BNA's

HEALTH CARE POLICY

BNA Employee-Owned Since 1947

VOL. 16, NO. 2 REPORT JANUARY 14, 2008

Health Information Privacy, Patient Safety, and Health Care Quality: Issues and Challenges in the Context of Treatment for Mental Health and Substance Use

BY J. ZOE BECKERMAN, JD, MPH[1], JOY PRITTS, JD[2], ERIC GOPLERUD, PHD[3], JACQUELINE C. LEIFER, JD[4], PHYLLIS C. BORZI, JD, MA[5], AND SARA ROSENBAUM, JD[6]

This article was written as part of a project funded by the California HealthCare Foundation. The authors gratefully acknowledge the thoughtful comments of our reviewers during this process.

[1] *Associate, Feldesman Tucker Leifer Fidell LLP, Washington, D.C.*

[2] *Research Associate Professor, Health Policy Institute, Georgetown University, Washington, D.C.*

[3] *Research Professor, Department of Health Policy, The George Washington University School of Public Health and Health Services, Washington, D.C.*

[4] *Senior Partner, Feldesman Tucker Leifer Fidell LLP, Washington, D.C.*

[5] *Research Professor, Department of Health Policy, The George Washington University School of Public Health Services, Washington, D.C.*

[6] *Hirsh Professor, Health Law and Policy, Chair, Department of Health Policy, The George Washington University School of Public Health and Health Services, Washington, D.C.*

Introduction

In an era of heightened concern over health care quality and patient safety on the one hand, and health information privacy on the other, finding the right balance between these two broad goals can represent a major policy challenge. No health issues better illustrate this challenge than the debate over use and disclosure of individualized information regarding mental health conditions and substance use disorders.

From one perspective, knowledge about a patient's history of mental health or substance use condition and treatment is vital to proper and safe treatment. Sharing information on diagnosis, treatment, and care plans can help promote a more comprehensive picture of a patient's needs and reduce the risks of error by treating providers.

From another perspective, however, disclosing or sharing vital patient-identifiable data, even when for entirely appropriate reasons, carries significant risks as well. These risks, however, are related to the impact on the patient caused by the potential for misuse of information, as well as the inappropriate re-disclosure of confidential information. In the case of mental health conditions and substance use disorders, these risks may include stigma, job loss, loss of occupational licensing, the imposition of health, disability or life insurance coverage barriers, and even criminal prosecution.

This article explores the law of health information privacy as it relates to mental health and substance use treatment, focusing on privacy and information-sharing in a treatment context. Although there are a considerable number of issues that arise when the purpose of information-sharing is to protect public health or public safety, discussion of these issues is beyond the scope of this article.

 ISSN 1068-1213

Even within the realm of treatment, however, the longstanding legal challenge of finding the correct balance between privacy and disclosure has grown more complex, as information technology advances have begun to alter the practice landscape by enabling a far greater level of rapid information exchange regarding health conditions, treatments, and risks. Whether and how technology-enabled treatment should affect this current legal landscape is our focus here.

Following an overview of the social and legal traditions underlying health information privacy, this article examines the federal and state legal framework for information privacy relating to treatment for mental health conditions and substance use.

The article then homes in on the distinction between the general consent to treatment-related information-sharing standard that exists under the Health Insurance Portability and Accountability Act (''HIPAA'') Privacy Rule and the specific consent standard that applies under federal laws governing substance use treatment information, as well as the numerous state laws that similarly apply specific consent standards to mental illness treatment information. The article identifies some health care scenarios that help illustrate how this tension between general and specific consent plays out in real-world situations.

Finally, the article concludes with recommendations for reconciling HIPAA's general consent standard with the specific consent standard governing mental illness and substance use treatment.

The Social and Legal Tradition of Protecting Health Information

Privacy is, according to Justice Brandeis, ''the right to be left alone.''[7] It is a critical part of the core belief structure of Americans, and it is at the root of how we operate as individuals within society.[8] Americans' concern for privacy protection dates back to the founding of our country, and privacy is a tenet of the common law, the very bedrock of the American legal system. Indeed, the Fourth Amendment to the U.S. Constitution guarantees ''the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures. . .''[9] The preamble to the federal privacy rule promulgated pursuant to the Health Insurance Portability and Accountability Act (The ''HIPAA Privacy Rule'' or ''Privacy Rule'') recognizes this core Constitutional right:

> By referring to the need for security of ''persons'' as well as ''papers and effects'' the Fourth Amendment suggests enduring values in American law that relate to privacy. The need for security of ''persons'' is consistent with obtaining patient consent before performing invasive medical procedures. The need for security in ''papers and effects'' underscores the importance of protecting information about the person, contained in sources such as personal diaries, medical records, or elsewhere.[10]

In sum, privacy matters deeply in American society and law, and no aspect of privacy is more important than the privacy of health information. In a recent national survey by the California HealthCare Foundation, 67 percent of consumers ages 18 and over expressed being ''somewhat'' or ''very'' concerned about the privacy of their personal medical records.[11] The statistics were somewhat higher for persons who were members of racial and ethnic minority groups (73 percent) and comparable for persons with chronic illness (67 percent).

Within the realm of privacy concerns, there has been a longstanding debate over whether certain types of health information records deserve greater legal protection than others.[12] In the case of information related to sensitive topics, such as mental health conditions or family genetic traits, unauthorized disclosures can create enormous harms, including social stigma, employment discrimination, insurance discrimination, and other types of injuries. Accordingly, changing laws to allow data to move more readily in the health care system may elevate the likelihood that people will not seek care, especially preventive care.

Information related to an individual's history of, or treatment for, the use of alcohol and illegal or other addictive substances presents its own particular set of issues. Perhaps the most notable issue affecting patient safety and health care quality is that fear of unauthorized disclosures can create disincentives for an individual to seek necessary treatment because of serious concerns about possible criminal prosecution and employment-related discrimination if health plan claims information is obtained by the employer.[13] Current and untreated substance use can also, in certain cases, result in the forfeiture of some legal protections, such as protection under the Americans with Disabilities Act or the right to receive disability benefits. Thus

---

[7] *Olmstead v. U.S.*, 277 U.S. 438, 478 (1928); *see also* Warren, S., and Brandeis, L. ''The Right to Privacy,'' *Harvard Law Review*, Vol. IV, No. 5, (Dec. 15, 1890).

[8] Consider, for example, growing concerns about identity fraud and the ease with which strangers can access another's personal data, either from on-line sources or from the age-old method of sifting through discarded personal effects. *See e.g.*, a 2006 survey conducted for the Markle Foundation that demonstrated that 80 percent of respondents were concerned about identity theft, available at http://www.markle.org/downloadable_assets/research_doc_120706.pdf, accessed on 6/6/07; *see also* the cases and examples listed on the Privacy Rights Clearinghouse hotline, available at http://www.privacyrights.org/cases/victim.htm, accessed on 6/6/07.

[9] U.S. Const. amend. IV.

[10] Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000); *see also* Standards for Privacy of Individually Identifiable Health Information, Proposed Rule, 64 Fed. Reg. 59,918, 60,008 (Nov. 3, 1999).

