; or

(ii) Provides … legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this sub-chapter), management, administrative, accreditation, or financial services to or for such covered entity… where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.[14]

An HIE will be handling individually identifiable health information on behalf of participating health care providers for treatment purposes, a function regulated by HIPAA. The HIE thus will be the participating providers' business associate and will be subject to many of the HIPAA regulatory restrictions by virtue of contract, rather than direct regulatory application.[15] In the following discussion, we therefore assume that an HIE, even if not a HIPAA covered entity, will "step into the shoes" of its covered entity partners and will follow the HIPAA regulations.

The pharmaceutical company partners in a pharmacovigilance program will not meet the definition of a HIPAA covered entity. Whether the pharmaceutical companies will be HIPAA business associates will depend on the particular circumstances of how the relationship is structured. For example, if the company de-identifies the electronic health information that will be used for the project, the company will be acting as the covered entity's HIPAA business associate because the company will be performing a function on behalf of the covered entity that involves individually identifiable information. If the pharmaceutical company is acting as a business associate of the HIPAA covered entity, the covered entity must have a business associate agreement in place before the exchange of information that meets the requirements of the HIPAA Privacy Rule.[16] However, unless the company performs a de-identification function, in most other circumstances it will not be acting as a business associate of the covered entity partners in the project.[17]

2. Pharmacovigilance Program Utilization of Protected Health Information

The HIPAA regulations protect all "individually identifiable health information" handled by a covered entity. If information is individually identifiable, the Privacy Rule protects that information in all forms, including paper records, oral communications, and electronic information. This information is called "Protected Health Information" ("PHI").[18]

---

[14] 45 C.F.R. § 164.103 (defining "business associate").

[15] 45 C.F.R. § 164.502(e) (requirements for business associates); § 164.504(e) (same).

[16] *Id.*

[17] In the research context, the Office for Civil Rights has concluded that a researcher is <u>not</u> a business associate of the covered entity that provides the information for research, unless the researcher de-identifies the covered entity's health information to use for the research.

[18] 45 C.F.R. § 164.501 (defining PHI).

Breaking down the definition, health information[19] is "individually identifiable" if it meets three criteria:

(1) The information is created or received by a health care provider, health plan, employer, or health care clearinghouse;
(2) The information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present of future payment for the provision of health care; and
(3) The information identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual.[20]

Essentially, all information that identifies a health care provider's patients or a health plan's members, including even basic demographic information that comes from these entities, is treated as "individually identifiable health information" and thus as PHI under the HIPAA Privacy Rule.

If a covered entity "de-identifies" its information, then the HIPAA Privacy Rule does not govern the use and disclosure of that information. HIPAA permits two methods of de-identifying information[21]: (1) removing or coding the HIPAA "identifiers"; or (2) statistical de-identification. HIPAA identifiers include all of the following data about individuals and their family members, household members, or employers:

- Name;
- Street address, city, county, precinct, or zip code (unless only the first three digits of the zip code are used and the area has more than 20,000 residents);
- The month and day of dates directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death;
- Age if over 89 (unless aggregated into a single category of age 90 and older);
- Telephone numbers;
- Fax numbers;
- Email addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers, serial numbers, and license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses;
- Biometric identifiers, such as fingerprints
- Full-face photographs and any comparable images; or
- Any other unique identifying number, characteristic, or code.

[19] "Health information" is defined as "any information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, Health Plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103.
[20] 45 C.F.R. § 164.501; § 164.514(a).
[21] 45 C.F.R. § 164.514(a)-(b).

If the covered entity has actual knowledge that, even with these identifiers removed, the remaining information could be used alone or in combination with other information to identify the individual, then the information still must be treated as PHI.

The identifiers can also be coded, so that no identifiers are released. The code may not be derived from any information about the patient or plan member. For example, the code may not be derived from the individual's social security number, medical record number or name (such as initials), and may not be capable of being translated to identify the individual.

A covered entity may have one of its employees or a third party de-identify the PHI before use or disclosure of the information. This process of de-identifying PHI is treated as a covered entity "health care operation," which may be done without the individual's authorization.[22] If the covered entity uses a third party (non-employee) to de-identify the information, the covered entity must first have a "business associate agreement" in place with that third party.[23] After the de-identification process, the business associate may not retain the fully identifiable information.

The second option for de-identifying PHI is to have a qualified statistical expert determine that the risk is very small that the identifiers present could be used alone, or in combination with other available information, to identify the patient.[24] The statistical expert must be a person with knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information non-individually identifiable, and must document the methods and results of the analysis that justifies the conclusion of very small risk.[25] The HIPAA covered entity must keep this documentation for six years.

De-identification probably will not be a practical option for a pharmacovigilance program, although of course that will depend on the particular target of the program. Our understanding is that, while pharmacovigilance programs generally will not need direct identifiers such as name, address, and social security number, the programs will need access to some HIPAA identifiers—particularly dates of service—to determine whether a particular drug potentially caused a particular safety event. Moreover, if a potential drug safety event is identified, many programs will want to examine that individual's medical records to determine if the drug may have caused the safety event or if other factors in the individual's health condition or care caused or contributed to the event. However, if a health system or HIE has the ability to code the information it holds and to unlink the code only if that future information is required, it is possible at least that the first stage of the pharmacovigilance process could be conducted with de-identified information. Again, the participants should carefully examine this issue to determine whether and to which HIPAA identifiers they need access.

If only partially de-identified information will accomplish the program's objectives, the parties may be able to conduct the program under a "Limited Data Set." A Limited Data Set excludes all of the "identifiers", except that a Limited Data Set may include: (1) geographic designations above the street level or PO Box; (2) dates directly related to a patient, such as dates of service, birth date, admission date, discharge date, or date of death; or (3) any other unique identifying number, characteristic, or code that is not expressly listed as an "identifier."[26] The personnel who access, review, collect, or receive a Limited Data Set must sign a "Data Use Agreement" in which they agree to protect the confidentiality of the information.[27] This requirement applies to internal personnel, as well to outside parties.

---

[22] 45 C.F.R. § 164.501 (defining health care operations); 45 C.F.R. § 164.506 (use or disclosure of PHI for health care operations).
[23] 45 C.F.R. § 164.502(e); 45 C.F.R. § 164.504(e).
[24] 45 C.F.R. § 164.514(b).
[25] *Id.*
[26] 45 C.F.R. § 164.514(c).
[27] *Id.*

The following section describes appropriate use and disclose of PHI for a pharmacovigilance program, where information cannot be de-identified or included in a Limited Data Set.

3. Use and Disclosure of Protected Health Information in a Pharmacovigilance Program

The HIPAA Privacy Rule comprehensively regulates the internal use and external disclosure of PHI by covered entities. The Privacy Rule permits HIPAA covered entities to use or disclose health information without patient permission for basic health care functions, such as treating patients, getting paid for that treatment, and operating the health care organization (called "health care operations").[28] The Privacy Rule also permits HIPAA covered entities to disclose health information for a variety of public purposes, where the public interest in release of the individual's information outweighs the individual's interests in controlling the information, such as disclosures for public health activities and research.[29] HIPAA covered entities generally must get permission from the individual (called an "authorization") to use or disclose the individual's PHI for any purpose not expressly permitted by the regulations.

Obtaining individual authorization to access medical records for a pharmacovigilance program would be difficult and expensive. Large health systems and HIEs maintain hundreds of thousands, if not millions, of records. The process of contacting these patients—many of whom may not be at the address of record—would be time consuming and entail considerable expense. We will assume, then, that these pharmacovigilance programs will proceed if possible without patients' authorization to have their records included in the analysis. We thus look at other feasible options for pharmacovigilance program HIPAA compliance.

---

[28] 45 C.F.R. § 164.506.

[29] 45 C.F.R. § 164.512. "These public purpose" disclosures include disclosures of health information that are:

(1) Required by law;
(2) For certain public health activities, such as communicable disease reporting and child abuse reporting;
(3) About victims of abuse, neglect or domestic violence;
(4) For health oversight activities, such as to a state department of health services to regulate the health care organization;
(5) For judicial and administrative proceedings, such as in response to court orders or subpoenas;
(5) For certain law enforcement purposes, such as when presented with a search warrant or to identify a missing person;
(6) To coroners, medical examiners and funeral directors about deceased persons;
(7) For cadaveric organ, eye or tissue donation purposes;
(8) For research;
(9) To avert a serious threat to health or safety;
(10) For certain government functions, such as military and veterans activities, national security and intelligence, protective services for the President, correctional organizational custodial situations, or government programs providing public benefits; and
(11) For workers' compensation.

a. Use and Disclosure for Public Health Purposes

The HIPAA Privacy Rule permits a variety of PHI disclosures for public health purposes,[30] two of which may apply in the context of a pharmacovigilance program. First, HIPAA permits a covered entity to release health information to a person or company subject to the FDA's jurisdiction "with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity" including:

> (A) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
>
> (B) To track FDA-regulated products;
>
> (C) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback); or
>
> (D) To conduct post marketing surveillance.[31]

The pharmaceutical company partners in a pharmacovigilance program are subject to the FDA's jurisdiction with regard to drugs monitored under such a program. Moreover, because post-marketing surveillance is not limited under the HIPAA regulations to post-marketing studies regulated by the FDA (Phase IV studies), a pharmacovigilance program should meet this requirement.[32]

Second, HIPAA permits a covered entity to release health information to a "public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority."[33] A "public health authority is defined as "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, *or a person or entity acting under a grant of authority from or contract with such public agency*, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."[34]

---

[30] 45 C.F.R. §164.512(b).

[31] *Id*.

[32] *See* Preamble, HIPAA Privacy Rule, 65 Fed. Reg. at 82525 (Dec. 28, 2000) ("The terms included in Sec. 164.512(b)(iii) are intended to have both their commonly understood meanings, as well as any specialized meanings, pursuant to the Food, Drug, and Cosmetic Act (21 U.S.C. 321 et seq.) or the Public Health Service Act (42 U.S.C. 201 et seq.). For example, "post-marketing surveillance" is intended to mean activities related to determining the safety or effectiveness of a product after it has been approved and is in commercial distribution, as well as certain Phase IV (post-approval) commitments by pharmaceutical companies. With respect to devices, "post-marketing surveillance" can be construed to refer to requirements of section 522 of the Food, Drug, and Cosmetic Act regarding certain implanted, life-sustaining, or life- supporting devices.").

[33] 45 CFR 164.512(b).

[34] 45 CFR 164.501 (emphasis added).

This public health exception is a feasible option if the FDA agrees to designate the participants in a pharmacovigilance program (or one of the participants) to act under a grant of authority from the FDA to collect post-marketing drug safety surveillance information. The FDA is very interested in improving post-marketing drug safety surveillance (see Section V regarding the Food and Drug Administration Amendments Act of 2007), and an FDA-designation to the participants in a private surveillance system may be a feasible option in the future.

b. Use and Disclosure for Research

(1) Public Health Surveillance Versus Research

Many pharmacovigilance programs will be structured as research programs. Whether a particular pharmacovigilance program is "research" or a public health activity may be a difficult call, however, as the distinction between public health surveillance activities and research is sometimes a thin one.

The HIPAA Privacy Rule (and the Common Rule, see section III) defines "research" as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[35] A 1999 report by the Centers for Disease Control (CDC) explored the differences between public health surveillance activities and research.[36] The CDC explained:

> The key word in the regulations' definition of research for the purpose of classifying public health activities as either research or non-research is "designed." The major difference between research and non-research lies in the primary intent of the activity. The primary intent of research is to generate or contribute to generalizable knowledge. The primary intent of non-research in public health is to prevent or control disease or injury and improve health, or to improve a public health program or service. Knowledge may be gained in any public health endeavor designed to prevent disease or injury or improve a program or service. In some cases, that knowledge may be generalizable, but the primary intention of the endeavor is to benefit clients participating in a public health program or a population by controlling a health problem in the population from which the information is gathered.[37]

More helpfully, the CDC also explained that public health surveillance involves the collection and analysis of health-related data conducted to monitor the frequency of occurrence and distribution of disease or a health condition in the population:

> Surveillance systems that most easily fit into this category are ones in which the data are limited to describing the occurrence of a health-related problem (disease reporting) and systems in which non-analytic (etiologic) analyses can be conducted. Subjects are rarely selected according to a design; rather, all cases are entered into the surveillance system because they are passive reporting systems.[38]

In contrast, the CDC explains that surveillance systems are

---

[35] 45 C.F.R. § 164.501.

[36] Centers for Disease Control, *Guidelines for Defining Public Health Research and Public Health Non*-Research (Oct. 4, 1999) at http://www.cdc.gov/od/science/regs/hrpp/researchDefinition.htm.

[37] *Id.*

[38] *Id.*

> likely to be research when they involve the collection and analysis of health-related data conducted either to generate knowledge that is applicable to other populations and settings than the ones from which the data were collected or to contribute to new knowledge about the health condition.... Characteristics of surveillance systems that most easily fit into this [research] category are: longitudinal data collection systems (e.g. follow-up surveys and registries) that allow for hypothesis testing; the scope of the data is broad and includes more information than occurrence of a health-related problem; analytic analyses can be conducted; and cases may be identified to be included in subsequent studies.[39]

While the CDC's guidance is not binding law, its guidance is a useful demonstration of the distinction HHS is likely to draw between public health surveillance functions and research.

Whether a pharmacovigilance program falls into public health surveillance or whether it is "research" will depend on the specific characteristics of the program. Programs that attempt to determine whether a specific drug potentially caused a specific event are etiologic analyses (i.e. they look to the cause of the event) and would be research. Programs that collect safety events that are potentially correlated with drugs, but do not attempt to determine the causation of those events, would not be etiologic analyses and thus would not be research. The participants in the pharmacovigilance program thus will need to evaluate whether and at what stage of the program adverse event causation is determined. For example, if the health system or HIE simply collects information about safety events and transmits that information to the pharmaceutical partners for evaluation, the HIE or health system itself would not be involved in research. An HIE or health system developing a pharmacovigilance program will need to work carefully with individuals knowledgeable about the research process to determine whether the program meets the definition of "research."

(2) Use and Disclosure of PHI for Research

If the participants in the pharmacovigilance program determine that the HIE or health system indeed would be involved in research, they should ensure that they meet one of the HIPAA Privacy Rule's requirements. Under the HIPAA Privacy Rule, covered entities may use PHI internally for research or disclose PHI externally to third parties for research only if the requirements of at least one of the nine rules below are met, [40] some of which have been discussed separately in this paper:

1. The research involves only de-identified data;

2. The research uses or discloses a Limited Data Set and the covered entity has a Data Use Agreement in place with the recipient of the PHI;

3. The research subject or the subject's authorized representative has signed a written HIPAA authorization;

4. An IRB has waived the requirement for authorization;

5. The activities are just to prepare for research and required representations are obtained from the researchers;

---

[39] *Id*.

[40] 45 C.F.R. § 164.512(i) (general rules for use and disclosure of patient information for research). Other HIPAA rules are cited as applicable.

6. The use or disclosure is for patient recruitment purposes by a treating provider;

7. The research involves only the information of decedents and required representations are obtained from the researchers;

8. The disclosure of the PHI is required by law; or

9. The research is "grandfathered" under the HIPAA rules.

The HIPAA rules apply both to internal use (including employees accessing, collecting, or otherwise using PHI) and to access by or disclosure to third parties outside of the HIPAA covered entity.

We addressed de-identification, creation of a Limited Data Set, and collection of HIPAA authorizations in the discussion above. In this section, we address the IRB waiver of HIPAA authorization. (The other HIPAA options for research will not work in the context of a pharmacovigilance program. These include activities to prepare for research,[41] use or disclosure of PHI for recruitment of research participants,[42] research involving only the information of decedents,[43] disclosures that are required by law,[44] or research that is "grandfathered" under the HIPAA Privacy Rule.[45])

---

[41] If researchers merely want to access, review or collect PHI to prepare for research, such as a records review to determine which patients may be appropriate subjects, researchers may obtain that information if they provide the covered entity with the following representations in writing:

1. The PHI is sought solely to prepare for research;
2. The PHI is necessary to prepare for research; and
3. No information identifying individuals will be removed from the premises in the course of the review.

If researchers will need to remove the information from the covered entity premises to review it, the researchers must ask the IRB to waive authorization instead, or another HIPAA option must be satisfied.

[42]HIPAA permits the use or disclosure of PHI for patient recruitment. First, a health care provider may contact the provider's own patients to determine if the patients are interested in participating in a clinical trial. If the provider or the provider's employees contact the providers' own patients, that use of PHI is for either "treatment" or "health care operations" purposes, both of which are permitted without patient authorization under HIPAA. The health care provider also may use a non-employed third party (including the researcher) to contact patients for recruitment purposes, but the provider first must have a business associate agreement in place with the third party. Finally, the researcher can request an IRB to partially waive authorization, so that authorization is not required for the initial contact, but will be sought for enrollment in the study. Contacting patients for recruitment is not a "preparatory to research" activity. *See* OHRP, *Clinical Research and the HIPAA Privacy Rule*, p. 4 (NIH 6/22/04), at http://privacyruleandresearch.nih.gov/clin_research.rtf ("Under the "preparatory to research" provision, covered entities may use or disclose PHI to researchers to aid in study recruitment. The covered entity may allow a researcher, either within or outside the covered entity, to identify, but not contact, potential study participants under the "preparatory to research" provision.").

[43] Where the research involves only the information of deceased individuals, researchers may access this information if they provide the covered entity with the following representations in writing:

1. The use or disclosure of information is sought solely for the research on the information of decedents;
2. The information is necessary for the research; and
3. The researcher will provide documentation of the death of the research participants upon request.

[44] 45 C.F.R. § 164.512(a).

[45] 45 C.F.R. § 164.532(c) (research is grandfathered if the participant signed an informed consent before April 14, 2003) (and the informed consent has not been modified since that date) or if the IRB waived informed consent before April 14, 2003).

