A Delicate Balance: Behavioral Health, Patient Privacy, and the Need to Know

California HealthCare Foundation

ISSUE BRIEF

March 2008

Introduction

Finding the right balance among health care quality, patient safety, and health information privacy is a major policy challenge. No health issue better illustrates this challenge than the use and disclosure of personal information about mental illness and substance use disorders in electronic health information systems.

Knowing about a patient's history of mental illness or substance use disorders, and their past treatment, is vital to proper and safe care. Sharing information on diagnosis, treatment, and care plans can help promote a more comprehensive picture of a patient's needs and reduce the risk of medical error.

But disclosing or sharing personally identifiable data about mental illness and substance use disorders, even when done for entirely appropriate reasons, carries significant risks. Misuse or inappropriate disclosure could lead to the loss of a patient's job or occupational licensing; raise barriers to health, disability, or life insurance coverage; and even result in criminal prosecution.

This issue brief explores federal and state laws governing health information privacy as they relate to treatment for mental illness and substance use disorders, focusing on privacy and the sharing of information in treatment contexts. Three scenarios illustrate some of the challenges of finding the correct balance between privacy and disclosure. The brief concludes with three recommendations that could reduce the risks of misuse of information or inappropriate disclosure while promoting patient safety and health care quality.

Overview

The Social and Legal Tradition of Protecting Health Information

Privacy is an article of faith for Americans. Concern about privacy protection dates to the nation's founding. Privacy is a tenet of the common law, the very bedrock of the American legal system. Indeed, 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…."[1] Federal regulations promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule recognize 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.[2]

There has been a longstanding debate over whether certain types of health information records deserve greater legal protection than others. Unauthorized disclosure of sensitive health information about mental illness, substance use disorders, or genetic traits can cause enormous harm, including social stigma, employment discrimination, insurance discrimination, and, for addictions, possible

criminal prosecution, job termination, forfeiture of legal protections such as protection under the Americans with Disabilities Act, or the right to receive disability benefits. Fear of unauthorized disclosure of sensitive health information can create a strong disincentive for someone to seek treatment. Advocates point out that punishing unwarranted disclosures after they occur provides little relief because the damage already has occurred and the penalties are weak.

Accordingly, state and federal laws generally provide a higher degree of protection for personal mental health information—especially information relating to a substance use disorder—than for other personal health information. Unlike HIPAA, the predominant privacy law governing personal health information, these laws typically require the individual's specific written consent before any such information can be disclosed.

The Special Status Accorded Mental Illness and Substance Use Disorder Information

HIPAA and the Privacy Rule

The enactment of HIPAA coincided with the explosive growth of electronic health information technology.[3] Converting from paper medical records to electronic health records is a national health policy priority articulated in presidential executive orders and legal and payment reforms aimed at spurring technology adoption, such as compensation incentives for physicians. Policies to promote health information technology are driven by the belief that electronic health records will improve patient safety and health care quality while lowering costs.

HIPAA is a legal framework for the handling of individually identifiable health information that reconciles the need for broad information exchange with the need for individual privacy. It provides a federal floor for privacy protection while preserving more stringent state laws. HIPAA does not displace other federal laws; separate, more protective federal privacy standards for records with personally identifiable information about mental illness and substance use disorders must be considered in tandem with HIPAA.

The Privacy Rule applies to covered health care entities, which can include health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form for administrative purposes.[4] The rule protects individually identifiable health information—called "protected health information"—held by those entities. It recognizes that other federal and state privacy and confidentiality laws accord greater protection to certain types of health information and leaves those laws undisturbed.

In general, the Privacy Rule permits the use and disclosure of protected health information for treatment, payment, and health care operations without an individual's written permission. In recognition of professional traditions and ethical obligations, the rule permits covered entities to obtain written permission and consent to use and disclose health information for these core purposes, in accordance with their own privacy policies.[5] Thus, the Privacy Rule establishes a "general consent" standard that allows health professionals who treat patients to share, at their discretion, patient information with other such professionals or providers without getting specific written consent.