[11] California HealthCare Foundation, National Consumer Health Privacy Survey 2005 (available at http://www.chcf.org/topics/view.cfm?itemID=115694; accessed on 6/6/07).

[12] *See e.g.*, Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462, 82,471 (Dec. 28, 2000) in which the preamble discusses the need for balance between and among various stakeholders.

[13] As the Drug Abuse Office and Treatment Act indicates, Congress passed legislation requiring the confidentiality of information related to substance and alcohol abuse treatment in order to encourage people to seek treatment without fear of prosecution. *See* H.R. Conf. Rep. No. 92-775, at 28 (1972), reprinted in 1972 U.S.C.C.A.N. 2045, 2072 (explaining the confidentiality provisions in the predecessor to Section 290dd-2 were necessary because ''[w]ithout that assurance, fear of public disclosure of drug abuse or of records that will attach for life will discourage thousands from seeking the treatment they must have if this tragic national problem is to be overcome.'').

   ISSN 1068-1213

individuals avoid obtaining necessary care because they are terrified that there are not sufficient legal protections or practical steps that can be taken to assure that unauthorized disclosure, even if illegal, can be sufficiently remedied.

In response to this heightened concern over the consequences flowing from the unauthorized disclosure of highly sensitive information, some interest groups and individuals argue that some types of sensitive information should receive more stringent legal protections at the front end, since appropriate remedies at the back end after the illegal disclosure has been made are hard to fashion because the societal harm to the individual or the individual's reputation has already occurred and cannot be erased.[14]

Accordingly, many state and some federal laws do afford a higher degree of protection for these specialized categories of personal health information than is generally accorded to other types of personal health information.[15] In general, these laws require the individual's written consent, or permission, prior to any disclosure of certain sensitive information. Of course, laws requiring prior written permission for disclosure still raise numerous additional legal and practical issues, such as the degree of specificity with which such written permission must be drafted, the type and quality of information that should be used in obtaining a patient's consent to treatment and to the disclosure of health information to other treating providers, how long a patient's written permission should be considered effective before it must be re-executed, and whether electronic signatures, or ''e-signatures,'' will suffice. Not surprisingly, existing laws vary on some of these points.

Federal Privacy Law and the Special Status Accorded Mental Health and Substance Use Information

1. The Health Insurance Portability and Accountability Act and the Privacy Rule

Against this existing legal framework, the HIPAA was enacted. The statute and its Privacy Rule coincided with—and indeed were bound up in—the advent of the era of health information technology (HIT) growth, which many observers consider to be a potentially transformational event in health care practice and quality.[16] The potential of HIT has been evident for a considerable length of time. In recent years the Bush Administration has made adoption of health information technology and national conversion from a paper medical records system to an electronic medical records system a national health policy priority through Executive Orders and legal reforms aimed at spurring adoption (such as incentivizing adoption through physician compensation).[17] The Administration's focus on information technology reflects its often stated belief that technology has the potential to improve quality and patient safety while lowering costs. This belief has been given added support by reports by the Institute of Medicine on health care quality, which also advocated the use of increased health information technology as a matter of patient safety.[18]

HIPAA was intended to establish a legal framework for individually identifiable health information that reconciles the need for broad information exchange with the need for individual privacy. Provider custom, practice and discretion over many types of disclosures, bolstered by key safeguards, lie at the heart of the HIPAA regulatory framework. HIPAA creates a federal ''floor'' of privacy protections[19] while preserving ''more stringent'' state laws.[20] Additionally, HIPAA does not displace other federal laws, so separate and more protective federal privacy standards must be considered in tandem with HIPAA. It is clear that the potential for conflicts to arise between HIPAA's standard for recon-

[14] *See e.g.*, Testimony of Kathleen Zeitz, Nebraska Lead Coordinator, National Breast Cancer Coalition, before the Senate Health, Education, Labor, and Pensions Committee (July 21, 2001) regarding the need for specific federal legislation barring misuse of genetic information. Available at http://www.natlbcc.org/bin/index.asp?strid=475&depid=3, accessed on 6/7/07. In fact, legislation specifically aimed at prohibiting employers and health insurers from discriminating based on genetic information has been introduced during the last few sessions of Congress. *See e.g.*, Genetic Information Nondiscrimination Act, H.R. 493, 110th Cong. (2007) and Genetic Information Nondiscrimination Act, S. 306, 109th Cong. (2006).

[15] For information on specific state law protections, *see* Pritts, J., et al., *The State of Health Privacy,* published by the Georgetown University Health Policy Institute, http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm, http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf, and http://ihcrp.georgetown.edu/privacy/pdfs/statereport2.pdf, accessed on 6/1/07.

[16] Blumenthal, David, and Glaser, John, Information Technology Comes to Medicine, *NEJM* 356:24 2527-2534 (June 14, 2007) 2527.

[17] *See* http://www.whitehouse.gov.news.releases/2004/04/20040427-4.html (accessed on 7/3/04). *See also* The Federal Physician Self-Referral Law (the Stark Law), 42 U.S.C. § 1395nn and regulations, 69 Fed. Reg. 10,053 (March 26, 2004). *See also* http://www.hhs.gov/news/press/2007pres/10/pr20071030a.html (accessed on 11/3/07) relating to a Medicare demonstration effort to reward physicians for the use of electronic health records.

[18] *See* Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, Chapter 7 ''Using Information Technology'' (2001) and Institute of Medicine, *Improving the Quality of Health Care for Mental Health and Substance Use Conditions,* Quality Chasm Series, Chapters 5 & 6 (2005).

[19] Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 (Dec. 28, 2000) as amended.

[20] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, Sec. 264(c)(2) (Aug. 21, 1996). ''More stringent'' was not defined in the Act, but in the implementing regulations ''more stringent'' is defined as ''in the context of a comparison of a provision of State law and a standard [from the HIPAA regulations], a State law that meets one or more of the following criteria: (1) with respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted [under the HIPAA regulations], except if the disclosure is [required by the Secretary of HHS to determine compliance with the HIPAA regulations] or to the individual who is the subject of the individually identifiable health information;. . . (4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individually identifiable health information, for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded. . ., or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.'' 45 C.F.R. § 160.202.

ciliation of the tension between the need to further transparency and privacy objectives and the goals of other more protective privacy standards was recognized early in the policy process.[21]

The Privacy Rule applies to ''covered health care entities,'' which consist of health plans, health care clearinghouses, or health care providers who transmit any health information in electronic form for certain administrative purposes.[22] The Privacy Rule affords protections to individually identifiable health information held by those entities, called ''protected health information'' or ''PHI.'' With very limited exceptions, the Privacy Rule does not distinguish between types of data that are PHI.[23] As noted above, the Rule does, however, recognize that some existing federal and state privacy and confidentiality laws accord greater protection for certain types of health information and leaves these laws undisturbed.

In general, the Privacy Rule permits a covered entity to use and disclose protected health information for certain core purposes, including treatment, payment and health care operations, without an individual's written permission. However, the Rule also recognizes professional tradition and ethical obligation by *permitting* covered entities to obtain written permission to use and disclose health information for these core purposes (this type of permission is called ''consent'' under the Rule[24]) as part of their privacy policies. In so doing, the Privacy Rule establishes a ''general consent'' standard where disclosure for patient treatment is concerned. In other words, a treating health professional can share patient information with another treating professional or provider without getting specific written consent. In addition, the Rule eschews specific format or content requirements for consent when it is utilized.