To have the IRB grant a request to waive HIPAA authorization, the researcher must demonstrate three things:

1. The use or disclosure of the subjects' identifiable information involves no more than minimal risk to their privacy, based on: (a) an adequate plan to protect information identifying the subjects from improper use and disclosure; (b) an adequate plan to destroy information identifying the subjects at the earliest opportunity consistent with conduct of the research (unless there is a health or research justification for retention or if retention is required by law); and (c) adequate written assurances that the information identifying the subjects will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the study, or for other research permitted by the rules;

2. The research could not practicably be conducted without the waiver or alteration of authorization; and

3. The research could not practicably be conducted without access to and use of information identifying the subjects.[46]

With appropriate confidentiality protections in place, many IRBs would approve waiver of HIPAA authorization for a pharmacovigilance program. Because these programs seek to evaluate all records held by a health system or HIE, the program is potentially examining huge numbers of patient records. Indeed, the more patient records that are evaluated, the greater number of safety events will be identified and the more rigorous the conclusions will be regarding causation. However, it would be exceedingly difficult and expensive to contact all patients whose records are housed in a system's EHR or an HIE—many patients would not be at the address of record and efforts to contact them would require substantial personnel time and expense. We believe that an IRB could conclude, then, that the research could not practicably be conducted without a waiver of authorization (element #2).

The researchers would also have to demonstrate to the IRB that the research could not practicably be conducted without access to and use of individually identifiable information (element #3). As discussed above in the section on de-identification, complete de-identification probably will not be a practical option for a pharmacovigilance program. Our understanding is that, while a pharmacovigilance program generally will not need direct identifiers such as name, address, and social security number, the programs will need access to some HIPAA identifiers—particularly dates of service—to determine whether a particular drug potentially caused a particular safety event. Moreover, if a potential drug safety event is identified, many programs may want to examine that individual's complete medical records to determine if the drug may have caused the safety event or if other factors in the individual's health condition or care caused or contributed to the event. The participants should carefully examine this issue to determine whether and to which HIPAA identifiers they need access.

Finally, the researchers will need to demonstrate to the IRB that the protocol poses no more than minimal risk to patients' privacy (element #1). They must have a plan to protect the patient information from improper use and disclosure. For example, the research plan might commit to keeping all PHI on site for the research project to reduce the security risks in electronic transmission of the information or require rigorous encryption or other secure method of electronic transmission. Another option might be to screen out all direct identifiers, such as name, address and social security number so that any risk of identification of an individual is low. The IRB also will require the researchers to destroy information identifying the subjects at the earliest opportunity consistent with conduct of the research (unless there is a health or research justification for retention or if retention is required by law); this will apply to any separate data files created for the research purposes. The IRB also will require written assurances from

[46] 45 C.F.R. § 164.512(i).

the researchers that the individually identifiable information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the study, or for other research permitted by the rules. The contract between the health system or HIE and the pharmaceutical companies should reflect this restriction.

c. Use and Disclosure for Health Care Operations

Another potential option for HIPAA compliance is to treat the collection and analysis of drug safety data for a pharmacovigilance program as "health care operations" under HIPAA,[47] which are defined as including "quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; *population-based activities relating to improving health* or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment…"[48] We examine here whether pharmacovigilance falls within "population-based activities relating to improving health."

Population-based activities are not defined in the HIPAA regulations, but the Preamble to the HIPAA regulations indicates that an analysis applied across an entire patient population that does not result in the treatment of an individual may be treated as population-based activities. HHS explains:

> We do not agree that population based services should be considered treatment activities. The definition of "treatment" is closely linked to the Sec. 160.103 definition of "health care," which describes care, services and procedures related to the health of an individual. The activities described by "treatment," therefore, all involve health care providers supplying health care to a particular patient. While many activities beneficial to patients are offered to entire populations *or involve examining health information about entire populations*, treatment involves health services provided by a health care provider and tailored to the specific needs of an individual patient. Although a population-wide analysis or intervention may prompt a health care provider to offer specific treatment to an individual, we consider the population-based analyses to improve health care or reduce health care costs to be health care operations (see definition of "health care operations," above).[49]

At another point in the Preamble, however, HHS appears to require the population-based activities to have application to the individual covered entity's development of treatment protocols to help its own patients or health plan members:

> We add population-based activities to improve health care or reduce health care costs to the definition of health care operations. Outreach programs as described by the commenter may be considered either health care operations or treatment, depending on whether population-wide or patient-specific activities occur, and if patient-specific, whether the individualized communication with a patient occurs on behalf of health care provider or a health plan. For example, a call placed by a nurse in a doctor's office to a patient to discuss follow-up care is a

[47] 45 C.F.R. § 164.506.

[48] 45 CFR 164.501 (defining health care operations) (emphasis added).

[49] 65 Fed. Reg. at 82626 (Dec. 28, 2000).

> treatment activity. The same activity performed by a nurse working for a health plan would be a health care operation. In both cases, the database analysis that created a list of patients that would benefit from the intervention would be a health care operation.

Moreover, the definition of health care operations makes clear that research activities are excluded, as health care operations do not include outcomes evaluation and development of clinical guidelines if "obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities."[50] Finally, to utilize the health care operations exception, the covered entity would have to determine that the disclosure was for the *entity's* health care operations, not the HIE's or a non-covered entity recipient.[51]

Because the scope of "population-based activities" is unclear, and because of the restrictions on releasing information to non-covered entities for health care operations purposes, the participants should strive to meet the public health or research HIPAA rules, if it is not possible to de-identify the information for the pharmacovigilance program.

4. Compliance with the HIPAA Security Rule

A HIPAA covered entity participating in a pharmacovigilance program must follow the HIPAA Security Rule in its handling of PHI. The Security Rule requires administrative, technical, and physical security safeguards to protect health information in electronic form.[52] The Security Rule has detailed standards that implement four basic requirements:

- To ensure the confidentiality, integrity, and availability of all electronic PHI the entity creates, receives, maintains, or transmits;
- To protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- To protect against any reasonably anticipated uses or disclosures of the information that are not permitted under the Privacy Rule; and
- To ensure that the entity's workforce complies with the Security Rule.[53]

For example, covered entities must take measures to shield electronic health information against outside hackers, to protect the hardware on which electronic health information is stored, to protect the facilities that house that hardware, and to preserve the retrievability of electronic health information in natural disasters or physical emergencies.

A covered entity's conduct of a pharmacovigilance program does not pose any additional challenges for compliance with the HIPAA Security Rule, and we thus do not include a detailed discussion of the HIPAA security requirements. The entity should apply its normal rigorous security requirements to the storage and transmission of the electronic PHI accessed and generated as part of the pharmacovigilance program. For example, a covered entity is required to implement technical policies and procedures to allow access to information systems and electronic PHI only to individuals or software that have been granted access rights under the entity's access policies;[54] any access granted to third parties under a pharmacovigilance program must comply with the entity's policies on access control. The Security Rule also requires a covered entity to implement procedures preventing the unauthorized access to electronic

---

[50] 45 C.F.R. § 164.501 (defining health care operations) (emphasis added).
[51] 45 C.F.R. § 164.506(c) (restricting disclosures for health care operations).
[52] 45 C.F.R. Part 164, Subpart C.
[53] *Id.*
[54] 45 C.F.R. § 164.312.

transmissions of electronic PHI;[55] any electronic transmission of electronic PHI in the pharmacovigilance program of course should comply with the entity's policies on encryption or otherwise secure transmission of information.

If an HIE or other business associate of covered entities is involved in the pharmacovigilance program, the business associate contract must obligate the business associate to implement "administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains or transmits on behalf of the covered entity."[56] The business associate also must agree to report to the covered entity any security incident of which it becomes aware.[57] This reporting requirement will include any security incident related to the business associate's system, or any of its downstream contracted entities.

B. Federal Alcohol and Drug Abuse Treatment Program Regulations

The federal regulations governing alcohol and drug abuse treatment information, called the "Part 2 regulations" because they are found at 42 Code of Federal Regulations Part2,[58] apply to any "federally assisted" alcohol or drug abuse "program."[59] Some health systems participating in a pharmacovigilance program may own a federally-assisted substance abuse treatment program. While many health systems with such a program segregate this sensitive information from the rest of the information on the system's EHR and it would not be included in the EHR information evaluated through a pharmacovigilance program, that issue requires careful consideration.

Even if a health system or HIE is not directly covered, to the extent that a health system (or an HIE) receives information from other federally-assisted substance abuse treatment programs, that information *may* be protected by the Part 2 regulations. If a federally-assisted substance abuse treatment program obtains patient consent to release the patient's information to the system or HIE, the treatment program must include a written statement that warns the recipient of the information that the recipient may not further disclose the information unless permitted by the Part 2 regulations.[60] A health system or HIE that

---

[55] *Id*.
[56] 45 C.F.R. § 164.514.
[57] *Id*.
[58] See 42 C.F.R. §§ 2.1 through 2.67.
[59] 42 C.F.R. § 2.3. A "program" is a person or entity that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment, or referral for treatment. 42 C.F.R. § 2.11. A program is "federally assisted" if it: (1) is conducted entirely or in part by any federal agency or department (with some exceptions for Veterans Administration and Armed Forces programs); (2) is conducted under a license, certificate, registration, or other authorization from any federal agency or department, including certified Medicare providers, authorized methadone maintenance treatment providers, and programs registered under the Controlled Substances Act to dispense controlled substances for alcohol or drug abuse treatment; (3) is tax-exempt or to whom contributions are tax deductible; or (4) is the recipient of any federal funds. 42 C.F.R. § 2.12(b). The types of programs that may be covered include treatment or rehabilitation programs, employee assistance programs, programs within general hospitals, school-based programs, and private practitioners who hold themselves out as providing, and do provide, alcohol or drug diagnosis, treatment, or referral for treatment, if they are federally assisted. A general medical facility is not a "program" unless it has a discrete, identified unit that holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment, or referral for treatment, so these federal regulations do not have wide applicability.
[60] 42 C.F.R. § 2.32 (requiring written statement: "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR part 2. A general

receives confidential substance abuse information from a substance abuse program, pursuant to a patient's consent, therefore must follow the Part 2 regulations in redisclosing that information. That might occur if the program receives consent to release the information to another treating provider in a non-emergency situation.

If the Part 2 regulations apply to any information held by the health system or the HIE, that information may be used or disclosed only with patient consent or in very limited circumstances.[61] The only exception likely to apply is if the pharmacovigilance program is structured as a research protocol.[62]

The Part 2 regulations require approval of a research protocol by the substance abuse treatment program director and contain greater restrictions on the dissemination of patient identifiers than does HIPAA.[63] Under the Part 2 regulations, identifying information may be released for research only if the program director[64] determines that the recipient:

1. Is qualified to conduct the research;

2. Has a research protocol under which the patient identifying information will be maintained in accordance with the security requirements of the regulations[65] and will only be redisclosed as permitted by the regulations;[66] and

---

authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.").

[61] *See* 42 C.F.R. § 2.12, § 2.13, § 2.51, § 2.52, and § 2.53. These permitted disclosures include:
(1) To communicate internally in connection with duties related to the provision of diagnosis, treatment or referral for treatment of alcohol or drug abuse;
(2) To communicate with an entity that has direct administrative control over the program;
(3) To notify law enforcement officers when a patient commits or threatens to commit a crime on the premises or against program personnel;
(4) To report suspected child abuse and neglect as required by state law;
(5) To medical personnel for the purpose of treating a condition that poses an immediate threat to the health of any individual and that requires immediate medical intervention;
(6) To the Food and Drug Administration ("FDA") for purposes of notifying patients and their physicians of dangers to the health of any individual due to mislabeling, error in manufacture, or the sale of products under FDA jurisdiction;
(7) For research activities, but only if certain protections are followed;
(8) To communicate with "qualified service organizations" (third party business partners that provide data processing, legal services, and other functions for the program); and
(9) Audit and evaluation activities of the program.

[62] 42 C.F.R. § 2.52. Another exception permits release of information to the FDA "for purposes of notifying patients and their physicians of dangers to the health of any individual due to mislabeling, error in manufacture, or the sale of products under FDA jurisdiction." 42 C.F.R. § 2.51. However, that exception is not likely to apply to pharmacovigilance programs, where the immediate release is not to the FDA, but to the participants in the program for evaluation purposes.

[63] 42 C.F.R. § 2.52.

[64] A program director is an individual who is "designated as director, managing director, or otherwise vested with authority to act as chief executive of the organization." 42 C.F.R § 2.11 (definitions).

[65] *See* 42 C.F.R. § 2.16 ("Security for written records. (a) Written records which are subject to these regulations must be maintained in a secure room, locked file cabinet, safe or other similar container when not in use; and (b) Each program shall adopt in writing procedures which regulate and control access to and use of written records which are subject to these regulations.").

3. "Has provided a satisfactory written statement that a group of three or more individuals who are independent of the research project [an IRB] has reviewed the protocol and determined that: (i) The rights and welfare of patients will be adequately protected; and (ii) The risks in disclosing patient identifying information are outweighed by the potential benefits of the research."

C. Other Federal Laws

Two other laws deserve brief mention in a discussion of federal confidentiality requirements. First, Medicare-certified health care providers must follow regulations called "Conditions of Participation." These regulations contain medical record confidentiality requirements, but do not impose greater limitations than the HIPAA Privacy Rule.[67]

Second, the federal Privacy Act[68] applies to federal government agencies that provide health care, such as the Veterans Administration. The Privacy Act's requirements are quite similar to the HIPAA Privacy Rule restrictions.

D. State Health Information Confidentiality Laws

A pharmacovigilance program involving patient information implicates state health information confidentiality laws, as well. Each health system or HIE contemplating such a program should look carefully at its state statutes and regulations to determine whether those state laws impose any additional restrictions on the conduct of the program beyond the federal law requirements discussed above.

It is beyond the scope of this report to cover the laws of all 50 states. We thus address typical *categories* of state laws that health systems and HIEs likely will need to address to conduct a pharmacovigilance program, using different state laws as examples of the analysis that would be applied. Typically, states will have laws that provide additional confidentiality protection for categories of health information that are viewed as more sensitive, in which unauthorized release could lead to stigmatization or discrimination of the individual. These often include genetic testing information, mental health information and substance abuse treatment information, or HIV/AIDS and other communicable disease information.

In determining the effect of state laws on a pharmacovigilance program, participants should examine four discrete questions. First, state health information confidentiality laws have varying applicability to different entities in the health care system. Some state statutes and regulations apply only to certain types of providers; for example, a state's mental health laws may apply only to licensed behavioral health providers. Other state laws may have broader application to any entity or person who handles sensitive information, such as information that an individual has received substance abuse treatment. The first element of analysis for the application of state information laws, then, is to determine their scope of application—do they apply to the proposed participants in the pharmacovigilance program? If these

---

[66] 42 C.F.R. § 2.52(b) (the person conducting the research may not release patient identifying information, except back to the program from which the information was obtained, and may not identify the patient in any report).

[67] *See, e.g.*, 42 C.F.R. § 482.24(a)(3) (requiring hospitals to have a "procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with Federal or State laws, court orders, or subpoenas.").

[68] Privacy Act of 1974, Pub. L. No. 93-579 (1974), 5 U.S.C. § 552a.

laws do apply and create substantial hurdles for the program, the participants may choose to structure the program to exclude that type of health information.

Second, state health information laws often prohibit the release of information without patient consent, except for specific listed exceptions. Some states have fairly broad patient consent requirements, where regardless of the type of information, the state law requires patient consent to release the patient's health information for most purposes, including non-emergency treatment. Other states have laws that permit release of information in ways that mirror HIPAA. The second element of analysis for the application of state health information laws, then, is to determine whether the state laws permit the participants to release an individual's health information—and what type—for the pharmacovigilance program.

Next, while many state laws apply only to external disclosure of health information, some state laws also apply to the internal use of such information. The third element of analysis for the application of state health information laws, then, is to determine whether they apply to external disclosures or to internal use, or both. That may impact the decision of whether to permit outside third parties who are partners in the pharmacovigilance program to access patient-identifying information, or whether all analysis of patient information will be done internally, with only reporting of aggregated information to outside third parties.

Finally, in evaluating the impact of state laws, the analysis should consider whether existing consent processes cover the proposed use of the health information for pharmacovigilance. For example, if a community seeks patient consent to include health information in the HIE, the consent form should be examined to determine whether it will cover pharmacovigilance purposes. If it covers only treatment or exchange between health care providers for treatment purposes, the HIE would need to seek additional consent from the patient (or would need to determine that the pharmacovigilance program did not require consent).

With that framework in mind, the following sections explore examples of how state laws in different categories would impact pharmacovigilance programs. There are many resources available that will assist health systems and HIEs and their lawyers in identifying and understanding applicable state laws. The National Conference of State Legislatures Web Site (http://www.ncsl.org/) contains a summary of state laws**.** The Georgetown Privacy Project Web site (http://www.healthprivacy.org/) contains summaries of health confidentiality laws, although has not updated many states' sites since 2002. Another resource is the reports issued as part of the Health Information Security and Privacy Collaboration, which reviews barriers to HIE reported by 34 states and territories, and posts reports by some states summarizing their state laws that pose barriers to HIE (http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0). Of course, none of these resources substitute for good legal advice, and we recommend consultation with legal counsel familiar with the state statutes, regulations and practices in each state in designing a pharmacovigilance program.

1. Genetic Testing Information

As the medical research community uncovers more information about the genetic basis for disease, many individuals are becoming increasingly concerned about the way in which information about their genetic makeup will be used. Some individuals who have had genetic testing or who have a family history of inherited disease have a fear that, if their insurance companies or employers have access to this information, it will lead to denial of insurance, termination of employment to avoid expected future medical costs, and other discrimination.[69] In an effort to control the dissemination and use of this

[69] *See, e.g.*, Genetic Alliance Web Site at http://www.geneticalliance.org/ws_display.asp?filter=about; Electronic Privacy Information Center Web Site at http://www.epic.org/privacy/genetic/.

sensitive genetic information, many states have enacted rigorous state laws controlling genetic testing and the disclosure of the resulting information.

Example State Law: *Arizona.* In Arizona, the results of a genetic test[70] are confidential and may be released only to individuals for the purposes expressly listed in the statute.[71] Moreover, when a person

---

[70] A.R.S. § 12-2801(1) defines "genetic test" or "genetic testing" as:

"(a) …a test of a person's genes, genetic sequence, gene products or chromosomes for abnormalities or deficiencies, including carrier status, that:

(i) Are linked to physical or mental disorder or impairments.