Although not required to do so, professionals who treat patients may ask them to share protected health information. The Privacy Rule does not require any specific forms or procedures when obtaining consent; instead, the rule imposes a "minimum necessary" standard. This means that in disclosing protected health information, covered entities must limit their disclosures to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.[6] However, the "minimum necessary" rule does not apply to requests for or disclosures of protected health information for treatment purposes, in which case providers can share

any protected health information in the patient's medical record.

In addition, the Privacy Rule allows covered entities to use and disclose protected health information for a number of "permissive" purposes without an individual's written consent. These include national priorities such as health care oversight, public health, research, and law enforcement, and disclosure required by other laws.[7] This approach allows health care professionals to continue many of their existing privacy practices as long as their policies and practices are explained to patients in advance and in writing.

Beyond treatment, payment, and health care operations, or outside of the permissive exceptions noted above, the Privacy Rule requires that entities obtain written authorization from patients before using or disclosing protected health information. Authorizations must meet specific content and format requirements.

A special authorization rule in HIPAA regulates psychotherapy notes. In this single instance, HIPAA accords greater protection to a specific type of information than it does to other forms of personal health information, in deference to longstanding legal and policy concerns and professional custom.

HIPAA is enforced by the Office for Civil Rights in the U.S. Department of Health and Human Services. The office ensures compliance, investigates reported violations, and imposes civil monetary penalties.[8] Since 2003, it has received approximately 32,000 complaints, investigated about 8,000 of them, and achieved corrective action in about 5,400 cases (68 percent).[9] The office has not assessed any civil fines to date. HIPAA does not include a private right of action that would enable persons to sue covered entities to halt disclosures or to recover damages for injuries arising from such.

HIPAA is widely viewed as a national code of conduct for health professionals regarding protected health information. While it leaves much discretion to professionals, it also holds them accountable for certain disclosures that require patient authorization.

HIPAA's Relationship to State Law

The Privacy Rule essentially establishes a road map for reconciling differences between HIPAA and state law. HIPAA generally preempts state laws that are contrary to it—that is, when complying with both state and federal requirements would be impossible or when provisions of the state law would impede compliance with the Privacy Rule.[10] However, because HIPAA expressly permits covered entities to make disclosures "as required" by other laws,[11] state laws that mandate disclosures are not deemed contrary to HIPAA and thus do not conflict with it.

HIPAA also specifies that its standards do not supersede a contrary provision of state law if the provision imposes substantive or procedural requirements or standards that are more stringent or more protective than HIPAA's standards.[12] State laws that accord greater privacy protections are considered more stringent than HIPAA.

HIPAA does not preempt state laws that govern the reporting of various types of information, including but not limited to disease, injury, child abuse, public health surveillance, investigation, or intervention.[13] It does not interfere with provisions of state law that require a health plan to report or to provide access to information for management, financial audits, and certain other limited purposes.[14]

HIPAA's Relationship to Other Federal Laws

In addition to HIPAA, several federal laws directly govern the disclosure of mental illness and substance use disorder information. Table 1 (on the following page) compares these laws, which are discussed in greater detail.

Table 1. Consent Requirements in Key Federal Laws for Disclosure of Individually Identifiable Information

Privacy Law or Regulation	Type of Patient Authorization or Consent Necessary for Use or Disclosure
HIPAA Privacy Rule	No consent necessary for disclosure of information regarding treatment, payment, or health care operations
42 C.F.R. Part 2 Federal Confidentiality of Alcohol and Drug Abuse Patient Records	Specific consent necessary for disclosure, including for treatment, payment, or health care operations
Family Education Rights and Privacy Act (FERPA)	Specific consent necessary for disclosure of educational records for medical purposes
Medicaid Law	Unclear—no specific federal ruling or official interpretation in the wake of HIPAA

The Federal Confidentiality of Alcohol and Drug Abuse Patient Records law, otherwise known as "Part 2," has the most profound impact on the sharing of personal health information related to mental illness or substance use disorders. It reflects congressional concern about the stigma associated with, and the legal implications of, seeking alcohol and drug treatment,[15] creating a virtual shield against the disclosure of personal health information pertaining to alcohol- and substance-related conditions and treatment. This law has important implications for the electronic exchange of data that includes mental illness and substance use disorder information.