For most purposes, including payment and health care operations, the Rule uses a ''minimum necessary'' standard to measure disclosure of protected information. This limits covered entities' uses, disclosures, and requests from other covered entities of protected health information to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.[25] However, the ''minimum necessary'' rule does not apply to requests for or disclosures of protected health information for treatment purposes.[26] In other words, HIPAA allows that for treatment purposes, providers can share any PHI in the patient's medical record.

No written authorization is needed when protected health information is being provided to the individual who is the subject of the information.[27] In fact, disclosure to the individual himself or herself is one of only two *required* disclosures (the other one is to the Secretary for purposes of auditing the covered entity for compliance). Similarly, if the individual is present and has an opportunity to either agree or object in the case of disclosures to family members or others involved in the care of the individual, no written authorization is needed.[28]

Moreover, the HIPAA privacy rule allows covered entities substantial flexibility to maintain their own framework for use or disclosure of PHI by establishing a series of categories for *permissive* disclosures. This structure facilitates the ability of health care professionals to continue many of their existing privacy practices, thus allowing them to develop their own approach to health information privacy in key care areas as long as their policies and practices are explained in writing to their patients in advance. Covered entities may also, if they elect to do so, use and disclose protected health information without an individual's written permission for certain other national priority purposes.

A few of these permissive disclosure categories are worth mentioning briefly here. For instance, covered entities may use and disclose protected health information without an individual's written permission for a variety of national priority purposes including health care oversight, public health, research, law enforcement, and when disclosure is required by other law.[29]

Outside of treatment, payment, and health care operations, or the permissive exceptions noted above, the Rule requires that entities obtain written permission (called ''authorization'') from patients prior to the use or disclosure of PHI.[30] These authorizations must meet specific content and format requirements. In addition, psychotherapy notes are covered by a special authorization rule,[31] even though such notes arguably relate to

---

[21] Confidentiality of Individually-Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996, submitted to the Senate's Committee on Labor and Human Resources and the Committee on Finance, and the House of Representatives' Committee on Commerce and the Committee on Ways and Means, Section J, (Sept. 11, 1997), available at: http://www.epic.org/privacy/medical/hhs_recommendations_1997.html, accessed on 5/22/07.

[22] § § 45 C.F.R. 160.102(a), 164.500.

[23] Standards for Privacy of Individually Identifiable Health Information at 82,621, in which the preamble discusses the choice not to single out various types of protected health information in the text. The Privacy Rule does afford a higher degree of protection for psychotherapy notes (*see* note 31) generally requiring the individual's written authorization to disclose these notes for most purposes. *See* 45 C.F.R. § 164.501.

[24] When a covered entity opts to obtain the patient's permission to use or disclose PHI for the core functions of treatment, payment, or health care operations, this permission is called ''consent.'' This is in contrast to the process for obtaining the patient's permission to disclose PHI to a third party for other purposes—this type of permission is called ''authorization'' and the conditions under which an authorization is valid under the Rule are described in 45 C.F.R. § 164.508(c) and discussed later in the article.

[25] 45 C.F.R. §§ 164.502(b), 164.508.

[26] The Privacy Rule does however impose the minimum necessary requirement on *internal* uses of protected health information, generally requiring a covered entity to identify the individuals within their organization who need access to such information to perform their duties and to limit their access to the type and amount of information needed. *See* 45 C.F.R. § 164.514(d)(2).

[27] 45 C.F.R. § 164.502(a)(2)(i).

[28] 45 C.F.R. § 164.510, this also includes facility directories, for notification purposes, in limited situations when the individual is not present, and for disaster relief purposes.

[29] *See* 45 C.F.R. § 164.512.

[30] Interested readers can obtain from the authors a comprehensive chart summarizing HIPAA's rules regarding mandatory and permissive disclosures, when authorizations are necessary, and what penalties attach for unauthorized disclosures.

[31] ''Psychotherapy notes'' are ''notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the

   ISSN 1068-1213

treatment, payment, and health care operations, and should therefore be covered by the general consent and disclosure rule. This is the single instance in which HIPAA accords information greater protection than other forms of PHI in deference to longstanding legal and policy concerns and professional custom.

Under HIPAA, authorizations must be written in plain language and contain:

- a specific and meaningful description of the information to be disclosed or used;
- the name or specific identification of the person(s) authorized to disclose the information;
- the name or specific identification of the person(s) to whom the information can be disclosed;
- a description of each purpose of the requested use or disclosure;
- expiration date or event;
- the signature of the individual and date; and
- a few required statements to place the individual on notice of his/her rights, including the right to revoke consent.[32]

In the case of routine disclosures of protected health information to a third party who performs business functions for a covered entity, a covered entity must enter into an agreement with the ''business associate.''[33] Such agreements must include assurances that the business associate will appropriately safeguard protected health information.[34]

HIPAA establishes a regulatory framework, enforced through the U.S. Department of Health and Human Service's Office for Civil Rights (''OCR''), which has the power to ensure compliance, investigate reported violations, and impose civil monetary penalties of not more than $100 per violation, which may not exceed $25,000 per year.[35] Since 2003, approximately 32,000 complaints have been filed with HHS OCR; of these about 8,000 were investigated, and about 5,400 (or 67 percent) of those investigated achieved corrective action.[36] No civil fines have been assessed to date.

HIPAA does not create a federal private right of action that would permit private persons to sue covered entities to halt disclosures or to recover damages for injuries arising from disclosures. Yet, HIPAA is viewed by experts as establishing a standard against which health professionals' conduct might be measured in considering liability under other federal and state laws that do permit private enforcement actions.

In sum, HIPAA creates a general consent protocol in the context of treatment, payment, and health care operations. Providers can use a specific consent standard at their option. The Privacy Rule also sets forth disclosure procedures and standards governing other circumstances. At the same time, the Rule leaves undisturbed more stringent state laws, as well as other federal laws that may accord greater deference to personal health information privacy. Finally, the Rule's own terms reflect the special status of mental health treatment and include separate specific authorization provisions governing the disclosure of psychotherapy notes.

Thus, HIPAA is widely viewed as establishing a national code of general conduct for covered health professionals where personal health information is concerned. HIPAA leaves much discretion to health professionals themselves in fashioning this code of conduct, while at the same time, holding them accountable for certain disclosures that require patient authorization.

HIPAA's Relationship to State Law

The Privacy Rule essentially establishes a ''roadmap'' for reconciling the diversity between HIPAA's legal standard and state law,[37] which can be summarized as follows:

First, HIPAA generally preempts state laws that are ''contrary to'' it.[38] A state law is contrary to the HIPAA Privacy Rule when it would be impossible to comply with both the state and federal requirements or when the provisions of the state law would be an obstacle to the accomplishment and execution of the HIPAA Privacy Rule.[39] Because HIPAA expressly permits covered entities to make disclosures ''as required'' by other laws,[40] state laws that require disclosures (even when HIPAA would make them optional) are not in conflict with the federal law. Thus, under HIPAA, covered entities are permitted to comply with state mandatory disclosure laws that otherwise would appear to be preempted by federal privacy standards.