(ii) Indicate a susceptibility to any illness, disease, impairment or other disorder, whether physical or mental.

(iii) Demonstrate genetic or chromosomal damage due to any environmental factor.

(b) Does not include:

(i) Chemical, blood and urine analyses that are widely accepted and used in clinical practice and that are not used to determine genetic traits.

(ii) Tests used in a criminal investigation or prosecution or as a result of a criminal conviction.

(iii) Tests for the presence of the human immunodeficiency virus.

(iv) Tests to determine paternity conducted pursuant to title 25, chapter 6, article 1.

(v) Tests given for use in biomedical research that is conducted to generate scientific knowledge about genes or to learn about the genetic basis of disease or for developing pharmaceutical and other treatment of disease.")."

[71] A.R.S. §§ 12-2802 provides:

"A. Except as otherwise provided in this article, genetic testing and information derived from genetic testing are confidential and considered privileged to the person tested and shall be released only to:

(1) The person tested;

(2) Any person who is specifically authorized in writing by the person tested or by that person's health care decision maker to receive this information;

(3) The health care decision maker of the person tested;

(4) A researcher for medical research or public health purposes only if the research is conducted pursuant to applicable federal or state laws and regulations governing clinical and biological research or if the identity of the individual providing the sample is not disclosed to the person collecting and conducting the research;

(5) A third person if approved by a human subjects review committee or a human ethics committee, with respect to persons who are subject to an Arizona cancer registry;

(6) An authorized agent or employee of a health care provider if all of the following are true:

(a) The health care provider performs the test or is authorized to obtain the test results by the person tested for the purposes of genetic counseling or treatment;

(b) The agent or employee provides patient care, treatment or counseling;

(c) The agent or employee needs to know the information in order to conduct the test or provide patient care, treatment or counseling;

(7) A health care provider that procures, processes, distributes or uses:

(a) A human body part from a deceased person with respect to medical information regarding that person;

(b) Semen or ova for the purpose of artificial insemination;

(8) A health care provider to conduct utilization review, peer review and quality assurance pursuant to section 36-441, 36-445, 36-2402 or 36-2917;

(9) The authorized agent of a federal, state or county health department to conduct activities specifically authorized pursuant to the laws of this state for the birth defects registry, children's rehabilitative services, newborn screening and sickle cell diagnosis and treatment programs and chronic, environmentally provoked and infectious disease programs;

(10) To obtain legal advice, the legal representative of a health care provider that is in possession of the medical record;

has received genetic testing information from someone else, the recipient also must follow the state statutory rules on disclosing that information.[72] Information and records held by a state agency or a local health authority relating to genetic testing information are confidential and are exempt from public copying and inspection.[73] Finally, health plans are subject to even more restrictive rules on disclosing genetic testing information, and may not release those results to any party without the written, express consent of the subject of the test.[74]

Example of Analysis Applied to State Law: Arizona law poses a barrier to the use of EHRs and HIEs for pharmacovigilance programs if genetic testing information is included in the information evaluated. Applying our decision elements discussed in the introduction to this section, the participants in the program might answer the questions in the following manner:

(1) Does the law apply to the proposed participants in the drug safety surveillance program? Yes. In Arizona, the genetic testing statute applies to any recipient of genetic testing information. Pharmacovigilance program participants therefore might choose to exclude genetic testing information from the information evaluated, if feasible. Whether a certain category of information can be excluded from information evaluated in the pharmacovigilance program will, of course, depend whether the EHR or HIE stores that information separately from other electronic information. If the EHR or HIE receives information from laboratories, the program participants should evaluate whether the laboratories include genetic testing information in the information sent to the EHR or HIE, as it is possible that laboratories will not adequately segregate these test results.

(2) Does the law permit individual information to be utilized in a pharmacovigilance program? Arizona would permit inclusion of genetic testing information in a pharmacovigilance program only if it is structured as a research protocol. Arizona's genetic testing law permits very limited release of genetic testing information for non-treatment related purposes. The only feasible exception that we can apply to a

---

(11) A health care provider that assumes the responsibility to provide care for, or consultation to, the patient from another health care provider that had access to the patient's genetic records.

B. A person shall not disclose or be compelled to disclose the identity of any person on whom a genetic test is performed or the results of a genetic test in a manner that allows identification of the person tested except to the persons specified in the circumstances set forth in subsection A of this section.
C. If genetic testing information is subpoenaed, a health care provider shall respond pursuant to section 12-2294.01, subsection E. In determining whether to order production of the genetic testing information, the court shall take all steps necessary to prevent the disclosure or dissemination of that information.
D. Except as provided in this section, chapter 13, article 7.1 of this title does not apply to genetic testing information that is contained within a patient's medical record.
E. Following the death of a person who had genetic testing performed, the release of the testing information is governed by section 12-2294, subsection D, except that the person may deny, release or limit release of the genetic testing results by adopting a provision in a testamentary document.
F. Except as specifically provided in this article, a person to whom test results have been disclosed pursuant to this article, other than the person tested, shall not disclose the test results to any other person.
G. A health care provider and the provider's agents and employees that act in good faith and that comply with this article are not subject to civil liability. The good faith of a health care provider that complies with this article is presumed. The presumption may be rebutted by a preponderance of the evidence.
H. This article does not limit the effect of title 20 provisions governing the confidentiality and use of genetic testing information."

[72] A.R.S. § 12-2802(F).
[73] A.R.S. § 12-2804.
[74] A.R.S. § 20-448.02.

pharmacovigilance program is to "[a] researcher for medical research or public health purposes … if the research is conducted pursuant to applicable federal or state laws and regulations governing clinical and biological research or if the identity of the individual providing the sample is not disclosed to the person collecting and conducting the research."[75] Therefore, if individually identifiable genetic testing information will be utilized in the pharmacovigilance program, it would need to be structured as a research protocol with IRB approval.

(3) Does the law apply only to external disclosure, or does it apply to internal uses, as well? Arizona's genetic testing statute applies only to the *release* of genetic testing information, not to internal use by the provider that generates the information. One other option in Arizona for structuring a pharmacovigilance program, then, is for a health system to do the analysis internally, and to release only aggregate non-individually identifiable information to other participants in the drug safety surveillance program. This option would not apply to an HIE, because the HIE would not generate the genetic testing information.

(4) Do existing consent processes cover the pharmacovigilance program? In Arizona, a consent for release of genetic testing information must be specific to genetic testing.[76] General consents gathered by a health system or an HIE therefore would not suffice for release of genetic testing information.

2. Mental Health Information

Example State Law: Indiana. Indiana law restricts the disclosure of "mental health records" — recorded or unrecorded information about the diagnosis, treatment or prognosis of a patient receiving mental health services or developmental disability training.[77] Mental health records are confidential and generally may be disclosed only with the patient's consent or for certain listed purposes.[78]

---

[75] A.R.S. §§ 12-2802(A)(4).

[76] A.R.S. § 12-2802(A)(3) (permitting release to "[a]ny person who is specifically authorized in writing by the person tested or by that person's health care decision maker to receive this information.").

[77] Ind. Code Ann. § 16-18-2-226 (defining "mental health record" for purposes of article 39 of title 16 of the Indiana Code). The term does not include alcohol and drug abuse records. *Id*.

[78] Ind. Code Ann. § 16-39-2-3 ("A patient's mental health record is confidential and shall be disclosed only with the consent of the patient unless otherwise provided in the following: (1) This chapter. (2) IC 16-39-3 [release in investigations and legal proceedings]. (3) IC 16-39-4 [release to insurers]. (4) IC 16-39-5-3.").

"Ind. Code. Ann. § 16-39-2-6: Disclosure without patient's consent; interpretation of records; immunities

Sec. 6. (a) Without the consent of the patient, the patient's mental health record may only be disclosed as follows:

(1) To individuals who meet the following conditions:

(A) Are employed by:

(i) the provider at the same facility or agency;

(ii) a managed care provider (as defined in IC 12-7-2-127(b)); or

(iii) a health care provider or mental health care provider, if the mental health records are needed to provide health care or mental health services to the patient.

(B) Are involved in the planning, provision, and monitoring of services.

(2) To the extent necessary to obtain payment for services rendered or other benefits to which the patient may be entitled, as provided in IC 16-39-5-3.

(3) To the patient's court appointed counsel and to the Indiana protection and advocacy services commission.

(4) For research conducted in accordance with IC 16-39-5-3 and the rules of the division of mental health and addiction, the rules of the division of disability and rehabilitative services, or the rules of the provider.

(5) To the division of mental health and addiction for the purpose of data collection, research, and monitoring managed care providers (as defined in IC 12-7-2-127(b)) who are operating under a contract with the division of mental health and addiction.

(6) To the extent necessary to make reports or give testimony required by the statutes pertaining to admissions, transfers, discharges, and guardianship proceedings.

(7) To a law enforcement agency if any of the following conditions are met:

(A) A patient escapes from a facility to which the patient is committed under IC 12-26.

(B) The superintendent of the facility determines that failure to provide the information may result in bodily harm to the patient or another individual.

(C) A patient commits or threatens to commit a crime on facility premises or against facility personnel.

(D) A patient is in the custody of a law enforcement officer or agency for any reason and:

(i) the information to be released is limited to medications currently prescribed for the patient or to the patient's history of adverse medication reactions; and

(ii) the provider determines that the release of the medication information will assist in protecting the health, safety, or welfare of the patient.

Mental health records released under this clause must be maintained in confidence by the law enforcement agency receiving them.

(8) To a coroner or medical examiner, in the performance of the individual's duties.

(9) To a school in which the patient is enrolled if the superintendent of the facility determines that the information will assist the school in meeting educational needs of a person with a disability under 20 U.S.C. 1400 et seq.

(10) To the extent necessary to satisfy reporting requirements under the following statutes:

(A) IC 12-10-3-10.

(B) IC 12-24-17-5.

(C) IC 16-41-2-3.

(D) IC 31-25-3-2.

(E) IC 31-33-5-4.

(F) IC 34-30-16-2.

(G) IC 35-46-1-13.

(11) To the extent necessary to satisfy release of information requirements under the following statutes:

(A) IC 12-24-11-2.

(B) IC 12-24-12-3, IC 12-24-12-4, and IC 12-24-12-6.

(C) IC 12-26-11.

(12) To another health care provider in a health care emergency.

(13) For legitimate business purposes as described in IC 16-39-5-3.

(14) Under a court order under IC 16-39-3.

(15) With respect to records from a mental health or developmental disability facility, to the United States Secret Service if the following conditions are met:

(A) The request does not apply to alcohol or drug abuse records described in 42 U.S.C. 290dd-2 unless authorized by a court order under 42 U.S.C. 290dd-2(b)(2)(c).

(B) The request relates to the United States Secret Service's protective responsibility and investigative authority under 18 U.S.C. 3056, 18 U.S.C. 871, or 18 U.S.C. 879.

(C) The request specifies an individual patient.

(D) The director or superintendent of the facility determines that disclosure of the mental health record may be necessary to protect a person under the protection of the United States Secret Service from serious bodily injury or death.

(E) The United States Secret Service agrees to only use the mental health record information for investigative purposes and not disclose the information publicly.

(F) The mental health record information disclosed to the United States Secret Service includes only:

(i) the patient's name, age, and address;

(ii) the date of the patient's admission to or discharge from the facility; and

(iii) any information that indicates whether or not the patient has a history of violence or presents a danger to the person under protection.

(16) To the statewide waiver ombudsman established under IC 12-11-13, in the performance of the ombudsman's duties.

(b) After information is disclosed under subsection (a)(15) and if the patient is evaluated to be dangerous, the records shall be interpreted in consultation with a licensed mental health professional on the staff of the United States Secret Service.

(c) A person who discloses information under subsection (a)(7) or (a)(15) in good faith is immune from civil and criminal liability."

"Indiana Code Ann. § IC 16-39-5-3: Provider's use of records; confidentiality; violations

Sec. 3. (a) As used in this section, "association" refers to an Indiana hospital trade association founded in 1921.

(b) As used in this section, "data aggregation" means a combination of information obtained from the health records of a provider with information obtained from the health records of one (1) or more other providers to permit data analysis that relates to the health care operations of the providers.

(c) Except as provided in IC 16-39-4-5, the original health record of the patient is the property of the provider and as such may be used by the provider without specific written authorization for legitimate business purposes, including the following:

(1) Submission of claims for payment from third parties.

(2) Collection of accounts.

(3) Litigation defense.

(4) Quality assurance.

(5) Peer review.

(6) Scientific, statistical, and educational purposes.

(d) In use under subsection (c), the provider shall at all times protect the confidentiality of the health record and may disclose the identity of the patient only when disclosure is essential to the provider's business use or to quality assurance and peer review.

(e) A provider may disclose a health record to another provider or to a nonprofit medical research organization to be used in connection with a joint scientific, statistical, or educational project. Each party that receives information from a health record in connection with the joint project shall protect the confidentiality of the health record and may not disclose the patient's identity except as allowed under this article.

(f) A provider may disclose a health record or information obtained from a health record to the association for use in connection with a data aggregation project undertaken by the association. However, the provider may disclose the identity of a patient to the association only when the disclosure is essential to the project. The association may disclose the information it receives from a provider under this subsection to the state department to be used in connection with a public health activity or data aggregation of inpatient and outpatient discharge information submitted under IC 16-21-6-6. The information disclosed by:

(1) a provider to the association; or

(2) the association to the state department;

under this subsection is confidential.

(g) Information contained in final results obtained by the state department for a public health activity that:

(1) is based on information disclosed under subsection (f); and

(2) identifies or could be used to determine the identity of a patient;

is confidential. All other information contained in the final results is not confidential.

(h) Information that is:

(1) advisory or deliberative material of a speculative nature; or

Example of Analysis Applied to State Law: Applying our decision elements discussed in the introduction to this section, the participants in the program might answer the questions in the following manner:

(1) Does the law apply to the proposed participants in the pharmacovigilance program? The Indiana mental health records statute does not expressly describe to whom it applies, and states the prohibition against disclosures in the passive voice (the "patient's mental health record may only be disclosed as follows"). Indiana counsel reports that the prevailing interpretation is that the statute applies only to providers defined in Title 16, because the providers are responsible for safekeeping of the mental health records.[79] This issue would need to be resolved with local counsel.

(2) Does the law permit individual information to be utilized in a drug safety surveillance program? Yes. Indiana law permits release of mental health records for research—as long as it is conducted in accordance with the rules of the state Division of Mental Health—and for scientific purposes. In addition, to the extent the program is treated as "health care operations," providers may release mental health information for "legitimate business purposes" under the statute, which Indiana counsel treat as consistent with HIPAA's definition of health care operations.

(3) *Does the law apply only to external disclosure, or does it apply to internal uses as well?* The Indiana law applies only to external disclosure of mental health records. One option for structuring the pharmacovigilance program is for a health system to do the analysis internally, and to release only aggregated non-individually identifiable information to other participants in the pharmacovigilance program. This option would not apply to an HIE, however, because it would receive the records from treating providers.

---

(2) an expression of opinion;

including preliminary reports produced in connection with a public health activity using information disclosed under subsection (f), is confidential and may only be disclosed by the state department to the association and to the provider who disclosed the information to the association.

(i) The association shall, upon the request of a provider that contracts with the association to perform data aggregation, make available information contained in the final results of data aggregation activities performed by the association in compliance with subsection (f).

(j) A person who recklessly violates or fails to comply with subsections (e) through (h) commits a Class C infraction. Each day a violation continues constitutes a separate offense.

(k) This chapter does not do any of the following:

(1) Repeal, modify, or amend any statute requiring or authorizing the disclosure of information about any person.

(2) Prevent disclosure or confirmation of information about patients involved in incidents that are reported or required to be reported to governmental agencies and not required to be kept confidential by the governmental agencies.

[79] "IC 16-39-2-2 ("Maintenance of records by provider; contents; dominion; time limits. Sec. 2. A record for each patient receiving mental health services shall be maintained by the provider. The mental health record must contain the information that the division of mental health and addiction, the division of disability and rehabilitative services, or the state department requires by rule. The provider is:

(1) the owner of the mental health record;

(2) responsible for the record's safekeeping; and

(3) entitled to retain possession of the record.

The information contained in the mental health record belongs to the patient involved as well as to the provider. The provider shall maintain the original mental health record or a microfilm of the mental health record for at least seven (7) years.

(4) *Do existing consent processes cover the drug safety surveillance program?* If consent is sought to utilize mental health information for the program, the consent for release must describe the information to be released from the mental health record.[80]

3. HIV/AIDS

*Example State Law: Massachusetts***.** Physicians, other health care providers, hospitals, clinics and other facilities (broadly defined) are prohibited from conducting an HIV test, disclosing the test results, or identifying the subject of such a test without the prior written informed consent of the patient.[81]

---

[80]IC 16-39-2-5

Access to patient's designee or legal representative; written request

Sec. 5. (a) This section applies to private and public treating providers.

(b) Upon a patient's written request and reasonable notice, a patient's mental health record shall be made available for inspection and copying by the provider at any time to an individual or organization designated by the patient or to the patient's legal representative.

(c) A patient's written request for the release of the patient's mental health record under this section must include the following:

(1) The name of the patient.

(2) The name of the person requested to release the patient's mental health record.

(3) The name of the person, provider, or organization to whom the patient's mental health record is to be released.

(4) The purpose of the release.

(5) A description of the information to be released from the mental health record.

(6) The signature of the patient.

(7) The date the request is signed.

(8) A statement that the patient's consent to release of mental health records is subject to revocation at any time, except to the extent that action has been taken in reliance on the patient's consent.

(9) The date, event, or condition on which the patient's consent to release of mental health records will expire if not previously revoked.

(d) Unless otherwise specified in a written request under this section, a request for release of records is valid for one hundred eighty (180) days after the date the request is made.

(e) A request for release of records under this section may be revoked by the patient at any time, except to the extent that action has been taken in reliance on the consent.

(f) Mental health records requested by the patient to be released under this section may be released by the provider receiving the request, regardless of whether the patient is still receiving services from the provider.

[81] Mass. Gen. Laws ch. 111, § 70F.

"No health care facility, as defined in section seventy E, and no physician or health care provider shall (1) test any person for the presence of the HTLV-III antibody or antigen without first obtaining his written informed consent; (2) disclose the results of such test to any person other than the subject thereof without first obtaining the subject's written informed consent; or (3) identify the subject of such tests to any person without first obtaining the subject's written informed consent.

No employer shall require HTLV-III antibody or antigen tests as a condition for employment.

Whoever violates the provisions of this section shall be deemed to have violated section two of chapter ninety-three A.

For the purpose of this section "written informed consent" shall mean a written consent form for each requested release of the results of an individual's HTLV-III antibody or antigen test, or for the release of medical records containing such information. Such written consent form shall state the purpose for which the information is being requested and shall be distinguished from written consent for the release of any other medical information, and for the purpose of this section "HTLV-III test" shall mean a licensed screening antibody test for the human T-cell lymphotrophic virus type III."

Example of Analysis Applied to State Law: Applying our decision elements discussed in the introduction to this section, the participants in the program might answer the questions in the following manner:

(1) Does the law apply to the proposed participants in the pharmacovigilance program? Yes, the law applies to health systems, but does not appear to apply to the other participants in a drug safety surveillance program.

(2) Does the law permit this information to be utilized in a pharmacovigilance program? No, providers may not release the results of an HIV test without the consent of the patient. Our understanding is, however, that this statute applies only to the HIV test results themselves, but does not apply to other information in the clinical records that indicates that a patient has HIV/AIDS. This conclusion would of course have to be confirmed with local counsel. One option then, would be to ensure that HIV test results were excluded from information analyzed in the pharmacovigilance program.

(3) Does the law apply only to external disclosure, or does it apply to internal uses, as well? The Massachusetts law does not define what the meaning of "disclosing" is, but it is likely to mean only release to external third parties. If that conclusion is correct, one option for structuring the pharmacovigilance program is for a health system to do the analysis internally, so that any individually identifiable information HIV test results would not be released to other participants in the drug safety surveillance program. Again, this option would not apply to an HIE that receives information from treating providers.

(4) Do existing consent processes cover the drug safety surveillance program? The consent must be separate from a general authorization to release other medical information.[82]

4. General Health Information Laws

A few states have rigorous confidentiality laws that require individual consent for release of health information for most purposes. These laws will pose substantial challenges to the use of health information in EHRs or an HIE for pharmacovigilance programs.

*Example State Law: Minnesota***.** Minnesota law requires consent for the release of health information, except where release is specifically authorized by law, in an emergency when the provider is unable to obtain the patient's consent, to other providers within a related health care entity when necessary for the current treatment of a patient, to a health facility where the patient is returning and unable to consent or where the patient is a resident of the facility, and for research.[83]

---

[82] Mass. Gen. Laws ch. 111, § 70F.

[83] "Minn. 144.293 RELEASE OR DISCLOSURE OF HEALTH RECORDS.

Subdivision 1. Release or disclosure of health records. Health records can be released or disclosed as specified in subdivisions 2 to 9 and sections 144.294 and 144.295.

Subd. 2. Patient consent to release of records. A provider, or a person who receives health records from a provider, may not release a patient's health records to a person without:

(1) a signed and dated consent from the patient or the patient's legally authorized representative authorizing the release;

(2) specific authorization in law; or

(3) a representation from a provider that holds a signed and dated consent from the patient authorizing the release.

Subd. 3. Release from one provider to another. A patient's health record, including, but not limited to, laboratory reports, x-rays, prescriptions, and other technical information used in assessing the patient's condition, or the pertinent portion of the record relating to a specific condition, or a summary of the record, shall promptly be furnished to another provider upon the written request of the patient. The written request shall specify the name of the provider to whom the health record is to be furnished. The provider who furnishes the health record or summary

may retain a copy of the materials furnished. The patient shall be responsible for the reasonable costs of furnishing the information.

Subd. 4. Duration of consent. Except as provided in this section, a consent is valid for one year or for a lesser period specified in the consent or for a different period provided by law.

Subd. 5. Exceptions to consent requirement. This section does not prohibit the release of health records:

(1) for a medical emergency when the provider is unable to obtain the patient's consent due to the patient's condition or the nature of the medical emergency;

(2) to other providers within related health care entities when necessary for the current treatment of the patient; or

(3) to a health care facility licensed by this chapter, chapter 144A, or to the same types of health care facilities licensed by this chapter and chapter 144A that are licensed in another state when a patient:

(i) is returning to the health care facility and unable to provide consent; or

(ii) who resides in the health care facility, has services provided by an outside resource under Code of Federal Regulations, title 42, section 483.75(h), and is unable to provide consent.

Subd. 6. Consent does not expire. Notwithstanding subdivision 4, if a patient explicitly gives informed consent to the release of health records for the purposes and restrictions in clauses (1) and (2), the consent does not expire after one year for:

(1) the release of health records to a provider who is being advised or consulted with in connection with the releasing provider's current treatment of the patient;

(2) the release of health records to an accident and health insurer, health service plan corporation, health maintenance organization, or third-party administrator for purposes of payment of claims, fraud investigation, or quality of care review and studies, provided that:

(i) the use or release of the records complies with sections 72A.49 to 72A.505;

(ii) further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited; and

(iii) the recipient establishes adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient.

Subd. 7. Exception to consent. Subdivision 2 does not apply to the release of health records to the commissioner of health or the Health Data Institute under chapter 62J, provided that the commissioner encrypts the patient identifier upon receipt of the data.

Subd. 8. Record locator service. (a) A provider or group purchaser may release patient identifying information and information about the location of the patient's health records to a record locator service without consent from the patient, unless the patient has elected to be excluded from the service under paragraph (d). The Department of Health may not access the record locator service or receive data from the record locator service. Only a provider may have access to patient identifying information in a record locator service. Except in the case of a medical emergency, a provider participating in a health information exchange using a record locator service does not have access to patient identifying information and information about the location of the patient's health records unless the patient specifically consents to the access. A consent does not expire but may be revoked by the patient at any time by providing written notice of the revocation to the provider.

(b) A health information exchange maintaining a record locator service must maintain an audit log of providers accessing information in a record locator service that at least contains information on:

(1) the identity of the provider accessing the information;

(2) the identity of the patient whose information was accessed by the provider; and

(3) the date the information was accessed.

(c) No group purchaser may in any way require a provider to participate in a record locator service as a condition of payment or participation.

(d) A provider or an entity operating a record locator service must provide a mechanism under which patients may exclude their identifying information and information about the location of their health records from a record locator service. At a minimum, a consent form that permits a provider to access a record locator service must include a conspicuous check-box option that allows a patient to exclude all of the patient's information from the record locator service. A provider participating in a health information exchange with a record locator service who receives a patient's request to exclude all of the patient's information from the record locator service or to have a specific provider contact excluded from the record locator service is responsible for removing that information from the record locator service.

Subd. 9. Documentation of release. (a) In cases where a provider releases health records without patient consent as authorized by law, the release must be documented in the patient's health record. In the case of a release under section 144.294, subdivision 2, the documentation must include the date and circumstances under which the release was made, the person or agency to whom the release was made, and the records that were released.

(b) When a health record is released using a representation from a provider that holds a consent from the patient, the releasing provider shall document:

(1) the provider requesting the health records;

(2) the identity of the patient;

(3) the health records requested; and

(4) the date the health records were requested.

Subd. 10. Warranties regarding consents, requests, and disclosures. (a) When requesting health records using consent, a person warrants that the consent:

(1) contains no information known to the person to be false; and

(2) accurately states the patient's desire to have health records disclosed or that there is specific authorization in law.

(b) When requesting health records using consent, or a representation of holding a consent, a provider warrants that the request:

(1) contains no information known to the provider to be false;

(2) accurately states the patient's desire to have health records disclosed or that there is specific authorization in law; and

(3) does not exceed any limits imposed by the patient in the consent.

(c) When disclosing health records, a person releasing health records warrants that the person:

(1) has complied with the requirements of this section regarding disclosure of health records;

(2) knows of no information related to the request that is false; and

(3) has complied with the limits set by the patient in the consent.

144.294 RECORDS RELATING TO MENTAL HEALTH.

***

144.295 DISCLOSURE OF HEALTH RECORDS FOR EXTERNAL RESEARCH.

Subdivision 1. Methods of release. (a) Notwithstanding section 144.293, subdivisions 2 and 4, health records may be released to an external researcher solely for purposes of medical or scientific research only as follows:

(1) health records generated before January 1, 1997, may be released if the patient has not objected or does not elect to object after that date;

(2) for health records generated on or after January 1, 1997, the provider must:

(i) disclose in writing to patients currently being treated by the provider that health records, regardless of when generated, may be released and that the patient may object, in which case the records will not be released; and

(ii) use reasonable efforts to obtain the patient's written general authorization that describes the release of records in item (i), which does not expire but may be revoked or limited in writing at any time by the patient or the patient's authorized representative;

(3) the provider must advise the patient of the rights specified in clause (4); and

Example of Analysis Applied to State Law: Applying our decision elements discussed in the introduction to this section, the participants in the program might answer the questions in the following manner:

(1) Does the law apply to the proposed participants in the pharmacovigilance program? Yes, because Minnesota law applies to a "provider, or a person who receives health records from a provider."[84]

(2) Does the law permit individual information to be utilized in a pharmacovigilance program? Minnesota law would permit health information to be used in a pharmacovigilance program if it is structured as a research protocol, and by following the fairly strict limitations of the Minnesota law.[85]

(3) Does the law apply only to external disclosure, or does it apply to internal uses, as well? The Minnesota law applies only to external releases. One option for structuring the pharmacovigilance program is for a health system to do the analysis internally, so that any individually identifiable information would not be released to other participants in the pharmacovigilance program. This option would not apply to the HIE, which would be receiving information from treating providers.

(4) *Do existing consent processes cover the pharmacovigilance program?* Minnesota law does not appear to have specific requirements for consent; this conclusion would of course need to be confirmed with local counsel. Moreover, any consent form used would need to be drafted carefully to incorporate patient permission to utilize information for a pharmacovigilance program.

III. Research Compliance Issues

As explored in the privacy compliance sections, if a pharmacovigilance program is structured as a research protocol, it will meet the terms of most of the federal and state confidentiality laws discussed above. Of course, conducting research with human subjects may require compliance with federal (and sometimes state) requirements relating to the protection of human subjects involved in research. This section will address the federal requirements related to research.

---

(4) the provider must, at the request of the patient, provide information on how the patient may contact an external researcher to whom the health record was released and the date it was released.

(b) Authorization may be established if an authorization is mailed at least two times to the patient's last known address with a postage prepaid return envelope and a conspicuous notice that the patient's medical records may be released if the patient does not object, and at least 60 days have expired since the second notice was sent.

Subd. 2. Duties of researcher. In making a release for research purposes, the provider shall make a reasonable effort to determine that:

(1) the use or disclosure does not violate any limitations under which the record was collected;

(2) the use or disclosure in individually identifiable form is necessary to accomplish the research or statistical purpose for which the use or disclosure is to be made;

(3) the recipient has established and maintains adequate safeguards to protect the records from unauthorized disclosure, including a procedure for removal or destruction of information that identifies the patient; and

(4) further use or release of the records in individually identifiable form to a person other than the patient without the patient's consent is prohibited.

[84] Minn. Stat. 144.293.

[85] Minn. Stat. 144.295.

A. Definition of "Research"

While structuring a pharmacovigilance program as a research protocol is a path through the morass of most federal and state privacy laws, the program designers would need to confirm that the program indeed meets the definition of "research." Research is defined as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge"[86] As discussed in the HIPAA section (see section II(A)(3)(b)(1)), the distinction between public health surveillance activities and "research" is sometimes a thin one.

B. Review by an Institutional Review Board

Research involving human subjects regulated by federal law often requires review by an Institutional Review Board (IRB)—a group of at least five people that review and approve the conduct of research. The first inquiry then, is whether federal law applies to the research protocol. The Federal Policy for the Protection of Human Subjects (also known as the "Common Rule") applies to research involving obtaining identifiable private information, if that research (a) is not otherwise exempt, and (b) is conducted or supported by a federal department or agency that has adopted the Common Rule or where the institution engage in the research has agreed to apply the federal regulations under the institution's Federalwide Assurance (FWA) to all non-exempt human subjects research regardless of the funding source.[87] The extension of the HHS regulations to non-federally conducted or supported research is voluntary, so the institution's FWA should be examined. The FDA regulations apply to all clinical investigations regulated by the FDA or that support marketing applications for FDA approval.[88] While some research is not covered by either the Common Rule or FDA regulations, many institutions have internal policies requiring IRB review of all research conducted at the institution.

1. "Human Subject Research"

Both the HHS and FDA regulations require review by an IRB in most circumstances, of research involving "human subjects." [89] Human subjects are defined by HHS as "living individual(s) about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information."[90] If the pharmacovigilance project accesses identifiable personal information, the program constitutes human subject research.

---

[86] 45 C.F.R. § 46.102(d).
[87] 45 C.F.R. § 46.101; § 46.103. OHRP has issued a "Human Subjects Regulations Decision Chart" at http://www.hhs.gov/ohrp/humansubjects/guidance/decisioncharts.htm that is helpful in understanding the analysis of what activities are subject to IRB review.
[88] 21 C.F.R. § 50.1.
[89] 45 C.F.R. § 46.101; 21 C.F.R. § 20 56.101.
[90] 45 C.F.R. § 46.102(f)(1). The FDA regulations define "human subject" as "an individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may either be a healthy individual or a patient." 21 C.F.R. § 20 56.101.

2. Research Exempt from IRB Review

In some circumstances, human subject research is exempt from the requirements of federal human subject protection regulations, including requirements related to IRB review. Under the Common Rule, research is exempt if it involves the "collection or study of existing data, documents, or pathological or diagnostic specimens, if publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers."[91] The use of EHRs and HIEs to conduct pharmacovigilance programs would involve the study of existing data generated through clinical care. Whether the research would be exempt thus depends on the manner in which the information for the research is recorded. If the investigators record their findings in a manner that permits the investigators or others to trace those findings back to individual patients, either because the information recorded contains identifiers or has links, then the research would not be exempt. (The FDA regulations' requirements, if applicable, have considerably stricter requirements for exemption.)[92]

Moreover, even where research is exempt, an organization's policies may require review of research.[93] So, it is unlikely that a pharmacovigilance research protocol will not be subject to IRB review.

3. Research Subject to Expedited Review

Even if the research protocol requires IRB review, it is possible that the protocol will be subject to expedited review by the IRB Chair or an experienced IRB member designated by the IRB Chair, rather than subject to a full board review. Both the HHS and FDA regulations allow expedited review where:

- The research involves no more than minimal risk to the subjects;
- The research does not place subjects at risk of criminal or civil liability or damage to the subjects' financial standing, employability, insurability, reputation, or be stigmatizing, unless reasonable

---

[91] 45 C.F.R. § 46.101(b). The HHS regulations also exempt research from IRB review where it:

(1) Is conducted in established or commonly accepted educational settings, involving normal education practices;
(2) Involves educational tests, survey procedures, interview procedures, or observation of public behavior (unless identifying information will be recorded that can link subjects to the data, and disclosure of that data could place subjects at risk of civil or criminal liability or be damaging to the subjects' financial standing, employability or reputation). Note that this exemption for surveys, interviews, and observation of public behavior does not apply to children unless the investigator observes public behavior and does not participate in the activities being observed;
(4) Involves studying, evaluating, or examining public benefit or service programs; and
(5) Involves taste and food quality evaluation or consumer acceptance studies.

Id.

[92] 21 C.F.R. § 56.104. The FDA regulations exempt research from IRB review where:

(1) The research was begun before July 27, 1981;
(2) The research involves emergency use of a test article, and the emergency use is reported to the IRB within 5 working days (and any subsequent use of the test article is subject to IRB review); or
(3) The research involves taste and food quality evaluations.

[93] *See* Office for Human Research Protections, IRB Guidebook at p. 15 ("While the regulations further specify that this requirement "need not be applicable to any research exempted...under §___.101(b)," many institutions' human subjects policies provide that all research, even research that is exempt from review under the federal regulations, is to be reviewed by the IRB. In such cases, the IRB has jurisdiction over all human subjects research, thereby providing broader protection for subjects than that required by the regulations. It is crucial that IRBs keep in mind that their authority to approve, require modifications in, or disapprove research derives from both federal law and institutional policy."), at http://www.hhs.gov/ohrp/irb/irb_guidebook.htm.

and appropriate protections will be implemented so that risks related to invasion of privacy and breach of confidentiality are no greater than minimal; and

- The research falls within the categories for expedited review, including research involving data, documents, records, or specimens that have been collected, or will be collected solely for nonresearch purposes (such as medical treatment or diagnosis).[94]

Depending on the policies of the institution and the confidentiality protections in place for the pharmacovigilance program, an IRB may agree to provide expedited review.

4. Criteria for IRB Approval

To approve research, federal regulations require an IRB to determine that a number of criteria are met:[95]

(1) Risks to subjects are minimized by using procedures (i) that are consistent with sound research design, (ii) that do not unnecessarily expose subjects to risk, and (iii) whenever appropriate, that already are being performed on the subjects for diagnostic or treatment purposes.

(2) Risks to subjects are reasonable in relation to anticipated benefits to subjects, if any, and the importance of the knowledge that may reasonably be expected to result.