Second, HIPAA also specifies that its standards do not supersede a contrary provision of state law, if the provision of state law imposes requirements, standards, or implementation specifications that are ''more strin-

individual's medical record. The term ''psychotherapy notes'' excludes data relating to medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.'' 45 C.F.R. § 164.501. According to the Legal Action Center, there has been no definitive opinion from the Department of Health and Human Services as to whether psychotherapy notes include drug and alcohol counseling notes, or what it means to keep a record separate from the rest of the record. *See* Legal Action Center, *Confidentiality and Communication: A Guide to the Federal Drug and Alcohol Confidentiality Law and HIPAA*, Sixth Edition, at 84 (2006).

[32] *See* 45 C.F.R § 164.508(c).

[33] A business associate is a person or organization who, on behalf of the covered entity, but ''other than in the capacity of a member of the workforce of such covered entity or arrangement'' performs ''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 ''legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity.'' 45 C.F.R. § 160.103.

[34] 45 C.F.R.§ 164.502(e).

[35] 42 U.S.C. § 1320d-5. Penalties are more severe for wrongful disclosure, including fines of not more than $50,000, imprisonment, or both.

[36] http://www.hhs.gov/ocr/privacy/enforcement/numbersglance.html, accessed on 12/20/07.

[37] *See* Rosenbaum, S., Borzi, P., Burke, T., and Nath, S., ''Does HIPAA Preemption Pose a Legal Barrier to Health Information Transparency and Interoperability?'' in Bureau of National Affairs' Health Care Policy Report, Vol. 15, No. 11 (March 19, 2007).

[38] A law that is ''preempted'' by another means that it is superseded.

[39] *See* 45 C.F.R. § 160.202.

[40] *See* 45 C.F.R. 164.512(a).

gent than'' HIPAA's own standards.[41] As previously noted, HIPAA sets a ''floor'' for conduct where privacy is concerned. State laws that accord greater privacy protections—those that either provide individuals greater access to their own records or contain more restrictive use and disclosure requirements—are considered ''more stringent than'' HIPAA.

Third, HIPAA does not preempt state laws that provide for the reporting of various types of information, including but not limited to, disease, injury, child abuse, public health surveillance, investigation, or intervention, because disclosure of this type of information, even if it is PHI, is permitted by HIPAA.[42]

Fourth, HIPAA does not interfere with provisions of State law that require a health plan to report or to provide access to, information for management or financial audits and certain other limited purposes.[43]

A recent review of nearly 500 judicial opinions interpreting the HIPAA privacy rule shows the great range of questions that can arise under this roadmap outlining the relationship between HIPAA and state laws.[44] The

[41] P.L. 104-191 § 264(c)(2).
[42] *See* 42 U.S.C. § 1130d-7(b); 45 C.F.R. § 160.203(c).
[43] *See* 42 U.S.C. § 1130d-7(c); 45 C.F.R. § 160.203(d).
[44] *See* note 37, *supra*.

   ISSN 1068-1213

cases considered illustrate the extent to which provider discretion guides the question of whether to comply with certain state disclosure laws. Some of the cases focus on the disclosure of patient health information related to mental illness and substance use, although none of the cases relate to provider-to-provider exchange of health information for treatment reasons.

2. Special Federal Privacy Laws Applicable to Substance Use Treatment and Mental Health

In addition to HIPAA, several federal laws pertain directly to the disclosure of mental illness and substance use information. These laws are set forth in Figure 1 and are discussed in greater detail below.

Figure 1: Comparison of Key Federal Laws' Consent Requirements for Disclosures of Individually Identifiable Information

Name of Privacy Law or Regulation	*HIPAA Privacy Rule*	*42 C.F.R. Part 2 (Alcohol and Drug Use Provisions of the Federal Confidentiality of Alcohol and Drug Abuse Patient Records law)*	*FERPA*	*Medicaid*
Type of Patient Authorization or Consent Required for Use or Disclosure for Treatment, Payment or Health Care Operations Purposes	*No consent needed for treatment, payment, or health care operations purposes*	*Specific consent needed for disclosures, (including for treatment, payment, health care operations purposes)*	*Specific consent needed for disclosures of educational records for medical purposes*	*Unclear (no specific federal ruling or official interpretation in wake of HIPAA; appears to be widely understood as relying on a more traditional approach of requiring specific consent to disclose rather than using the general consent standard found in HIPAA)*

a. Federal Confidentiality of Alcohol and Drug Abuse Patient Records

Since the early 1970s, patient records for alcohol and drug use treatment have been entitled to special provider/patient confidentiality protections as a matter of federal law.[45] These laws have important implications for the electronic exchange of health information data. The Federal Confidentiality of Alcohol and Drug Abuse Patient Records law, reflecting Congressional concern about the stigmatizing and legal implications of seeking alcohol and drug treatment,[46] creates a virtual shield against the disclosure of personal health information related to alcohol and substance-related conditions and treatment. Its implementing regulations[47] have become such a staple of the legal landscape that they are known simply as ''Part 2'' of the broader body of federal substance use regulations of which they are a part.[48]

With certain conditions and exceptions, Part 2 strictly prohibits the disclosure and use of drug and alcohol use records maintained in connection with the performance of any federally assisted alcohol and drug use program.[49] Disclosure in this instance means ''a communi-

[45] The Drug Abuse Prevention, Treatment, and Rehabilitation Act (21 U.S.C. 1175), was transferred to section 527 of the Public Health Service Act, codified at 42 U.S.C. 290ee-3 and then later transferred to § 290dd-2. The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 (42 U.S.C. 4582) was amended and transferred to section 523 of the Public Health Service Act, codified at 42 U.S.C. 290dd-3 and eventually omitted, presumably because confidentiality for alcohol treatment was eventually bundled with confidentiality for substance use treatment.

[46] Kamoie, B., and Borzi, P. ''A Crosswalk Between the Final HIPAA Privacy Rule and Existing Federal Substance Abuse Confidentiality Requirements,'' Double Issue Brief #18-19, Center for Health Services Research and Policy, The George Washington University School of Public Health and Health Services (2001) at 17.

[47] 42 C.F.R. Part 2. The original statutes are still included as full text in the beginning of 42 C.F.R. Part 2, at §§ 2.1 and 2.2.

[48] The regulations for Part 2 were originally proposed in 1974 as an Advance Notice of Proposed Rulemaking (39 Fed. Reg. 30,426 (Aug. 22, 1974); proposed jointly by the Department of Health Education, and Welfare and the Special Action Office for Drug Abuse Prevention in 1975 (40 Fed. Reg. 20,521 (May 9, 1975); promulgated in final form later that same year (40 Fed. Reg. 27,801 (July 1, 1975). They were substantively updated during the 1980s (45 Fed. Reg. 53 (Jan. 2, 1980), 48 Fed. Reg. 38,758 (Aug. 25, 1983), and 52 Fed. Reg. 21,796 (June 9, 1987)) and clarified slightly in the mid-1990s (59 Fed. Reg. 42,561 (Aug. 18, 1994), 59 Fed. Reg. 45,063 (Aug. 31, 1994), 60 Fed. Reg. 22,296 (May 5, 1995)).