---

[94] *See* 45 C.F.R. § 46.110 and 21 C.F.R. § 56.110 (1). Categories of research in which expedited review is permitted include:
(1) Clinical studies of drugs and medical devices where:
(a) Research on drugs for which an investigational new drug application is not required; or
(b) Research on medical devices for which (i) an investigational device exemption application is not required; or (ii) the medical device is cleared or approved for marketing and the medical device is being used in accordance with its cleared or approved labeling.
(2) Collection of blood samples by finger stick, heel stick, ear stick, or venipuncture as follows:
(a) From healthy, nonpregnant adults who weigh at least 110 pounds. For these subjects, the amounts drawn may not exceed 550 ml in an 8 week period and collection may not occur more frequently than 2 times per week; or
(b) From other adults and children, considering the age, weight, and health of the subjects, the collection procedure, the amount of blood to be collected, and the frequency with which it will be collected. For these subjects, the amount drawn may not exceed the lesser of 50 ml or 3 ml per kg in an 8 week period and collection may not occur more frequently than 2 times per week.
(3) Prospective collection of biological specimens for research purposes by noninvasive means (such as hair and nail clippings, excrement, sweat, uncannulated saliva, placenta and amniotic fluid at delivery, dental plaque and calculus, mucosal and skin cells, and sputum).
(4) Collection of data through noninvasive procedures routinely employed in clinical practice, excluding general anesthesia, sedation, x-rays or microwaves (such as physical sensors, weighing, testing sensory acuity, MRI, electrocardiography, electroencephalography, thermography, detection of naturally occurring radioactivity, electroretinography, ultrasound, diagnostic infrared imaging, doppler blood flow, echocardiography, moderate exercise, muscular strength testing, body composition assessment, and flexibility testing where appropriate given the age, weight, and health of the individual).
(5) Research involving data, documents, records, or specimens that have been collected, or will be collected solely for nonresearch purposes (such as medical treatment or diagnosis).
(6) Collection of data from voice, video, digital, or image recordings made for research purposes.
(7) Research on individual or group characteristics or behavior or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

[95] *See* 45 C.F.R. § 46.111; 21 C.F.R. § 56.111.

(3) Selection of subjects is equitable. In making this assessment the IRB should take into account the purposes of the research and the setting in which the research will be conducted and should be particularly cognizant of the special problems of research involving vulnerable populations, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons.

(4) Informed consent will be sought from each prospective subject or the subject's legally authorized representative, and documented (unless waived by the IRB).

(5) When appropriate, the research plan makes adequate provision for monitoring the data collected to ensure the safety of subjects.

(6) When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

(7) When some or all of the subjects are likely to be vulnerable to coercion or undue influence, such as children, prisoners, pregnant women, mentally disabled persons, or economically or educationally disadvantaged persons, additional safeguards have been included in the study to protect the rights and welfare of these subjects.

In a protocol involving access to electronic health records, where the research does not involve any individual therapeutic intervention, we anticipate the issue of greatest interest to the IRB will be how the researchers will maintain the privacy and confidentiality of the information utilized in the project. Reducing the risks to individual privacy is discussed in the next section.

5. Waiver of Informed Consent

Federal regulations generally require informed consent for an individual to participate in research (or for an individual's identifiable information to be used in research).[96] However, because a pharmacovigilance research protocol would seek to evaluate all records held by a health system or HIE, a huge number of patient records would be utilized. It would be exceedingly difficult and expensive to contact all patients whose records are housed in a system's EHR or an HIE—many patients would not be at the address of record and efforts to contact them would require substantial personnel time and expense. So, investigators likely would ask an IRB to waive informed consent.

To waive informed consent, HHS regulations require an IRB to make the determination that all of the following requirements are met:[97]

(1) The research involves no more than minimal risk to the subjects. "Minimal risk" is defined as "the probability and magnitude of harm or discomfort anticipated in the research is not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests."[98]

(2) The waiver or alteration will not adversely affect the rights and welfare of the subjects.

(3) The research could not practicably be carried out without the waiver or alteration.

---

[96] See 45 C.F.R. § 46.116-.117; 21 C.F.R. §§ 50.20-.27 and § 56.109.
[97] See 45 C.F.R. § 46.117(c)-(d) (general waiver). The FDA regulations permit waiver of informed consent only in emergency research, 21 C.F.R. § 50.24, although the FDA recently issued guidance that it would not enforce the informed consent requirement for use of non-individually identifiable tissue for *in vitro* diagnostic studies, in certain circumstances. *See* 71 Fed. Reg. at 23924 (April 25, 2006).
[98] 45 C.F.R. § 46.102(i); 21 C.F.R. § 50.3(k) (same).

(4) Whenever appropriate, the subjects will be provided with additional pertinent information after participation.

These elements are very similar to the IRB waiver of a HIPAA authorization. With appropriate confidentiality protections in place, many IRBs would approve waiver of informed consent, as well as waiver of HIPAA authorization, for a pharmacovigilance program. Because these programs seek to evaluate all records held by a health system or HIE, the program is potentially examining huge numbers of patient records. Indeed, the more patient records that are evaluated, the greater number of safety events will be determined and the more rigorous the conclusions will be regarding causation, if that is the intent of the program. As discussed previously, it would be exceedingly difficult and expensive to contact all patients whose records are housed in a system's EHR or an HIE. We believe that an IRB could conclude, then, that the research could not practicably be conducted without a waiver of informed consent.

Next, the researchers will need to demonstrate to the IRB that the research involves no more than minimal risk to the subjects and that waiver of informed consent will not adversely affect the rights and welfare of the subjects. In a research project involving analysis of health information where there is no experimental intervention with the individual, this analysis will depend on whether the patient information is adequately protected against improper use and disclosure. For example, an IRB may require the researchers to keep all PHI on site for the research project to reduce the security risks in electronic transmission of the information. If electronic transmission or remote access to an EHR will be utilized, the researchers should demonstrate adequate encryption or other secure transmission method. The IRB may also require the researchers to demonstrate that only the data needed for the protocol are accessed, such as by screening out all direct identifiers like name, address and social security number.

Under HIPAA, the IRB also may require the researchers to destroy information identifying the subjects at the earliest opportunity consistent with conduct of the research (unless there is a health or research justification for retention or if retention is required by law). The IRB also will require written assurances from the researchers that that the individually identifiable information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the study, or for other research permitted by the rules. These HIPAA restrictions will assist in demonstrating that the risks to participants have been minimized.

Finally, the regulations require the IRB to consider whether the subjects will be provided with additional pertinent information after participation. The investigators should think carefully about type of information would be provided to participants, or the entity's patients in general, and the timing of that information.

C. Whose IRB May Conduct the Review?

IRB review traditionally has been done locally by the institution conducting the research. A health system participating in a pharmacovigilance program, for example, likely will have its own IRB or contract with another IRB to provide research review services.

However, if multiple institutions (health systems, hospitals, HIEs, and other providers) will be participating in a pharmacovigilance program, it is also possible for those multiple institutions to designate one IRB as the reviewing IRB for the program. Both OHRP and FDA regulations permit reliance on an outside IRB,[99] and the FDA actively encourages the use of one IRB for multiple institutions

[99] *See* 45 CFR 46.114 ("With the approval of the department or agency head, an institution participating in a cooperative project may enter into a joint review arrangement, rely upon the review of another qualified IRB, or make similar arrangements for avoiding duplication of effort."); 21 CFR 56.114

conducting the same protocol to minimize cost and variation across IRBs.[100] Those participating institutions that have a FWA simply must designate the reviewing IRB on its FWA (along with any other IRBs the institution uses) and ensure that the IRB is registered with HHS.[101]

The Association of American Medical Colleges (AAMC) held a conference in November 2006, co-sponsored by the National Institutes of Health, the Office for Human Research Protections, the Veteran's Administration and the American Society of Clinical Oncology, to explore alternative IRB models. The conference planners issued a thorough report discussing the advantages and disadvantages of utilizing another institution's IRB and the contractual provisions institutions using another IRB should consider.[102] We do not discuss these issues further here, but refer readers to this excellent AAMC report.

In the context of a pharmacovigilance protocol, the use of a single IRB makes enormous sense to reduce the variability of IRB requirements across institutions. If different IRBs impose different requirements (such as what individually identifiable data may be accessed by the researchers and other confidentiality and security protections for the data), it may be difficult for the same pharmacovigilance protocol to be conducted across multiple institutions, which may reduce the viability of pharmacovigilance projects across the country.

IV. FDA Reporting Obligations[103]

The utilization of electronic health records for pharmacovigilance raises questions regarding the reporting responsibilities of the parties involved in that effort. For example, at what point will there be an obligation imposed on a participant in the pharmacovigilance effort to report any adverse drug effects discovered during the course of the project? To whom must such a report be made? These questions must be analyzed from the perspective of the pharmaceutical company participants in a pharmacovigilance effort and the holders of the electronic health information used (health systems that maintain EHRs for patients under their care and HIEs that have no direct relationship with patients). The following discussion addresses potential reporting requirements by each of these categories under the Food and Drug Administration (FDA) regulations.

A. Drug Manufacturer Obligations

The FDA requires mandatory reporting by drug manufacturers[104] in a variety of circumstances. Because results generated in a pharmacovigilance project do not fall squarely within the existing FDA reporting categories, we describe various reporting requirements and recommend how reporting is likely to apply

---

("institutions involved in multi-institutional studies may use joint review, reliance upon the review of another qualified IRB, or similar arrangements aimed at avoidance of duplication of effort.").

[100] *See* FDA Guidance: "Using a Centralized IRB Review Process in Multicenter Clinical Trials" (March 2006), at http://www.fda.gov/cder/guidance/OC2005201fnl.htm or http://www.fda.gov/cder/guidance/OC2005201fnl.pdf.

[101] *See* http://www.hhs.gov/ohrp/assurances/.

[102] *See* http://www.hhs.gov/ohrp/ (under Special Issues).

[103] Some states may have reporting requirements to other regulatory boards, however, it is beyond the scope of this report to indicate or address any such state requirements. Further, this report does not address reporting obligations in other countries or the European Union, which may be substantially different from those required by the FDA in the United States.

[104] Under the FDA proposed regulations, "manufacturer" describes persons subject to regulations relating to prescription drugs without an approved new drug application (NDA). 68 Fed. Reg. No. 50, II.A.3. The term "applicant" is used to describe persons subject to regulations relating to drugs with an approved NDA. *Id*. For ease of reference, we use the term "manufacturer" to describe persons subject to post-marketing safety reporting regulations without distinction as to whether there is an NDA.

in the context of pharmacovigilance projects undertaken in the electronic health information environment.

Manufacturers of new drugs must review and report to the FDA most adverse drug experiences about which they learn.[105] Regulatory reporting is divided into two categories: expedited safety reporting (also called 15-day Alert Reporting) and periodic safety reporting.[106] In order to determine whether an adverse drug experience must be reported in an expedited safety report or a periodic safety report, a manufacturer must consider three factors: (1) the source of the information; (2) whether the adverse drug reaction is deemed to be "serious" and "unexpected"; and (3) whether there is a potential causal relationship between a particular drug and the adverse event. In the following sections, we provide a brief overview of these factors and how they trigger different reporting requirements, and provide an analysis of which regulations will likely extend to manufacturers participating in a pharmacovigilance effort.

1. Expedited Safety Reporting (15-Day Alert Reporting)

The purpose of expedited reporting is to make regulators, investigators, and other appropriate parties aware of information about serious adverse drug reactions. When a manufacturer receives information about an adverse drug experience through a "solicited source," the manufacturer must make an expedited report if the adverse event is both "serious" and "unexpected" and the manufacturer determines that there is a potential causal relationship between the drug and the adverse event. However, when the information is received through a "spontaneous source," the manufacturer must make an expedited report if it determines that the adverse drug experience is serious and unexpected; in this circumstance, the potential causal relationship between the drug and the adverse event is assumed. It is critical, therefore, that the manufacturer identify whether the source of the information is a spontaneous source or a solicited source.

The FDA regulations do not define what constitutes a "spontaneous source" or a "solicited source."[107] However, both the FDA's proposed regulations and the International Conference on Harmonization (ICH) Guidelines provide thorough and consistent definitions for each, which we apply in this analysis. In 2003, the FDA published proposed regulations governing safety reporting requirements for human drug and biological products (called "The Tome" in the industry).[108] The proposed regulations added substantial detail and clarification to the existing regulations, but were never adopted. Where the current regulations are vague, we apply the proposed regulations and the ICH Guidelines (which closely resemble one another), as long as the proposed regulations and ICH Guidelines are not inconsistent with the current FDA regulations.

a. Spontaneous Source

The FDA regulations do not define "spontaneous source." However, the proposed regulations define a spontaneous source as:

> A communication from an individual (e.g. health care professional, consumer) to a company or regulatory authority that describes an SADR or medication error. It does not include cases identified from information solicited by the manufacturer or contractor [], such as individual case safety reports or findings derived from a study,

---

[105] *See* 21 C.F.R. § 310, 312, 600, *et seq*.
[106] 21 C.F.R. §§ 310.305, 314.80, and 600.80.
[107] In fact, despite industry practice, the FDA regulations do not use the term "solicited source," but rather "study."
[108] 68 Fed. Reg. No. 50 (August 1, 2002).

> company-sponsored patient support program, disease management program, patient registry, including pregnancy registries, or any organized data collection scheme. It also does not include information compiled in support of class action lawsuits.[109]

The ICH Guidelines similarly define a "spontaneous report" as an "unsolicited communication by healthcare professionals or consumers to a company, regulatory authority or other organization (e.g. WHO, Regional Centers, Poison Control Center) … and that does not derive from a study or any organized data collection scheme."[110]

If the manufacturer receives information about an adverse drug experience, it must determine whether it is serious and unexpected. The FDA regulations define a "serious adverse drug experience" as:

> Any adverse drug experience occurring at any dose that results in any of the following outcomes: Death, a life-threatening adverse drug experience, inpatient hospitalization or prolongation of existing hospitalization, a persistent or significant disability/incapacity, or a congenital anomaly/birth defect. Important medical events that may not result in death, be life-threatening, or require hospitalization may be considered a serious adverse drug experience when, based upon appropriate medical judgment, they may jeopardize the patient or subject and may require medical or surgical intervention to prevent one of the outcomes listed in this definition.[111]

The FDA regulations define an "unexpected adverse drug experience" as:

> Any adverse drug experience that is not listed in the current labeling for the drug product. This includes events that may be symptomatically and pathophysiologically related to an event listed in the labeling, but differ from the event because of greater severity or specificity. "Unexpected," as used in this definition, refers to an adverse drug experience that has not been previously observed (i.e., included in the labeling) rather than from the perspective of such experience not being anticipated from the pharmacological properties of the pharmaceutical product.[112]

If the manufacturer is unable to determine whether the adverse drug experience is serious and unexpected based on the information from the spontaneous report, the proposed regulations would require the manufacturer to engage in an "active query" to obtain further information.[113] Ultimately, once the manufacturer has obtained sufficient information, if it determines that the experience is both serious and unexpected it must file an expedited report in accordance with the FDA regulations.

b. Solicited Source

The FDA regulations do not define "solicited source." However, the proposed regulations provide:

> Cases identified from information solicited by companies, such as individual case safety reports or findings obtained from a study,

---

[109] 68 Fed. Reg. No. 50, III.A.7.
[110] ICH E2D ver. 3.8, 2.5.1.1.
[111] 21 C.F.R. §§ 310.305(b), 314.80(a), 600.80(a).
[112] *Id*.
[113] 68 Fed. Reg. No. 50, III.C.5.

> company-sponsored patient support program, disease management program, patient registry, including pregnancy registries, or any organized data collection scheme would not be considered spontaneous. Instead safety information from these sources would be considered "study" information and would be handled according to the post-marketing safety requirements for a "study."[114]

The ICH Guidelines similarly provide:

> Solicited reports are those derived from organized data collection systems, which include clinical trials, post-approval named patient use programs, other patient support and disease management programs, surveys of patients or healthcare providers, or information gathering on efficacy or patient compliance. Adverse event reports obtained from any of these should not be considered spontaneous. For the purposes of safety reporting, solicited reports should be handled as if they were study reports, and therefore should have an appropriate causality assessment.[115]

Where information is obtained from a solicited source, the FDA regulations do not require reporting by the manufacturer for serious and unexpected adverse drug experiences, "unless the [manufacturer] concludes that there is a reasonable possibility that the product caused the adverse experience."[116] As such, the manufacturer need only make an expedited report for adverse drug experiences that are serious, unexpected and determined to have a potential causal relationship to the drug.

c. Timing of Report

A manufacturer must make an expedited report to the FDA as soon as possible, but in no case later than fifteen calendar days after its initial receipt of information.[117] If a manufacturer makes an expedited report to the FDA, it must then submit a follow-up report for every adverse drug experience reported within fifteen calendar days of receipt of new information or as requested by the FDA.[118] It also must determine its obligations to make periodic safety reporting, as discussed later in this section.

d. Proposal for Expedited Reporting of All Adverse Drug Experiences

In the proposed regulations, the FDA proposed to require manufacturers to submit an expedited report for *every* suspected adverse drug reaction received or otherwise obtained, whether foreign or domestic, that is included in a specific list of medically significant drug reactions (called the "Always Expedited Report").[119] If this provision of the FDA's proposed regulations were finalized, it would require a manufacturer to make an expedited report of the specifically listed adverse events regardless of whether the information is received from a solicited source or a spontaneous report, whether the adverse drug experience was serious and unexpected, and whether the manufacturer determined a potentially causal relationship between the adverse event and the drug. Specifically, the proposed rules would require the following list of events to be reported to the FDA in every circumstance: congenital anomalies, acute respiratory failure, ventricular fibrillation, torsades de pointe, malignant hypertension, seizure, agranulocytosis, aplastic anemia, toxic epidermal necrolysis, liver necrosis, acute liver failure,

---

[114] 68 Fed. Reg. No. 50, III.A.7.
[115] ICH E2D ver. 3.8, 2.5.2.
[116] 21 C.F.R. §§ 314.80(e), 600.80(e).
[117] 21 C.F.R. §§ 310.305(c)(1)(i), 314.80(c)(1)(i), 600.80(c)(1)(i).
[118] 21 C.F.R. §§ 310.305(c)(2), 314.80(c)(1)(ii), 600.80(c)(1)(ii).
[119] 68 Fed. Reg. No. 50, III.D.4.

anaphylaxis, acute renal failure, sclerosing syndromes, pulmonary hypertension, and pulmonary fibrosis.[120] The FDA would also retain the right to add additional events to this list if it determines an event to be medically significant.

The industry does not believe this proposed rule will be finalized. There is no such corollary to this proposed rule in the ICH Guidelines. Moreover, the rule would substantially limit the value of company analyses and medical interpretation in determining the seriousness of an adverse drug experience and would not take into consideration the indication for use or the information contained in the product labeling. Finally, such a stringent reporting requirement would place an undue burden on both the FDA and manufacturers.

2. Periodic Safety Reporting Requirements

The FDA requires submission of post-marketing periodic safety reports to review and monitor adverse drug reactions on an ongoing basis.[121] Periodic adverse drug experience reports must be submitted at quarterly intervals, for three years from the date of approval of an application or the date of issuance of a license, and then at annual intervals.[122]

As a general matter, a periodic report is required to summarize and analyze every expedited report made during the reporting interval.[123] A manufacturer also is required to include every adverse drug experience received through a spontaneous report that was not included in expedited report.[124] In contrast, a manufacturer is not required to include adverse drug experiences received through solicited sources that were not included in an expedited reporting.[125] In other words, if the manufacturer receives information from a solicited source and does not make an expedited report either because it determines that the adverse drug experience is not serious and unexpected or that it does not have a causal relationship with the drug, then the manufacturer need not submit a periodic report discussing that adverse drug experience.

3. Application to a Pharmacovigilance Project

Because the purpose of a pharmacovigilance project is to determine whether approved drugs are safe—essentially to create an "early-warning" system for drug safety that does not rely on voluntary reporting by health care providers—a health system and HIE participating in the project will undoubtedly learn about adverse drug experiences and report those to the drug manufacturers. The critical inquiry is whether a health system or HIE would be treated as a solicited source or a spontaneous source for purposes of determining manufacturers' reporting obligations.

Where a health system or HIE partners with drug manufacturers in a pharmacovigilance program, we believe information generated by the health system or HIE will be treated as a solicited source. While pharmacovigilance programs are not expressly addressed in the proposed rules' list of solicited sources (which includes "findings obtained from a study, company-sponsored patient support program, disease management program, patient registry, including pregnancy registries, or any organized data collection scheme"), it is likely that a pharmacovigilance program would be considered an organized data collection system and thus treated as a solicited source (especially if the pharmacovigilance program is structured as a research protocol). Moreover, because the information would not be coming from an individual

---

[120] *Id*.
[121] 21 C.F.R. §§ 314.80(2)(i), 600.80(2)(i).
[122] 21 C.F.R. §§ 314.80(2)(ii), 600.80(2)(ii).
[123] *Id*.
[124] *Id*.
[125] 21 C.F.R. §§ 314.80(c)(2)(iii), 600.80(c)(2)(iii).

health care professional or consumer, it would not fall within the FDA's explanation of a spontaneous source.

A drug manufacturer, therefore, when learning of information about an adverse drug experience generated by the pharmacovigilance program, will be responsible for complying with the FDA regulations for reporting from a solicited source. That is, the manufacturer must determine if the adverse drug experience is both serious and unexpected and causally related to a drug. If these factors are present, then the manufacturer must make an expedited report to the FDA and later follow-up with a fifteen-day report, and then a periodic report. If, however, the manufacturer does not find all the factors present, it need not make an expedited or periodic report to the FDA.

B. Health System and HIE Obligations

1. Voluntary Reporting to MedWatch

The holders of electronic health information—HIEs and health systems—do not have mandatory reporting obligations under FDA regulations. Rather, reporting is purely voluntary. The FDA does not have the authority to regulate the practice of medicine or control the prescribing of drugs; its authority is limited to enforcing drug safety by regulating the manufacture, sale, distribution, and marketing of drugs. [126]

In 1993 the FDA launched a multiple adverse event reporting system (AERS) called MedWatch, designed for voluntary reporting to the FDA of problems with medical products.[127] Through its MedWatch program, the FDA receives adverse drug event reports from consumers and health professionals. However, the FDA does not mandate or regulate reporting to its MedWatch program by health professionals. When a report is received through the FDA's MedWatch program, it is the responsibility of the manufacturer to analyze the information and determine what reporting is triggered for the manufacturer.

2. Proposal for Expedited Reporting by Contractors

The current FDA regulations only require expedited reporting by "any person whose name appears on the label of a marketed prescription drug product as its manufacturer, packer, distributor, shared manufacturer, joint manufacturer, or any other participant involved in divided manufacturing."[128] The proposed rules, however, would expand reporting requirements to "contractors."[129] A "[c]ontractor means any person (e.g., manufacturer, joint manufacturer, packer, or distributor whether or not its name appears on the label of the product; licensee; contract research organization) that has entered into a contract with the manufacturer to manufacture, pack, sell, distribute, or develop the drug or to maintain, *create or submit records regarding SADRs or medication errors*."[130] It is possible that a health system or HIE that contracts with a manufacturer to use electronic health information for a pharmacovigilance project may be creating records regarding adverse drug experience, making a health system or HIE a contractor under the proposed rules.

---

[126] *See* 21 C.F.R. §§ 310.305, 314.80, 314.98, and 600.80 (providing that the following persons are subject to postmarketing safety reporting regulations: manufacturers and applicants, packers and distributors, joint manufacturers, shared manufacturers, any participant involved in divided manufacturing, and blood establishments); *see also* 68 Fed. Reg. No. 50, II.A.2.

[127] *See* MedWatch website: http://www.fda.gov/medwatch/how.htm (distinguishing between mandatory reporting and voluntary reporting).

[128] 21 C.F.R. §§ 310.305(c)(1)(i), 314.80(c)(1)(iii), 600.80(c)(1)(iii).

[129] 68 Fed. Reg. No. 50, III.D.9.

[130] 68 Fed. Reg. No. 50, III.A.4 (emphasis added).

The proposed rule provides that contractors would be subject to complying with certain post-marketing safety reporting responsibilities. Specifically, under the proposed regulations, contractors would be required to submit safety reports of *any* SADRs or medication errors about the manufacturer's product to the manufacturer within 5 calendar days of receipt of the report by the contractor.[131] The proposed rules would ultimately hold manufacturers responsible under the regulations for making expedited reports when necessary to the FDA.

The ICH Guidelines, unlike the proposed FDA rules, do not recommend that contractors report every adverse drug experience. Rather, the Guidelines recommend that when entering into contracts with other companies, manufacturers include in such contracts specific time frames for exchange of serious and non-serious adverse event reports based on date first learned by the contractor (e.g., 5 to 8 calendar days for serious adverse experiences and 30 calendar days for non-serious AEs).[132] In fact, the ICH Guidelines specifically provide that such agreements between manufacturers and contractors are necessary "to avoid duplicate reporting to the regulatory authority, e.g. assigning responsibility to one company for literature screening."[133] The ICH Guidelines, therefore, allow for greater flexibility between a manufacturer and a contractor for purposes of defining reporting obligations. However, like both the FDA regulations and proposed rules, the ICH Guidelines make clear that it is ultimately the manufacturer's responsibility, and not the contractor's, to fulfill all reporting obligations under the regulations.

Participants in a pharmacovigilance program should watch the development of these proposed rules carefully, to determine whether health systems or HIEs would ultimately be treated as "contractors" and what reporting obligations would be triggered.

V. The FDA Amendments Act of 2007

On September 27, 2007, the President signed legislation that makes significant changes to the FDA's statutory authority regarding postmarket drug safety. The Food and Drug Administration Amendments Act of 2007 (FDAAA)[134] includes a number of provisions relating to drug safety, requiring the FDA to establish a system for postmarket drug safety surveillance, granting the FDA power to require post-market studies, labeling changes and disclosure in direct-to-consumer advertising, and authorizing the FDA to require risk evaluation and mitigation strategies (REMS) by manufacturers. In this section we discuss the two new requirements relevant to pharmacovigilance programs: active postmarket risk identification and analysis and REMS.

The new law does not extend the FDA's jurisdiction beyond the regulation of manufacturers and applicants, packers and distributors, joint manufacturers, shared manufacturers, or any participant involved in divided manufacturing. Thus, even though the FDA may have broader regulatory powers under the new law, the law does not impose any additional requirements on HIEs or health systems.

A. Active Postmarket Risk Identification and Analysis

Title IX of the FDAAA requires the FDA to develop within two years enhanced postmarket surveillance, by creating methods to obtain access to different data sources and validated methods to link data from various sources.[135] The goal is to collaborate with public, academic and private entities to link and analyze safety data from at least 25 million patients by 2010 and 100 million patients by July 2012.

---

[131] Federal Register, Vol. 68, No. 50 III.D.9.
[132] ICH E2D ver. 3.8, 3.3.
[133] *Id*.
[134] Public Law 110-85.
[135] FDAAA § 905(a), *amdending* 21 U.S.C. § 355.

After these methods are developed, the Secretary is required to establish procedures for a "postmarket risk identification and analysis system" that complies with HIPAA and does not disclose individually identifiable health information. The system will report data on all serious adverse drug experiences, provide trends and patterns of events for the Secretary, serve as active surveillance with electronic health information from available data sources (such as Medicare and VA databases, health insurance claims, and pharmaceutical purchased data), and export data for further aggregation and analysis. The FDAAA also requires the Secretary to collaborate with public, academics, and private entities in advanced analysis of drug safety data to "(i) improve the quality and efficiency of postmarket drug safety risk-benefit analysis; (ii) provide the Secretary with routine access to outside expertise to study advanced drug safety questions; and (iii) enhance the ability of the Secretary to make timely assessments based on drug safety data."[136] The statute specifies that such advanced analysis "shall not disclose individually identifiable health information when presenting such drug safety signals and trends or when responding to inquiries."[137]

While the statute does not expressly mention HIEs or the electronic health records of health systems as potential data sources, the development of pharmacovigilance programs using these data sources likely will be of great interest to the FDA. Moreover, the statute authorizes the FDA to enter into contracts with "qualified entities" to classify, analyze or aggregate data, and to investigate drug safety questions. Sophisticated health systems and HIEs involved in pharmacovigilance programs may meet the requirements of "qualified entities" to collaborate with the FDA on these issues.

B. Risk Evaluation and Mitigation Strategies (REMS)

Title IX of the FDAAA authorizes the Secretary to require risk evaluation and mitigation strategies (REMS) when necessary to ensure that the benefits of a drug outweigh the risks.[138] The Secretary may require a REMS for new applications, as well as for drugs and biologics that already are approved where the Secretary becomes aware of new safety information. "New safety information" can come from a variety of sources, including clinical trial results, adverse event reports, postapproval studies (including Phase IV studies, peer-reviewed journals, and data derived from the REMS). Many of the risk management strategies will look familiar to those used today in Risk Minimization Action Plans (RiskMAPS).[139]

When the Secretary notifies a manufacturer that it requires a REMS for a certain drug, manufacturers must submit a proposed REMS within 120 days. The FDA will review the proposed REMS, require any additional elements the FDA believes are necessary, and, ultimately, approve the REMS (after structured negotiations if necessary). The REMS will again be reviewed at 18 months, 3 years, and 7 years (unless the risks are adequately managed before the 7-year review), as well as in labeling supplements and when FDA requests a review. The FDA also has authority to require communication with patients via medication guides or patient package inserts, and with prescribing health care providers through "dear doctor" letters or communications to professional societies.

The participants in a pharmacovigilance program should carefully monitor any regulations or guidance issued by the FDA to implement the REMS requirements in the FDAAA. The data generated from a pharmacovigilance program may be a valuable data source for the FDA to utilize in evaluating drug risks after approval.

---

[136] *Id.*

[137] *Id.*

[138] FDAAA § 901, *amending* 21 U.S.C. § 355.

[139] *See* http://www.fda.gov/OHRMS/DOCKETS/98fr/2004d-0188-gdl0001.doc.

VI. Tort Liability under the Common Law

In assessing the risks associated with a pharmacovigilance program, each of the participants must evaluate whether it will have a common law duty to warn patients or physicians of potential drug risks that are identified through the pharmacovigilance program and whether a failure to do so can result in liability under a common law tort theory. This section discusses the general state of the law relating to the common law duties and potential claims arising from a failure to warn of potential adverse side effects of FDA-approved drugs. If course, common law liability will be governed by applicable state law, so the participants in a pharmacovigilance program should look carefully at how the law of the applicable jurisdiction will affect this analysis.

A. Manufacturers

The law imposes a duty on drug manufacturers to warn of the dangers of a prescription drug under theories of products liability and negligence. This section discusses the development of these theories across various jurisdictions and the possibility of FDA preemption of common law liability.

1. Strict Product Liability

As a general matter, the law of products liability provides that "one engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect."[140] Thus, a manufacturer of a "defective" product is strictly liable for harms caused by the defect. A product is considered defective when, at the time of the sale or distribution, it contains a manufacturing defect, is defective in design, or is defective because of inadequate instructions or warnings.[141] A product is defective because of inadequate instructions or warnings when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller; the omission of the instructions or warnings renders the product not reasonably safe.[142] This section address liability from inadequate warnings; products liability claims based on alleged design or manufacturing defects are beyond the scope of our analysis.

Most courts deem prescription drugs to be "unavoidably unsafe" products and therefore "defective" only upon a failure to adequately warn of the product's dangers.[143] Most product liability claims in the context of prescription drugs therefore turn on the adequacy of the manufacturer's warnings of the risks associated with the drug.

---

[140] Restatement (Third) of Torts: Prod Liab. § 1 (1998).

[141] *Id*. at § 2.

[142] *Id.* at § 2(c).

[143] Restatement (Second) of Torts, § 402A, comment k. The majority of courts treat Section 402's comment k as an affirmative defense allowing a manufacturer to avoid strict liability upon a showing that the product cannot be reasonably redesigned. *See generally Ziliak v. Astrazeneca LP,* 324 F.3d 518 (7th Cir. 2003) (Indiana recognizes that some products such as pharmaceuticals are "unavoidably unsafe" in that they are incapable of being made completely safe for their intended or ordinary use; such a product, properly prepared and accompanied by proper directions and warnings, is not defective or unreasonably dangerous); *Martin v. Hacker,* 83 N.Y. 2d 1, 628 N.E.2d 1308, 607 N.Y.S.2d 598 (App. 1993) (although prescription drugs are by nature inherently unsafe and would in the usual case impose strict liability to its manufacturer, defense is provided against such liability when drug is properly prepared and accompanied by proper directions and warnings). Note that the Third Restatement has adopted a different rule requiring a balancing of foreseeable harm against foreseeable benefits. Restatement (Third) of Torts: Prod. Liab. § 6 (1998).

Importantly, a failure to comply with FDA reporting requirements can affect whether a prescription drug is deemed to be defective in a products liability claim. As the Restatement recognizes, a failure to comply with a product safety statute or administrative regulation may render a product "defective" for inadequate instructions or warnings,[144] and a number of courts across the country have held that a manufacturer's failure to comply with FDA reporting requirements renders a product defective under a products liability theory. In the Third Circuit Court of Appeals, for example, the court held a manufacturer of local anesthetic liable under a strict liability theory because the manufacturer failed to report adverse events to the FDA.[145]

On the other hand, compliance with FDA reporting requirements does not conclusively establish that a manufacturer has complied with its duty to warn of product dangers—such compliance is a factor to be considered in determining whether a product is "defective" and whether a manufacturer has complied with its common law duties, but is not determinative.[146] The majority of courts have held that compliance with product safety regulations is relevant and admissible on the question of defectiveness, but is not necessarily controlling.[147] However, while courts do not treat compliance with safety regulations to be conclusive, some courts give such compliance substantial weight. [148] Moreover, some states have enacted safety regulation statutes that create a presumption that a product is non-defective where a manufacturer complies with those regulations.[149] So, pharmacovigilance participants should pay close attention to the product liability laws in the state of operation.

---

[144] *See* Restatement (Third) of Torts: Prod. Liab. § 4 (a) (1998) ("a product's noncompliance with an applicable product safety statute or administrative regulation renders the product defective with respect to the risks sought to be reduced by the statute or regulation").

[145] *See Stanton by Brooks v. Astra Pharmaceutical Products, Inc.*, 718 F.2d 553 (3rd Cir. 1983) (imposing strict liability where the manufacturer's failure to comply with statutory and regulatory requirement for filing of adverse event reports with FDA rendered the anesthetic a "defective product"); 63 Am. Jur. 2d Products Liability § 603 (the Restatement of Torts 2d §402A, Comment k, does not apply where a drug manufacturer failed to comply with FDA regulations requiring submission of adverse event reports, since the manufacturer's failure rendered the product defective by depriving the FDA of information necessary to make an informed judgment concerning the conditions under which the product could be safely marketed).

[146] *See* Restatement (Third) of Torts, §4(b) (1998) ("In connection with liability for defective design or inadequate instructions or warnings: … (b) a product's compliance with an applicable product safety statute or administrative regulation is properly considered in determining whether the product is defective with respect to this risks sought to be reduced by the statute or regulation, but such compliance does not preclude as a matter of law a finding of product defect.").

[147] *See, e.g., O'Gilvie v. International Playtex, Inc.*, 821 F.2d 1438 (10th Cir. 1987) (hold that it was proper under Kansas law to give a jury instruction that a tampon package warning that complied with FDA regulations was not a defense in strict liability action if a reasonable and prudent manufacturer would have taken additional precautions); *Foyle v. Lederle Labs.* 674 F. Supp. 530 (E.D.N.C. 1987) (holding that the FDA regulations are simply minimum standards; compliance with the FDA regulations is mandatory but did not preclude the manufacturer from taking additional action); *Plenger v. Alza Corp.*, 13 Cal. Rptr. 2d 811 (1992) (holding that compliance with FDA warning regulations may not be sufficient to immunize the manufacturer from liability; the required warnings may be only minimal in nature and where the manufacturer knows or has reason to know of greater dangers that are not included in the warning, its duty to warn may not be fulfilled).

[148] *See, e.g., Sims v. Washex Mach. Corp.*, 932 S.W.2d 559 (Tex. App. 1995) (compliance with governmental regulations is strong evidence, although not conclusive, that a machine was not defectively designed).

[149] *See* Kan. Stat. Ann. § 60-3304; Colo. Rev. Stat. § 13-21-403; N. Dakota Code § 28-01.1-5(3); Tenn. Code Ann. § 29-28-104; Utah Judicial Code § 78-15-6(3).