[49] 42 C.F.R. § 2.3(a). Note that federal assistance is defined very broadly, and includes being (1) conducted in whole or in part by any U.S. department or agency; (2) licensed, certified, registered or otherwise authorized by any U.S. department or agency (including being certified with provider status under the Medicare program or being authorized to conduct methadone maintenance treatment or being registered to dispense controlled substances; (3) supported by funds provided by any U.S. department or agency, including as a recipient of federal financial assistance in any form (not limited to the provision of substance abuse or alcohol treatment), conducted by a state or local government that receives federal funds that could be used for alcohol or drug abuse treatment, or is assisted by the IRS through the allowance of contributions as tax deductions

cation of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the record of a patient who has been identified.''[50] Patient-identifying information includes many types of information, such as names, addresses, Social Security numbers, fingerprints, photographs, or ''similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information.''[51] Criminal penalties for violations include a fine of not more than $500 for first offenses and not more than $5,000 for each subsequent offense.[52]

Part 2 sweeps broadly in defining both patients and programs, as described below. Its provisions are stringent, prohibiting disclosure of any information[53] that could either directly or indirectly identify an individual as an alcohol or substance use patient.[54]

Part 2 applies to programs, which are defined as:

- individuals or entities (other than general medical facilities), or identified units within general medical facilities that *hold themselves out as providing*, and actually *provide* alcohol or drug abuse diagnosis, treatment, or referral for treatment; or

- medical personnel or other staff in a general medical care facility whose *primary function* is the provision of alcohol or drug abuse diagnosis, treatment, or referral for treatment and who are *identified* as such providers.[55]

Part 2 also uses the term ''patient'' broadly to include ''any individual who has *applied for or been given a diagnosis or treatment* for alcohol or drug abuse *at a federally assisted program* and includes any individual who, after arrest on a criminal charge, is identified as an alcohol or drug abuser in order to determine eligibility to participate in a program.''[56]

Importantly, all permissible disclosures under Part 2 of drug and alcohol use records maintained in connection with the performance of any federally assisted alcohol and drug use program are limited to ''that information which is necessary to carry out the purpose of the disclosure.''[57] While Part 2 prohibits the use of covered information to form the basis of a criminal charge,[58] the law does require disclosure in response to a subpoena issued as part of an ongoing court procedure pursuant to an authorizing court order.[59]

Nearly all disclosures under Part 2 require specific patient consent,[60] and the content and format of consent must meet the federal standards described below. In contrast, the HIPAA Privacy Rule does not require any consent to disclose protected health information for treatment, payment, or health care operations purposes. If a provider elects to obtain such consent, s/he is permitted under HIPAA to use a general consent form. Thus, Part 2's ''specific consent'' format sets a far higher bar than HIPAA with respect to consent requirements.

The required elements of a Part 2 consent form are:

- the specific name or designation of the program or person permitted to make the disclosure;
- the name or title of the individual or the name of the organization to which the disclosure is made;
- the name of the patient;
- the purpose of the disclosure;
- how much and what kind of information is to be disclosed;
- the signature of the patient (or if a minor or incompetent or deceased, then the signature of a person authorized to give consent);
- the date the consent is signed;
- a statement that the consent is subject to revocation at any time except to the extent the discloser has acted in reliance;
- the date, event, or condition upon which the consent will expire, if not revoked before;[61] and
- a statement that the information being disclosed may not be re-disclosed without the individual's consent.[62]

Part 2's restrictions on disclosure of drug and alcohol use records maintained in connection with the performance of any federally assisted alcohol and drug use program allow certain exceptions, the most pertinent of which for our purposes are (1) communications within a program or between a program and an entity having direct administrative control over that program;[63] and

---

or the granting of tax-exempt status to the program. 42 C.F.R. § 2.12(b). There are special exceptions for information on alcohol and drug use patients maintained in connection with the Department of Veterans Affairs and other limits for information obtained by the Armed Forces. *See* 42 C.F.R. § 2.12(c).

[50] 42 C.F.R. § 2.11.

[51] *Id.*

[52] 42 C.F.R. §§ 2.3 (b)(3), 2.4.

[53] 42 C.F.R. § 2.12(d).

[54] *See* Kamoie and Borzi, *supra* note 46, at 17. *See also* 42 C.F.R. § 2.11 *et seq*.

[55] 42 C.F.R. § 2.11. For clarification, this means that a physician in a hospital emergency room who makes a drug use diagnosis occasionally would not be considered a ''program'' unless substance abuse diagnosis and treatment is his primary function and he is identified specifically as that type of provider.

[56] 42 C.F.R. § 2.11.

[57] 42 C.F.R. § 2.13(a).

[58] *Id.*

[59] 42 C.F.R. § 2.61. Nonetheless, before a court may issue such an order, it must give notice to the patient and the treatment program, follow fact-finding procedures, and limit the disclosure to necessary information. 42 C.F.R. § 2.64.

[60] Part 2 does not distinguish between ''consent'' and ''authorization,'' like HIPAA does. Accordingly, we use the term consent when discussing Part 2 to mirror its regulations. For a complete list of when covered entities can disclose protected health information, with or without authorization, please contact the authors for a chart which summarizes the allowable disclosures in significant detail and explains the purpose of each disclosure, whether or not it is mandatory or permissive, who is the protected party, who makes the disclosure, to whom the disclosure can be made, what types of consent are needed, and what penalties attach.

[61] 42 C.F.R. § 2.31.

[62] 42 C.F.R. § 2.32.

[63] This means that communications of information between or among personnel having a need for the information in connection with their duties arising out of the provision of diagnosis, treatment, or referral for treatment of alcohol or drug use do not fall under Part 2 if the communications are within a program or between a program and entity that has direct admin-

   ISSN 1068-1213

(2) communications between a program and a qualified service organization (''QSO'').[64] These exceptions allow programs covered by Part 2 some operational leeway with respect to health information exchange.

QSO arrangements are similar to business associate arrangements under HIPAA, but QSOs that furnish medical care are subject to Part 2 as health care providers. Thus, medical QSOs that are also covered entities under HIPAA are bound both by HIPAA (which contains certain unique safeguards such as granting individuals access to their own health records) and the more specific consent requirements of Part 2.[65]

Part 2 defines certain limited circumstances under which disclosures can be made without patient consent, including medical emergencies, research activities and audit or evaluation activities.[66] Re-disclosures (i.e., secondary disclosures stemming from an initial one) are prohibited unless made back to the program from which the information was obtained.[67]

As with HIPAA, Part 2 sets a federal privacy floor, preempting state laws that are less protective regarding disclosures of drug and alcohol use records, while saving state laws that would be interpreted as being more stringent.[68]

There have been few legal challenges involving the interpretation of Part 2, most likely because its prohibitions are both broad and relatively clear, and because the programs covered by Part 2 (*i.e.*, federally assisted substance use and alcohol treatment providers) have a strong tradition of non-disclosure. Part 2 has such traction that even the Joint Commission on Accreditation of Healthcare Organizations and most state licensing agencies have explicit requirements regarding substance use and alcohol treatment record confidentiality and facility compliance with Part 2.[69]

istrative control over the program. 42 C.F.R § 2.12(c)(3). In effect, programs can ''report up'' to entities with direct administrative control (*e.g.*, parts of an integrated system that oversee the alcohol or drug use treatment program).