2. Negligence

The law of negligence also imposes a duty on drug manufacturers to warn of product dangers. Generally, the tort of negligence is comprised of three elements: (1) a duty that the defendant owes to the plaintiff; (2) the defendant's failure to conform its conduct to the requisite standard of care required by the defendant's relationship with the plaintiff; and (3) an injury to the plaintiff resulting from that failure.[150] To determine whether a duty exists, courts look to a state's statutes and controlling law,[151] so this analysis will vary from state to state.

Under both products liability and negligence, the focus of the legal inquiry is whether the manufacturer took adequate steps to warn of potential dangers. This overlap in analysis has led some courts to conflate the two causes of action:

> Products liability action may be brought against a supplier of an inherently unsafe or dangerous product on a theory of strict liability for harm caused by the product or its use unless adequate warnings or instructions are given and on a theory of negligence if the warnings are inadequate. Some courts will allow only claims of negligence, not strict liability, for an inadequate warning in a case involving an unavoidably unsafe product while other courts see this as a distinction without a difference and allow plaintiffs to plead either or both negligence and strict liability whether there is a failure to warn or an inadequate warning.[152]

Some jurisdictions, however, continue to draw a distinction between failure to warn for purposes of product liability and negligence:

> Failure to warn in strict liability differs markedly from a failure to warn in the negligence context. Negligence law in a failure-to-warn case requires a plaintiff to prove that a manufacturer or distributor did not warn of a particular risk for reasons which fell below acceptable standards of care, i.e., what a reasonably prudent manufacturer would have known and warned about. Strict liability is not concerned with the standard of due care or the reasonableness of a manufacturer's conduct. The rules of strict liability require a plaintiff to prove only that the defendant did not adequately warn of a particular risk that was known or knowable in light of the generally recognized and prevailing best scientific and medical knowledge available at the time of manufacture and distribution.[153]

Under either theory, there is a clear duty imposed on drug manufacturers to warn of the dangers of the drugs it manufactures. This duty applies regardless of the source of the information relating to the risks and, therefore, would most likely be applied by courts in connection with information learned through a pharmacovigilance program.

---

[150] *See, e.g. Ingram v. Hook's Drugs, Inc.*, 476 N.E.2d 881 (Ind. 1985).
[151] *Stanley v. McCarver,* 208 Ariz. 219, 92 P.3d 849 (2004).
[152] 63A Am. Jur. 2d Products Liability § 1116 (2007). *See also Feldman v. Lederle Labs,* 97 N.J. 429, 479 A.2d 374 (N.J. 1984) (in warnings cases, negligence and strict liability are "functional equivalents"); *Ortho Pharmaceutical Corp. v. Chapman,* 180 Ind. App. 33, 388 N.E. 2d 541 (1979) (where duty to warn is under consideration, standard of strict liability is essentially similar to standard for establishing negligence); *Martin v. Hacker,* 83 N.Y. 2d 1, 628 N.E.2d 1308, 607 N.Y.S.2d 598 (App. 1993) (where liability is predicated on failure to warn, New York views negligence and strict liability claims as equivalent).
[153] *Carlin v. Superior Court,* 13 Cal. 4th 1104, 56 Cal. Rptr. 2d 162, 920 P.2d 1347 (1996).

Like in products liability claims, a manufacturer's compliance or failure to comply with FDA reporting requirements will have an impact on failure to warn negligence claims. Compliance with regulatory safety requirements is generally considered evidence that a defendant was not negligent, but does not establish conclusively that there was no negligence.[154] In the negligence context, the requirements of a safety statute or regulations can serve as the reasonable standard of conduct applied to determine negligence.[155]

If a defendant fails to comply with regulatory safety requirements, however, courts have treated that failure in one of three ways: (1) as conclusive evidence of negligence or negligence per se;[156] (2) as evidence of negligence that must be considered in conjunction with other evidence;[157] or (3) as a presumption of negligence that may be rebutted by the defendant.[158] Unlike in the strict product liability context, in negligence claims courts in some jurisdictions have considered whether the failure to comply with regulatory safety requirements is "excusable," such as where the defendant is not able to provide a warning.[159] It is unlikely that a court would find a drug manufacturer's failure to comply with FDA reporting requirements as excusable, but may be amenable to arguments that direct warnings to physicians or patients were not feasible.

3. Content, Timing, Target and Methods of Warnings

The questions then become what must be included in the warnings, to whom warnings should be given, and how those warnings should be delivered. In both the products liability and negligence contexts, courts have imposed a duty on manufacturers to warn of dangers that should be known to them.[160] In

---

[154] *See Edwards v. Basel Pharmaceuticals,* 933 P.2d 298 (Okla. 1997) (compliance with FDA warning requirements did not necessarily satisfy manufacturer's common law duty to warn the consumer).
[155] *See* Restatement (Second) of Torts, § 286.
[156] *See Stanton, supra., Britton v. Wooten,* 817 S.W.2d 443 (Ky. 1991); *Bullington v. Texas Electric Service Co.,* 570 F.2d 1272 (5th Cir. 1978).
[157] *See Franco v. Bunyard,* 261 Ark. 144, 547 S.W.2d 91 (1977); *Roberts v. Shop & Go, Inc.,* 502 So. 2d 915 (Fla. App. 1986).
[158] *See Cloverleaf Car Co. v. Phillips Petroleum Co.,* 213 Mich. App. 186, 540 N.W.2d 297 (1995); *Babcock v. Chesapeake Ry. Co.,* 83 Ill. App. 3d 919, 404 N.E.2d 265 (1979); *Lewis v. Lockard,* 498 N.E.2d 1024 (Ind. App. 1986); *Toole v. Richardson-Merrell Inc.,* 251 Cal App. 2d 689, 60 Cal. Rptr. 398 (1967) (failure of drug manufacturer to comply with statute requiring submission of full reports of investigations made to show whether or not the drug is safe for use raised presumption of negligence).
[159] Restatement (Second) of Torts, §288A (a failure to comply may be considered excusable where: (1) the violation is reasonable because of the actor's incapacity to act; (2) the actor neither knows nor should know of the occasion for compliance; (3) the actor is unable after reasonable diligence or care to comply; (4) the actor is confronted by an emergency not due to the actor's own misconduct; or (e) compliance would involve a greater risk of harm to the actor or others); *see also Stanton, supra.*
[160] *See, e.g. Schaerrer v. Stewart's Plaza Pharmacy, Inc.,* 79 P.3d 922 (Utah 2003) (manufacturer is obligated to warn of any dangerous side effects of which it knows or has reason to know); *Motus v. Pfizer Inc.,* 196 F. Supp. 2d 984 (C.D. Cal. 2001 (manufacturer duty to warn about any known or reasonably knowable danger); *Martin v. Hacker,* 83 N.Y.2d 1, 628 N.E.2d 1308, 607 N.Y.S.2d 598 (1993) (manufacturer duty to warn of all potential dangers in its prescription drugs that it knew, or in the exercise of reasonable care, should have known to exist); *Wagner v. Roche Laboratories,* 77 Ohio St. 3d 116, 671 N.E.2d 252 (1996) (manufacturer has duty to warn of all potential adverse reactions inherent in use of the drug which manufacturer, being held to standard of expert in the field, knew or should have known at the time of marketing); *Edwards v. Basel Pharmaceuticals,* 933 P.2d 298 (Okla. 1997) (manufacturer required to warn of dangers which are foreseeable and known to the manufacturer); *Ziliak v. AstrazenecaLP,* 324 F.3d 518 (7th Cir. 2003) (under Indiana law, duty to provide adequate warnings arises when the manufacturer knows or should know of a risk posed by the product); *Ortho Pharmaceutical Corp. v. Chapman,* 180 Ind. App. 33,

determining what a manufacturer *should* know, courts will hold a manufacturer to the standard of an expert in the field and will impose a continuous duty to keep abreast of scientific developments touching upon its product and to notify the profession of any additional side effects discovered from its use.[161] Moreover, courts have imposed a duty to warn of side effects associated with a drug, even where an actual causal connection between the drug and adverse side effect has not been conclusively established.[162]

Once there is a duty to warn, the warning must be timely and adequate.[163] Generally, warnings are considered adequate when they contain a full and complete disclosure of the potential adverse reactions to the drug. A reasonable warning not only conveys a fair indication of the dangers involved, but also warns with a degree of intensity required by the nature of the risk.[164] Courts treat the following items as relevant in determining whether a warning is adequate: (1) the warning must adequately indicate the scope of the danger; (2) the warning must reasonably communicate the extent or seriousness of the harm that could result from a misuse of the drug; (3) the physical aspects of the warning must be adequate to alert a reasonably prudent person to the danger; (4) a simple directive warning (i.e. do not take with alcohol) may be inadequate when it fails to indicate the consequences that might result from a failure to follow it; and (5) the means to convey the warning must be adequate.[165]

Of course, one of the ways in which manufacturers fulfill their duty to warn is by updating product labeling when new information becomes available. FDA regulations require labeling "to be revised to include a warning as soon as there is reasonable evidence of an association of a serious hazard with a drug; a causal relationship need not have been proved."[166]

However, a manufacturer's duty to warn is not limited to FDA-approved label changes. When promulgating its regulations, the FDA made it clear that:

> These labeling requirements do not prohibit a manufacturer, packer, relabeler, or distributor from warning health care professionals whenever possibly harmful adverse effects associated with the use of the

---

388 N.E.2d 541 (1979) (manufacturer's duty to warn of risks attendant in use of its product does not arise until manufacturer knows or should know of a risk involving the drug's use; a manufacturer cannot be required to warn of a risk unknown to science).

[161] *See e.g., Schenebeck v. Sterling Drug Inc.,* 423 F.2d 919 (8th Cir. 1970); *McEwen v. Ortho Pharmaceutical Corp.,* 270 Or. 375, 528 P.2d 522 (1974).

[162] *See. E.g. Wooderson v. Ortho Pharmaceutical Corp.,* 235 Kan. 387, 681 P.2d 1038 (1984) (duty to warn where study showed a positive correlation between drug and side effect); *Seley v. G.D. Searle & Co.,* 67 Ohio St. 2d 192, 423 N.E.2d 831 (1981) (duty to warn where causal relationship not conclusively established; it is enough to trigger duty if a danger is associated with use of the drug); *Hamilton v. Hardy,* 37 Colo. App. 375, 549 P.2d 1099 (1976) (under strict liability theory, a manufacturer must warn of dangers and risks whether or not a causal relationship between the use of the product and injuries has been definitely established); *McNeil v. Wyeth,* 462 F.3d 364 (5th Cir. 2007) (Texas law does not absolve manufacturer of duty to warn of harmful conditions associated with use of its product merely because there are no existing studies or clinical trials proving actual causation).

[163] *See generally* C.J.S. Drugs and Narcotics § 60 (2007).

[164] *Pittman v. Upjohn Co.,* 890 S.W.2d 425 (Tenn. 1994).

[165] *Thom v. Bristol-Myers Squibb Co.,* 353 F.3d 848 (10th Cir. 2003), *quoting Pittman v. Upjohn Co.,* 890 S.W.2d 425 (Tenn. 1994). *See also Martin v. Hacker,* 83 N.Y.2d 1, 607 N.Y.S. 2d 598, 628 N.E.2d 1308 (App. 1993) (the warning of a prescription drug's dangers is to be read and understood by physicians, not laypersons, factors to be considered in determining whether a warning is adequate include whether the warning is accurate, clear, consistent on its face, and whether it portrays with sufficient intensity the risk involved in taking the drug).

[166] 21 C.F.R. § 201.57(e).

> drug are discovered. The addition to labeling and advertising of additional warnings, as well as contraindications, adverse reactions, and precautions regarding the drug, or the issuance of letters directed to health care professionals (e.g., "Dear Doctor" letters containing such information) is not prohibited by these regulations.[167]

Indeed, the FDA has promulgated regulations guiding the dissemination of information to health care professionals making it clear that it expects such communication to take place outside of labeling changes.[168] Specifically, FDA regulations state that:

> Manufacturers and distributors of drugs and the Food and Drug Administration occasionally are required to mail important information about drugs to physicians and others responsible for patient care. In the public interest, such mail should be distinctive in appearance so that it will be promptly recognized and read.[169]

In some cases, courts have found it insufficient for a manufacturer to simply notify the FDA of learned risks and have imposed upon manufacturers an obligation to send such "Dear Doctor" letters or to enlist the assistance of the manufacturer's sales force to alert physicians of particular risks.[170]

The FDA does not impose a duty to warn consumers directly. Warning to health care professionals also is consistent with the conclusions of most courts applying products liability and negligence theories. Under both types of claims, most courts have adopted the "learned intermediary doctrine," which holds that a manufacturer of prescription drugs satisfies its duty to give notice of potential drug dangers by notifying the physicians who will prescribe the drugs. Under this doctrine, the manufacturer of a prescription drug has no duty to directly warn consumers of drug dangers.

The rationale behind the learned intermediary doctrine is that only health care professionals are in a position to understand the significance of the risks involved and to assess the relative advantages and disadvantages of the prescription drug at issue. Once adequate warnings are provided to the physician, it becomes the duty of the physician to provide such information to the physician's patients to allow the patients to make informed decisions.[171]

There are, however, limitations to the learned intermediary defense that have eroded protections offered to manufacturers. If the manufacturer knows that physicians will not be in a position to reduce the risk

---

[167] 44 Fed. Reg. 37434, 37447 (June 26, 1979).
[168] *See* 21 C.F.R. § 200.5. *See generally Perry v. Novartis Pharma. Corp.*, 456 F. Supp. 2d 678 (E.D. Pa. 2006).
[169] 21 C.F.R. § 200.5. That regulation further details the appropriate "distinctive" characteristics that such mailings should have, including statements such as "IMPORTANT DRUG WARNING," IMPORTANT PRESCRIBING INFORMATION," OR IMPORTANT CORRECTION OF DRUG INFORMATION."
[170] *See, e.g. Mahr v. G.D. Searle & Co.*, 72 Ill. App. 3d 540, 390 N.E.2d 1214 (1979) (evidence that manufacturer's detailmen called upon practicing physicians an average of four times per year supported conclusion that practice of promotion of drug through personal contact by sales force permitted an effective form of communicating risks involved in use of drug and manufacturer's failure to make use of such form indicated that it also failed to make reasonable efforts to effectively warn medical community about dangers); *Mikell v. Hoffman, LaRoche, Inc.*, 649 So.2d 75 (La. App. 1994) (manufacturer satisfied duty to warn where it had sent "Dear Doctor" letter to all physicians in the country warning that it had received reports of possible side effect of inflammatory bowel disease associated with use of medication).
[171] *See, e.g., Harnish v. Children's Hospital Medical Center*, 387 Mass. 152, 155 (1982) (the prescribing physician has the ultimate duty to disclose in a reasonable manner all medical information that the physician possesses or reasonably should possess that is material to an intelligent decision by the patient whether to take the medication).

of harm to patients, the doctrine may not apply.[172] Courts have therefore recognized exceptions to the learned intermediary doctrine where: (1) there is unlikely to be a meaningful doctor-patient relationship, such as in mass inoculations;[173] (2) where the manufacturer conducts direct-to-consumer advertising;[174] or (3) the manufacturer has "over- promoted" the drug.[175] In addition, several courts have identified as a rationale for the learned intermediary doctrine the practical difficulties associated with a requirement on manufacturers to notify ultimate consumers of potential risks,[176] indicating that the ability to notify consumers may be a factor in a court deciding not to apply the learned intermediary doctrine. Moreover, at least one court refused to adopt the learned intermediary doctrine at all, finding the justifications for the rule to be "largely outdated and unpersuasive."[177] [178]

As evidenced by the growing number of exceptions to the learned intermediary doctrine and the expressed concerns regarding the continued viability of the justifications for this doctrine in modern times, this area of the law remains unsettled.[179] As noted in the Third Restatement, "The Institute leaves

---

[172] *See* Restatement (Third) of Torts: Prod. Liab. § 6(d) (A prescription drug or medical device is not reasonably safe due to inadequate instructions or warnings if reasonable instructions or warnings regarding foreseeable risks of harm are not provided to: (1) prescribing and other health care providers who are in a position to reduce the risks of harm in accordance with the instructions or warnings; or (2) the patient when the manufacturer knows or has reason to know that health-care providers will not be in a position to reduce the risks of harm in accordance with the instructions).

[173] *See, e.g., Davis v. Wyeth Laboratories, Inc.,* 399 F.2d 121 (9th Cir. 1968); *Givens v. Lederle,* 556 F.2d 1341 (5th Cir. 1977); *Brazzell v. United States,* 788 F.2d 1352 (8th Cir. 1986).

[174] *See Perez v. Wyeth Laboratories, Inc.,* 161 N.J. 1, 734 A.2d 1245 (1999) (when mass-marketing of prescription drugs seeks to influence a patient's choice of a drug, a manufacturer that makes direct claims to the consumer for the efficacy of its product should not be relieved of the duty to give proper warnings). Proponents of the doctrine assert that it should still apply in circumstances of direct patient advertising because a prescribing physician must still be involved in the administration of the prescription drug and is in the best position to determine whether a particular drug is appropriate for a particular patient. Further, it is argued, the FDA requires that drug manufacturers include in such advertisements information about side effects. Still, several courts have indicated that consumer-directed advertising is a factor to be taken into account in deciding whether to apply the learned intermediary rule. *See, e.g., Stephens v. G.D. Searle & Co.,* 602 F. Supp. 379 (E.D. Mich. 1985); *Hill v. Searle Labs,* 884 F.2d 1064 (8th Cir. 1989). *See also MacDonald v. Ortho Pharmaceutical Corp.,* 394 Mass. 131, 475 N.E.2d 65 (1985).

[175] *See, e.g., Proctor v. Davis,* 291 Ill. App. 3d 265, 682 N.E.2d 1203 (1997).

[176] *See Linnen v. A.H. Robbins Co., Inc.,* 2000 WL 89379 (Mass. Super. 1999) (where it is unreasonable to expect the manufacturer to communicate directly with the consumer, the manufacturer may be absolved from blame because of reliance on a middleman) (citations omitted); *Larkin v. Pfizer, Inc.,* 153 S.W. 3d 758 (Ky. 2005) (one rationale for the learned intermediary rule that relieves drug manufacturers from liability to ultimate consumers if they provide adequate warning to prescribing physicians is that manufacturers lack effective means to communicate directly with each patient); *Johnson & Johnson Corp. v. Karl,* 220 W. Va. 463, 647 S.E.2d 899 (2007) (among the primary justifications that have been advanced for the learned intermediary doctrine are the difficulties manufacturers would encounter in attempting to provide warnings to the ultimate users of the drugs).

[177] *Johnson & Johnson Corp. v. Karl*, 220 W. Va. 463, 647 S.E.2d 899 (2007) (exhaustively detailed the status of the learned intermediary doctrine in various states, identifying states in which the highest court has not adopted the learned intermediary doctrine and concluding that "while the doctrine is widely applied among lower courts, the number of high courts who have followed suit and expressly adopted the doctrine, while admittedly in the majority, do not make up the overwhelming majority that has often been suggested by courts and commentators").

[178] *Id.* at 905.

[179] *See, e.g., Vitanza v. Upjohn Co.,* 214 F.3d 73 (2nd Cir. 2000) (holding that the current effect of the doctrine was uncertain in Connecticut).

to developing case law whether exceptions to the learned intermediary rule in these or other situations should be recognized."[180]

The application of the learned intermediary doctrine in the context of a pharmacovigilance effort likely will be challenging. Depending on how the project is structured, the manufacturer may have access to specific doctor and patient information relating to the drug at issue. This would reduce the persuasiveness of arguing that it is not "practicable" for the manufacturer to identify and notify particular patients about drug risks. In light of the erosion of and uncertainty relating to the continued viability of the doctrine, a court might carve out another exception to the learned intermediary doctrine, requiring direct consumer notification of risks where the patient-identifying information is readily available to the manufacturer. Note, however, that the other justifications in support of the learned intermediary rule remain, including the position that only health care professionals are in a position to understand the significance of the warning and to weigh the risks and benefits of the medication. Manufacturers therefore still have a strong argument that the doctrine should continue to apply and that they should not be required to notify consumers directly of information about drug risks gathered through a pharmacovigilance project.

4. Preemption by FDA Regulation

Because manufacturers of prescription drugs are heavily regulated by the FDA, we discuss whether state law tort claims may be preempted by the federal scheme regulating these drugs. As a general matter, the FDA regulations for prescription drug manufacturing, advertising, and distribution do not preempt state law tort claims.[181]

Generally, there are three kinds of preemption: express preemption, field preemption, and conflict preemption. Express preemption exists when Congress states a clear intent to preempt state law.[182] Conflict preemption can be either direct or indirect. A direct conflict occurs "where it is impossible for a private party to comply with both state and federal requirements."[183] An indirect conflict exists "where state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."[184] Field preemption arises when "Congress has legislated comprehensively, thus occupying an entire field of regulation and leaving no room for the States to supplement federal law."[185]

Manufacturers charged with failure to warn in prescription drug cases most often assert that a plaintiff's case is barred by conflict preemption, where state law duties to warn necessarily result in violations of certain FDA regulations. The FDA regulations require that before a manufacturer amends or changes a warning label to include newly discovered risks of a prescription drug, the manufacturer must submit an application for approval.[186] Failure to comply with the FDA regulations may result in a finding that a drug was mislabeled and, ultimately, in the recall of the drug. Manufacturers, therefore, must strictly

---

[180] Restatement (Third) of Torts: Prod. Liab. § 6, comment e.

[181] *See MacDonald v. Ortho Pharmaceutical Corp*., 394 Mass. 131, 140 (1985) ("Compliance with FDA requirements, though admissible to demonstrate lack of negligence, is not conclusive on this issue, just as violation of FDA requirements is evidence, but not conclusive evidence, of negligence."); *McMullen v. Medtronic*, 421 F.3d 482, 489 (7th Cir. 2005) (holding that because a manufacturer does not have the unilateral authority to warn of a risk or issue a recall, it is not liable for post-sale duty to warn where FDA did not approve warning changes); *Smithline Beecham Consumer Healthcare*, 32 Cal.4th 910, 920 (Cal. 2004) (plaintiff's case preempted by federal law when defendant asked the FDA for permission to change the label and the FDA denied the request).

[182] *See, e.g*. Medical Device Amendment, 21 U.S.C. § 360c *et seq*.

[183] *English v. General Elec. Co.*, 496 U.S. 72, 79 (1990).

[184] *Id*.

[185] *Louisiana Public Service Comm'n v. F.C.C.*, 476 U.S. 355, 368 (1986).

[186] *See* 21 C.F.R. § 314.70.

comply with the process set forth in the FDA regulations when seeking to amend or change a warning label and may be unable to comply with contrary state labeling requirements. Based on this argument, some courts have held that preemption applies in a narrow scope of cases where state law requires the addition or change of a label warning but the FDA has determined that insufficient scientific evidence supports such a label change.[187] Courts generally have been reluctant to apply preemption to bar a plaintiff's claim absent this clear evidence of a conflict between state and federal requirements.[188]

Moreover, notwithstanding the FDA regulations requiring preapproval of all label changes, a manufacturer may disseminate safety information by other means, especially if the changes are intended "to add or strengthen a contradiction, warning, precaution, or adverse reaction."[189] Because the FDA regulations provide an alternative method to warn about newly discovered risks before an application for labeling changes is approved by the FDA, courts have rejected the argument that federal and state law is in conflict.[190] FDA preemption thus is unlikely to negate any duty by manufacturers to warn health care professionals (and potentially patients) of additional risks discovered under a pharmacovigilance program.

B. Health Systems and HIEs

Two categories of electronic health information holders may be involved in pharmacovigilance projects: (1) health systems that have a direct relationship to the patients whose records are being reviewed; and (2) HIEs where there is no direct relationship with the patients. This section addresses potential liability under strict liability and negligence theories for failure to warn.

1. Strict Product Liability

A health system first should consider whether its state laws would impose any liability for acting as a retailer or distributor of a prescription drug, because employees of the health system may be distributing prescription drugs under a physician's orders and the health system may run a retail pharmacy. However, courts generally have refused to hold nonmanufacturing retail sellers of prescription drugs liable under strict product liability, unless the retailer or distributor fails to exercise reasonable care in connection with the distribution of the drug. "In so limiting the liability of the intermediary parties, courts have held that they should be permitted to rely on the special expertise of manufacturers, prescribing and treating health-care providers, and governmental regulatory agencies."[191] Courts also have declined to extend strict product liability based on a failure to warn to hospitals and pharmacists, holding that they are providers of services rather than purveyors of products.[192] Thus, even where a

---

[187] *Id*.; *see also Ackerman v. Wyeth*, 2006 U.S. Dist. LEXIS 64499, *18 (E.D.Tex. 2006); *Colacicco v. Apotex, Inc*., 432 F.Supp.2d 514, 522 (E.D.Pa. 2006); *Perry v. Novartis Pharm. Corp*., 456 F.Supp.2d 678, 683 (E.D.Pa. 2006); *Witzak v. Pfizer, Inc*., 377 F.Supp.2d 726, 730 (D.Minn. 2005).

[188] *See Geier v. American Honda Motor Co., Inc*., 529 U.S. 861, 885 (2000); *Kelly v. Wyeth*, 2007 WL 1302589 (Mass. Super. 2007).

[189] 21 C.F.R. § 314.70 (c)(6)(iii)(A); *see also Novartis Pharm. Corp*., 456 F.Supp.2d at 683; *Laisure Radke v. Par Pharm, Inc*., 426 F.Supp.2d 1163, 1169 (W.D.Wash. 2006) (holding that a manufacturer can add or strengthen a contradiction, warning, precaution, or adverse reaction at any time without prior FDA approval).

[190] *See Kelly v. Wyeth*, 2007 WL 1302589 at *5-6 (finding no conflict between FDA regulations and state law).

[191] *See* Restatement (Third) of Torts: Prod. Liab. §6(e) and comment h.

[192] *Madison v. American Home Products, Corp.,* 257 S.C. 449, 595 S.E.2d 493 (2004) (a pharmacy will not be held strictly liable for properly filling a prescription in accordance with a physician's orders; in filling a prescription, a pharmacy is providing a service rather than selling a product); *In Re Breast Implant Product Liability Litigation,* 331 S.C. 540, 503 S.E.2d 445 (1998) (collecting cases in jurisdictions which hold health care professionals and institutions are providers of services rather than sellers of products for purposes of

health system learns of potential prescription drug dangers by participating in a pharmacovigilance project, it is unlikely that a court would hold the system liable under a strict liability theory.

Similarly, it is unlikely that a court would hold an HIE participant liable under a strict liability theory; an HIE is not in the retail or distribution chain of the pharmaceutical product.

2. Negligence

As discussed above, the essence of a claim for negligence is the imposition of a legal duty and the failure to carry out that duty.[193] Absent a doctor-patient relationship, the law generally has been reluctant to impose a duty to warn patients of potential dangers of drugs. Notably, many of these cases extend the learned intermediary doctrine to hospitals and pharmacies in support of a conclusion that there is no duty to warn of the dangers of a prescription drug or device prescribed by a physician.[194] (Of course, if a health system employs a prescribing physician, the health system might be held vicariously liable for the physician's actions.)

However, an evaluation of potential negligence liability is more complicated when a health system participates in a pharmacovigilance program that is designed to generate information about drug safety. To analyze this issue, we look to case law in which courts have imposed a duty to warn on individuals or entities that do not have a physician-patient relationship with the individual. Courts have found a duty under negligence claims where a defendant assumed an undertaking on which a plaintiff reasonably relied. Such a duty has been imposed, for example, in circumstances where a physician undertook a medical examination of the plaintiff for employment purposes, even where no doctor-patient relationship existed.[195] Courts likewise have imposed a duty on pharmacists to warn of the dangers of prescription

---

strict liability because the provision of medical services is qualitatively different from the sale of products). *See also Murphy v. E.R. Squibb & Sons,* 40 Cal. 3d 672, 221 Cal. Rptr. 447, 710 P.2d 247 (1985) (a pharmacy may not be held strictly liable for dispensing a prescription drug); *In re New York County Diet Drug Litigation,* 262 A.D.2d 132, 691 N.Y.S.2d 501 (1999) (where no allegation pharmacist failed to fill prescriptions as directed, no basis to hold pharmacist liable under theories of negligence, breach of warranty or strict liability); *Kohl v. American Home Products Corp.*, 78 F. Supp. 2d 885 (W.D. Ark. 1999) (holding pharmacists immune from strict liability); *Elsroth v. Johnson & Johnson,* 700 F. Supp. 151 (S.D.N.Y. 1988); *Jones v. Irvin,* 602 F. Supp. 399 (S.D. Ill. 1985); *Murphy v. E.R. Squibb & Sons, Inc.*, 710 P.2d 247 (Cal. 1985); *Leesley v. West,* 518 N.E. 2d 758 (Ill. App. 1988); *Parker v. St. Vincent Hosp.,* 919 P.2d 1104 (N.M. App. 1996) (hospital is analogous to prescription drug retailer and is therefore not strictly liable).

[193] The discussion herein is limited to potential negligence claims arising from an alleged failure to warn of the potential risks of prescription drugs. Negligence claims arising against a hospital or health system based on other alleged breaches of duty are outside the scope of this paper.

[194] *See, e.g., Kirk v. Michael Reese Hosp. and Medical Center,* 117 Ill.2d 507, 513 N.E.2d 387 (1987) (public policy and social requirements do not require that a duty be placed upon the hospital to warn the patient of the dangers of using the drug, prescribed by his physician, that would be extended to third-party non-patients); *Roell v. Stryker Corp.*, 2007 WL 2783357 (S.D. Miss. 2007) (hospital had no duty to warn patient of the duties of the dangers of a hip implant; because under the learned intermediary doctrine, the duty to warn flows from the manufacturer to the physician); *Johnson v. Parke-Davis,* 114 F. Supp. 2d 522 (S.D. Miss. 2000) (pharmaceutical sales representative did not owe duty to warn prescription drug users); *Schaerrer v. Stewart's Plaza Pharmacy, Inc.*, 79 P.3d 922 (Utah 2003) (so long as a pharmacist's ability to distribute prescription drugs is limited by the highly restricted FDA-regulated drug distribution system, and a pharmacist cannot supply a patient with prescription drugs without an intervening physician's prescription, duty will not be imposed on a pharmacist to warn of the risks associated with the use of prescription drugs). *But see Griffith v. Blatt,* 334 Or. 456, 51 P.3d 1256 (2002) (no learned intermediary rule protection for a pharmacist in connection with a "failure to warn" claim).

[195] *See, e.g., Stanley v. McCarver,* 208 Ariz. 219, 92 P.3d 849 (2004) (radiologist performing x-ray for pre-employment physical owed reasonable duty of care to patient); *Daly v. United States,* 946 F.2d 1467 (9th

drugs where a pharmacist had specific knowledge of an increased danger to a particular customer or where the pharmacist voluntarily assumed a duty to warn customers of drug side effects.[196] The imposition of a duty of care under these circumstances is supported by the Restatement (Second) of Torts:

> § 323. Negligent Performance of Undertaking to Render Services.
> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of the other's person or things, is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking, if (a) his failure to exercise such care increases the risk of such harm, or (b) the harm is suffered because of the other's reliance upon the undertaking.
>
> § 324A. Liability to Third Person for Negligent Performance of Undertaking
> One who undertakes, gratuitously or for consideration, to render services to another which he should recognize as necessary for the protection of a third person or his things, is subject to liability to the third person for physical harm resulting from his failure to exercise reasonable care to protect his undertaking, if (a) his failure to exercise reasonable care increases the risk of such harm, or (b) he has undertaken to perform a duty owed by the other to the third person, or (c) the harm is suffered because of reliance of the other or the third person upon the undertaking.

Under these legal theories, it is possible that a patient could argue that, by participating in the pharmacovigilance project a health system or HIE undertakes a service for the benefit of individuals to learn of adverse drug effects and therefore voluntarily assumes a duty to notify patients of any risks discovered during the course of the project. In the context of a health system, this argument would be bolstered by the pre-existing relationship between the health system and its patients. For an HIE, the lack of a treatment relationship with the consumer makes the imposition of a duty to warn more remote.

However, because liability does not attach unless there is a reasonable expectation by the patient that the health system or HIE would notify the patient of any discovered drug dangers, the risk of such a claim would be minimal if the health system or HIE does not publicize a plan to inform patients of adverse drug effects discovered in the program.[197] Further, the risk of such a claim can be further minimized by

---

Cir. 1991) (recognizing duty to report abnormal results obtained during a pre-employment physical exam despite absence of a physician-patient relationship); *Meinze v. Holmes*, 40 Ohio App. 3d 143, 532 N.E.2d 170 (1987) (containing dictum that insurer-retained doctors had a duty to communicate significant risk of danger to the plaintiff even in the absence of a doctor-patient relationship).

[196] *See, e.g. Horner v. Spalitto,* 1 S.W.3d 519 (Mo. Ct. App. 1999) (duty to warn when filling a prescription for what the pharmacist knew to be a lethal dose); *Lasley v. Shrake's Country Club Pharmacy, Inc.*, 179 Ariz. 583, 880 P.2d 1129 (App. 1994) (duty to warn when filling two prescriptions that adversely react with each other); *Hand v. Krakowski,* 89 A.D.2d 650, 453 N.Y.S.2d 121 (N.Y. 1982) (duty to warn of drug's adverse interaction with alcohol where the customer was known by the pharmacist to be an alcoholic); *Cottam v. CVS Pharmacy,* 436 Mass. 316, 764 N.E.2d 814 (2002) (pharmacy voluntarily assumed a duty to warn customer of all potential side effects of a prescribed drug where pharmacy provided patient with a list of possible side effects); *Baker v. Arbor Drugs, Inc.*, 215 Mich. App. 198, 544 N.W.2d 727 (1996) (pharmacy voluntarily assumed a duty of care when it advertised that it would monitor customer's medications and detect potential harmful drug interactions); *Sanderson v. Eckerd Corp.*, 780 So.2d 930 (Fla. Dist. Ct. App. 2001) (pharmacy advertising may constitute voluntary assumption of duty to warn of adverse drug reactions).

[197] *See Cottam, supra* (scope of duty depends on patient's reasonable understanding of what the pharmacy has undertaken to provide).

including information in any publicity related to the program that: (1) the purpose of the project is to gather raw data to be analyzed by the drug manufacturers; and (2) any adverse drug reactions will be reported to the FDA in accordance with regulatory requirements and not directly to patients or their physicians. It then would be difficult for patients to establish a reasonable expectation that warnings would be furnished directly to them by the health system or HIE. Finally, an argument against imposing patient warning requirements is further supported by the public policy interests in deferring to the expertise of drug manufacturers and the FDA and to limit any interference with the doctor-patient relationship.[198] Any contracts relating to a pharmacovigilance project should specify that there is no duty on the part of the health system or HIE to provide direct patient warnings.[199]

VII. Conclusion

The legal issues for HIEs, health systems and pharmaceutical companies engaging in pharmacovigilance programs are quite complicated, but we believe the legal risk is not high as long as the program is carefully constructed. The program must include a rigorous plan to protect the privacy and security of the health information evaluated and must minimize the use of individually identifiable health information to the extent possible. Moreover, the pharmaceutical company participants must follow FDA reporting obligations and communicate significant new findings of risk to health care providers. Of course, these issues have yet not been examined by courts in the context of pharmacovigilance programs, so we urge HIEs, health systems and pharmaceutical companies participating in pharmacovigilance programs to track the progress of issues noted in this guidance and closely evaluate the applicable laws in their jurisdictions.

[198] *See generally, Carlin v. Superior Court*, 13 Cal. 4th 1104, 56 Cal. Rptr. 2d 162, 920 P.2d 1347 (1996) (noting public policy in favor of FDA regulation of prescription drug warnings).
[199] *See Stanley, supra* (duty tied to scope of contractual undertaking).