[64] A qualified service organization is defined as a person—*i.e.*, an individual, partnership, corporation, federal, state or local government agency, or any other legal entity—that ''provides services to a program, such as data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting or other professional services, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy'' and ''has entered into a written agreement with a program.'' 42 C.F.R. § 2.11. The written agreement must include an acknowledgment that in receiving, storing, processing, or otherwise dealing with any patient records from the programs, the person is fully bound by Part 2 and if necessary will resist in judicial proceedings any efforts to obtain access to patient records except as provided for by Part 2. *Id.*

[65] *See* U.S. Department of Health and Human Services Substance Abuse and Mental Health Services Administration Center for Substance Abuse Treatment, ''*The Confidentiality of Alcohol and Drug Abuse Patient Records Regulation and the HIPAA Privacy Rule: Implications for Alcohol and Substance Abuse Programs*,'' at 2 (June 2004).

[66] *See* 42 C.F.R. Subpart D, ''Disclosures without Patient Consent.''

[67] *See* 42 C.F.R. § 2.52(b); *see also* 42 C.F.R. § 2.53(d).

[68] 42 C.F.R. § 2.20.

[69] Jade, R. ''The Secret Life of 42 CFR Part 2,'' 30-APR Champion 34 at FN 12 (2006).

b. The Family Education Rights and Privacy Act of 1974

Enacted in 1974, the Family Educational Rights and Privacy Act of 1974[70] (''FERPA'') protects the privacy of student education records and represents a ''response to what Congress saw as growing evidence of abuse of student records in the United States.''[71] FERPA serves two functions: (1) to create a right of access to student records for parents and students; and (2) to protect the privacy of those records by preventing unauthorized access by third parties.[72] FERPA has been substantively amended numerous times and its implementing regulations are comprehensive.[73]

FERPA prohibits the release of education records without parental consent, or, in the case of students age 18 or older or attending college, without the consent of the student.[74] FERPA applies to all public or private educational agencies, at the elementary, secondary, and higher education level that receive federal education funding.[75] The range of information considered protected records under FERPA is broad and can include information related to the treatment of a specific student for substance use or mental health conditions.

Under FERPA, any recorded information maintained by an educational agency or institution or by a party acting for the agency or institution constitutes a ''record'' under FERPA, with a few exceptions.[76] This means that treatment records can be records protected under FERPA. Under FERPA, student records are records, files, documents, and other materials which contain information directly related to a student and are maintained by an educational agency or institution or by a person acting for such agency or institution.[77] Records of both current and former students are covered.[78] For a record to be protected by FERPA, it must contain ''personally identifiable'' information about a student.[79]

Although FERPA protects health records if maintained by educational agencies, such as those kept by school-based clinics, it also permits certain disclosures

[70] 20 U.S.C. § 1232g.

[71] *Disability Rights Wis., Inc. v. Wis. Dep't. of Pub. Instruction*, 463 F. 3d 719, 730 (7th Cir. 2006).

[72] *Kestenbaum v. Michigan State University*, 294 N.W. 2d 228, 231 (1980); *see also* 120 Cong. Rec. 39,858, 39, 862-39863 (Dec. 13, 1974); 121 Cong. Rec. 7974 (May 13, 1975); *Rios v. Read*, 73 F.R.D. 589, 597 (E.D.N.Y. 1977). It should also be noted that FERPA was enacted as a floor amendment to other educational legislation, without intensive floor debate or other Congressional deliberations on its specific provisions. *See* Daggett, L., ''Bucking Up Buckley I: Making the Federal Student Records Statute Work,'' 46 Cath. U.L. Rev. 617 (1997).

[73] *See id.*; *see also* 34 C.F.R. Part 99.

[74] *See* 20 U.S.C. § 1232g(d).

[75] *See* 34 C.F.R. § 99.1.

[76] *See id.* These exceptions include ''sole possession'' notes, law enforcement notes, or those made by physicians, psychiatrists, psychologists, etc. in an institution of postsecondary education. This is significant for a few reasons. It means that for certain health records, including mental health records—albeit only those relating to students over age 18—parents cannot use FERPA to gain access to their children's records. Additionally, this exception to the definition of record also means that such health and mental health treatment records are left to other federal and state laws for protection.

[77] 20 U.S.C. § 1232g(a)(4)(A).

[78] *See* 34 C.F.R. § 99.3.

[79] *See id.*

regarding substance use and mental health conditions unless prohibited under more stringent and protective state law. FERPA also provides for a set of circumstances in which disclosures without consent are allowed.[80]

Accordingly, FERPA is similar in structure to HIPAA, requiring written consent for certain disclosures but allowing certain others to be made without consent. Specifically of interest to this analysis, parental or (where appropriate) student consent is required to release educational records involving medical treatment.

Finally, it should also be noted that records covered by FERPA are not subject to HIPAA because HIPAA's definition of protected health information specifically excludes FERPA records.[81] This means that unlike Part 2, HIPAA and FERPA do not overlap. Thus FERPA adds an extra layer to federal health information law and the policy protections regarding confidentiality of records.[82]

c. Medicaid Privacy Statute

The Medicaid privacy statute is a precursor to HIPAA—its provisions bear a striking resemblance to the basic HIPAA rule, yet HHS has never issued a formal interpretation that would align Medicaid privacy standards squarely with the HIPAA Privacy Rule. This lack of action by HHS has created a fair amount of confusion.

Federal Medicaid law requires state plans for medical assistance to provide safeguards that restrict use and disclosure of patient information to purposes directly connected with administration of the plan.[83] Implementing regulations[84] further define the purposes directly related to plan administration to include: establishing eligibility, determining the amount of medical assistance, providing services for recipients, and conducting or assisting investigations, prosecutions, or legal proceedings related to the administration of the plan.[85]

In addition, the regulations require agencies to establish criteria for safeguarding specific information about applicants and recipients, including at least names, addresses, medical services provided, social and economic conditions and circumstances, agency evaluations of personal information, medical data, including diagnosis and history of disease or disability, information received for verifying income eligibility and amount of medical assistance payments, and information received in connection with the identification of legally liable third party resources.[86]

The regulations also require agencies to have criteria specifying conditions for release and use of information about applicants and recipients.[87] Access to information concerning applicants or recipients must be restricted to individuals who are subject to standards of confidentiality that are comparable to those of the agency.[88] With certain exceptions, the regulations also require permission from a family or individual, wherever possible, before an agency can respond to an information request from an outside source.[89] Additionally, agencies must have data exchange agreements (similar to HIPAA business associate agreements) in order to exchange data with other agencies.[90]

Thus, as with HIPAA, the Medicaid statute outlines a basic floor of privacy and the use of formal protocols to guide data disclosures. Unlike HIPAA, Medicaid does not appear to address patient consent to disclosure in the context of treatment, payment, and health care operations as a general rule, but instead appears, like FERPA and Part 2, to rely on the more traditional approach of requiring specific patient consent for disclosures of personally identifiable information.

State Privacy Laws Governing Mental Health and Substance Use

A detailed survey of state privacy laws is beyond the scope of this article. However, as of 2002, fifty (50) states[91]—including the District of Columbia and excluding Arkansas—had specific statutes related to some aspect of mental health privacy in one or more settings. The Institute of Medicine's report, *Improving the Quality of Health Care for Mental and Substance-Use Conditions*, categorizes state laws governing mental health records into four types that govern patient records maintained: (1) in mental hospitals or mental health programs; (2) by mental health practitioners; (3) on behalf of patients who are involuntarily committed to mental institutions; or (4) on behalf of all patients receiving mental health treatment of any kind and in any setting.[92] Additionally, as of 2002, 36 states had specific laws pertaining to information privacy in one or more contexts for information related to substance use. With the exception of West Virginia, all state laws addressed the question of the privileged legal status of provider/patient communications involving either substance use or mental health information.

Many state laws were enacted prior to HIPAA; as a result, they do not use the same terms and nomencla-

[80] A notable exception is that of emergency situations, if the information is necessary to protect the health or safety of the student or others. *See* 20 U.S.C. §§ 1232g(b)(1)(I). For a complete list of allowable disclosures without consent, *see* 20 U.S.C. § 1232g.

[81] *See* 65 Fed. Reg. 82,462 at 82,621 (Dec. 28, 2000) for the HIPAA preamble comments regarding the exclusion of FERPA records from HIPAA.

[82] The most current analysis of FERPA and HIPAA is the study of the Virginia Tech shootings and the care Seung Hui Cho received, the information that was disclosed, the information that was kept confidential, and the decisions made by his university and health care providers throughout his college tenure. *Mass Shootings at Virginia Tech April 16, 2007*, available at http://www.vtreviewpanel.org/report/index.html, accessed on 8/31/07. The Virginia Tech Review Panel reported about the reach of HIPAA and FERPA and how perceptions of these privacy laws and fears of noncompliance often cause entities to default to nondisclosure, even when legally they are able to make disclosures. *Id*. at 63. It should be noted that the secrecy shrouding Cho's care neither helped him get proper treatment nor helped integrate him into society.

[83] 42 U.S.C. § 1396a(a)(7).

[84] 42 C.F.R. §§ 431.300-431.307.

[85] 42 C.F.R. § 431.302.

[86] 42 C.F.R. § 431.305.

[87] 42 C.F.R.§ 431.306(a).

[88] 42 C.F.R. § 431.306(b).

[89] 42 C.F.R. § 431.306(d).

[90] 42 C.F.R. § 431.306(f).

[91] *See* Pritts, Joy, et al., *The State of Health Privacy*, *supra* note 15.

[92] *See* Jost, T.S., ''Constraints on Sharing Mental Health and Substance Use Treatment Information Imposed by Federal and State Medical Record Privacy Laws,'' Appendix B to *Improving the Quality of Health Care for Mental and Substance-Use Conditions, supra* note 18.

   ISSN 1068-1213

ture as the Privacy Rule, which is structured to allow information disclosures for treatment, payment, and health care operations. The fact that state laws frequently use terms that differ fundamentally from HIPAA adds to the complexity of the analysis.

Applying Federal and State Law to "Real World" Scenarios of Treatment for Mental Health Conditions and Substance Use Disorders

The prior discussion underscores an overarching and critical difference between the Privacy Rule and the other federal laws related to mental health and substance use treatment, as well as state privacy laws, namely, the difference in the nature of consent required to authorize disclosure. HIPAA uses a general consent standard covering health information exchanges related to treatment, payment and health care operations. In contrast, Part 2, FERPA and many state laws require specific consent for disclosures of identifiable health information in a treatment context. So how are these differing standards reconciled at the point of delivery of a health care service, given the legal complexity of health information law in the context of mental health and substance use treatment?

To aid in thinking about these issues, we have, in consultation with provider experts in the field, developed several scenarios illustrating how current law applies to the exchange of data regarding alcohol treatment and substance use for treatment, payment, and health care operations. We discuss these in greater detail in a longer version of this article which will be released in 2008.[93] However, this article briefly examines one of those scenarios: what happens when there is a medical emergency.

Release of records for bona fide medical emergencies

► *A woman who presents unconscious to the emergency room from a car accident with multiple fractures, including a pelvic fracture, and requires surgery. Her daughter, who is accompanying her, explains to the emergency room physician that she believes that her mother has been prescribed a long-acting opiate antagonist to treat her alcohol dependence. If this is indeed the case, her mother may not respond to the normal course of analgesics and could be under-treated in the emergency room for pain stemming from the fractures. She would need to be given an alternate analgesic that would work, despite the opiate antagonist. Therefore, the emergency room doctor needs to know exactly what medication she has been taking, and how recently the medication to treat her alcohol dependence was administered. The physician calls the substance use treatment program (which is not a part of the health system that houses the emergency room) to determine the dosage prescribed and other information regarding prescribed timing of her medication, as well as her history of compliance with taking medications.*

In this scenario the patient is unconscious and in an emergency situation. The stakes are therefore fairly high and time is of the essence.

Under HIPAA, consent is not necessary for one physician to disclose protected health information to another in emergencies or for that matter, in the normal course of treatment.[94] Therefore, HIPAA would not bar disclosure in this instance.

As for Part 2, the first question would be whether the regulations even apply. If we assume the substance use treatment program receives some form of federal funding, which is likely, Part 2 would apply. In medical emergencies, Part 2 allows for the disclosure of patient identifying information without patient consent under certain conditions. 42 C.F.R. § 2.51(a) allows disclosures to be made to *medical personnel* who have a *need* for information about a patient, for the purpose of *treating* a condition which poses an *immediate threat* to the health of any individual, and which requires *immediate medical intervention*.

In this scenario, the substance use treatment program would be permitted to disclose patient identifying information to medical personnel (*i.e.*, the doctor in the emergency room) who need to know certain information about the patient. The information would be disclosed to treat a condition that poses an immediate threat to the patient—the pain from the multiple fractures—which requires immediate medical intervention. Of course, the disclosure would be limited, as all under Part 2 are, to information which is necessary to carry out the purpose of the disclosure and nothing more.

Part 2 imposes an additional requirement on disclosures made under these circumstances. In the emergency situation described above, receiving patient consent prior to making the disclosure to the medical staff is not necessary, reflecting the foresight the Part 2 drafters had in recognizing that requiring consent in bona fide medical emergencies could result in difficulty or poorer outcomes. In the case of an unconscious patient or in an instance in which time is of the essence, requiring consent would be either impossible or could take valuable minutes away from emergency treatment. However, Part 2 does require written documentation in the patient record immediately following the disclosure. This requirement ensures that there is a written record of every emergency-related disclosure made without the patient's written consent. Under Part 2, written documentation in the patient record must consist of:

- the name of the medical personnel to whom disclosure was made and his/her affiliation with any health care facility;
- the name of the individual making the disclosure;
- the date and time of the disclosure; and

[93] The longer version of this article can be found at http://www.gwumc.edu/sphhs/healthpolicy/chsrp/publications.cfm.

[94] *See* 45 C.F.R. § 164.506(b), in which consent ''may'' be obtained and § 164.506(c), in which a covered entity may use or disclose protected health information for treatment (without consent).

- the nature of the emergency (or error if the report was to the FDA).[95]

Because of the emergency nature of this scenario, many state laws will likely allow such disclosures without consent as well, but that will depend on the specifics of the state law. For example, California law permits disclosure of information related to alcohol and substance use treatment without the patient's written consent to medical persons to ''meet a bona fide emergency.''[96] Health systems would need to engage in a preemption analysis to determine whether state laws are stricter than HIPAA and Part 2, and if so, would need to follow the course of action most protective of the patient's information. Determining when a situation presents a legitimate emergency that warrants disclosure may be difficult. However, requests for information from emergency rooms would most likely qualify, permitting disclosure to occur.

In many respects, the scenario described above involving emergency treatment may be an easier one to understand and reconcile the various legal standards than others, because at every step of the process when a life is in the balance, overall policy typically favors disclosure to avert adverse health consequences.

However, reconciling competing legal standards and approaches when disclosure relating to mental health services and substance use treatment information is for the purpose of health care quality assessment and utilization management may raise more complex issues. For example, if the medical director of a Medicaid managed care organization (MCO) furnishing both physical and behavioral health care wanted to compare the quality of substance abuse treatment services furnished by network providers or evaluate use patterns for purposes of utilization management, HIPAA would allow the MCO to obtain all records as a health care operation matter, subject to the ''minimum necessary'' standard. But as an entity subject to Part 2, the MCO would also be bound by Part 2 and by any applicable state laws.

Arguably in this instance, the MCO would maintain direct control of its network pursuant to its contractual obligations to the plan. Accordingly, the Part 2 operational exception would apply,[97] as well as the Part 2 audit and evaluation exception. Under this exception, identifiable information regarding substance use treatment or mental health services can be disclosed to persons performing the audit or evaluation on behalf of:

- government agencies that provide financial assistance to or regulate a program;
- private entities that provide financial assistance or third party premium payments to a program;
- quality improvement or peer review organizations performing a utilization or quality control review; or
- someone who is determined by the program director to be qualified to conduct the audit or evaluation.[98]

But if the physical health and behavioral health care were furnished through separate corporate structures (*e.g.*, an MCO and a managed behavioral health organization (''MBHO'')), the MBHO could not disclose data to the MCO without the specific consent of the patients under its care. In this situation, the overall management of co-occurring conditions might be significantly impaired, as would overall utilization review and quality assurance activities. The need for specific consent covering health information held by a Part 2 provider would also prevent a primary care provider from obtaining information about a patient's mental illness or addiction treatment, unless the treatment were received from the same health care entity furnishing the primary care (*i.e.*, a community health center with an addiction treatment program).

Recommendations

This article discusses how key differences in health information privacy standards can affect the sharing of information (whether manually or electronically) related to mental illness and addiction treatment. What is generally disclosable for treatment-related purposes under the HIPAA Privacy Rule is subject to a far stricter specific consent standard under Part 2 and other federal and state laws. The justification for this higher standard—avoidance of stigma, potential employment discrimination and prosecutorial exposure that come with the revelation of such highly sensitive information—remains as strong today as it did when heightened privacy protections were first adopted. On the other hand, much more is known about the importance of having access to complete and accurate information about any existing conditions, prior treatment, medications and medical history of the patient to assure safe, high quality and effective patient treatment.

To that end, three recommendations are worthy of consideration to assist in reconciling the tension between full disclosure and patient privacy. These steps will help to advance the dialogue and ensure that the benefits of technology-enabled information directly relevant to the quality and safety of patient care do not elude persons with mental illness or substance use conditions.

Recommendation 1: Use Technology's Capabilities to Standardize and Operationalize a Specific Consent System

With the advent of electronic data systems, arguably the potential for violations of the right to privacy is greater now than ever before because individually identifiable data moves more easily electronically. At the same time, however, technology-enabled information can improve the likelihood of higher quality and safer care, particularly for patients with complex medical needs, because of the existence of more complete information about a patient's condition and course of treatment.

Thus to ensure the benefits of technology reach individuals with mental health and substance use conditions while ensuring privacy of sensitive medical information, greater emphasis should be placed on technology designs that enable specific, secure consent to the disclosure of personal information for treatment and quality assurance purposes. In other words, the emphasis has to decisively shift away from a relaxation or ''harmonization'' of standards and toward systems that can operate on a specific consent standard.

Current and developing technology should be capable of supporting such a system. For example, fire-

[95] 42 C.F.R. § 2.51(b).
[96] Cal. Health & Safety Code § 11845.5.
[97] *See* 42 C.F.R. § 2.12(c)(3).
[98] *See* 42 C F. R. § 2.53.

   ISSN 1068-1213

walls can be established that would protect information that must be kept private under Part 2. In addition, decision support pop-ups for elements of consent can be included in data systems to assist providers in following the necessary steps for obtaining consent. Indeed, it is through a specific focus on the adaptation of technology to support solutions that are capable of accommodating both the elements of a specific consent and a general consent standard that this apparent inconsistency can be resolved without having to face the profoundly more contentious question of whether specific consent standards should give way.

Recommendation 2: Ensure that Patient's Decision to Withhold Health Information from Other Treating Providers is Truly ''Informed.''

Much of the focus in specific consent statutes is on the importance of *shielding* information that is the subject of a specific consent. In our view, far less attention has been placed on ensuring that a decision by a patient undergoing mental health or substance use treatment to *withhold* information from other treating health professionals is truly informed. An informed consent must rest on full information and enable the patient to understand the material risks and benefits associated with a course of conduct. Withholding consent to the release of personal health information to a patient's other treating health professionals when that information will be used *only for the purpose of enabling other treating providers to best assure safety and quality* carries significant risks. To be sure, in a health emergency even specific consent statutes can be overridden. But an equally great concern may be the withholding of important health information from a patient's treating primary health care professionals or specialists, especially diagnostic information or information about a particular course of therapy related to mental illness or addition. In an age of patient empowerment, it is essential that patients fully understand the nature of the special privacy shield that applies to data about mental illness and addiction and that they be counseled impartially and carefully regarding their right to specifically consent to the sharing of such information in certain circumstances.

Recommendation 3: Strengthen the Tools of Enforcement for Violations of Privacy

Individuals may become more secure with a broader approach toward approved information sharing if they know that the sanctions for violations for re-disclosure of controlled information are swift and serious. Remedies for unauthorized re-disclosures or misuse of confidential information might include steep penalties (*e.g.*, significant fines, debarment from participation in federal or state health care programs, suspension of licensure) for health professionals who re-disclose for any purpose other than the purpose covered by the consent.

Conclusion

These recommendations require significant follow-up by policymakers, health care providers, agency administrators, those who design information technology, and health care regulators.

This much is clear, however: *first*, that mental health and substance use treatment should not be excluded from the potential benefits and transformational power of technology-enabled health care; *second*, that a specific consent standard does not have to—and should not be permitted to—operate as a barrier to such a transformation given the potential of technology adaptation; and *third*, that through operational design, a commitment to genuine informed consent, and provider accountability if the limits of patient-controlled consent are exceeded, it may be possible to reconcile the important goals of protecting the privacy of personal health information and improving health information transparency for the critical purposes of quality improvement and health disparities reduction.