With certain conditions and exceptions, Part 2 strictly prohibits the disclosure and use of drug and alcohol records maintained in connection with any federally assisted alcohol and drug program.[16] Disclosure in this instance means "a communication 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."[17] Patient identifying information includes 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.[18] Criminal penalties for violations include a fine of up to $500 for the first offense and up to $5,000 for each subsequent offense.[19]

Part 2 is stringent, prohibiting disclosure of any information that could directly or indirectly identify an individual as a drug or alcohol patient.[20,21] And it broadly defines "programs" and "patients." Programs are:

- Individuals, entities (other than general medical care facilities), or identified units within such facilities that provide or claim to provide alcohol or drug abuse diagnosis, treatment, or referral for treatment.
- Medical personnel or other staff in general medical care facilities whose primary function is to provide alcohol or drug abuse diagnosis, treatment, or referral for treatment, and who are identified as such providers.[22]

A patient is "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."[23] All permissible disclosures are limited to "that information which is necessary to carry out the purpose of the disclosure."[24]

Nearly all disclosures under Part 2 require specific patient consent, and the content and format of consent must meet the federal standards. In contrast, the HIPAA Privacy Rule does not require any consent to disclose protected health information for purposes of treatment, payment, or health care operations; providers who elect to obtain consent may do so using a general consent form. Thus, the "specific consent" content and format mandated by Part 2 set a far higher bar than HIPAA does.

Part 2's restrictions on disclosure allow certain exceptions. Among these are communications within a program or between a program and an entity that has direct administrative control over that program, and communications between a program and a qualified service organization. Disclosures without patient consent also are acceptable in certain limited circumstances, including medical emergencies, research activities, and audit or evaluation activities.[25] Re-disclosures — that is, secondary disclosures stemming from an initial one — are prohibited unless they are back to the program from which the information was obtained.[26]

FERPA

The Family Educational Rights and Privacy Act of 1974 protects the privacy of student education records.[27,28] FERPA:

- Gives parents and students the right to access student records, and protects the privacy of those records by preventing unauthorized third-party access.[29]
- Prohibits the release of educational records without parental consent or, in the case of students age 18 or older or attending college, without the student's consent.[30]
- Applies to all public or private educational agencies that receive federal education funding.[31]

The range of information that is considered protected under FERPA is broad and can include information related to the treatment of a specific student for substance use disorders or mental illness.

Although FERPA protects health records maintained by educational agencies, such as school-based clinics, it permits certain disclosures regarding substance use disorders and mental illness unless disclosure is prohibited under more stringent and protective state law. It also cites circumstances in which disclosures without consent are allowed.

Accordingly, FERPA is similar to HIPAA, requiring written consent for certain disclosures but allowing certain others to be made without consent. Of specific interest in this issue brief is the requirement that parental or, when appropriate, student consent be obtained to release educational records involving medical treatment.

Records covered by FERPA are not subject to HIPAA because the latter's definition of protected health information specifically excludes FERPA records.[32] Thus, unlike HIPAA and Part 2, HIPAA and FERPA do not overlap. FERPA adds an extra layer to federal law governing health information and policy protections regarding the confidentiality of records.[33]

Medicaid Privacy Statute

Medicaid law contains privacy provisions dating from its enactment.[34] Although the language in Medicaid's privacy statute closely parallels the language in HIPAA, it has not been specifically interpreted since the HIPAA Privacy Rule was promulgated.

In general, state Medicaid programs require specific written consent to disclose personal health information. The U.S. Department of Health and Human Services has never issued a formal interpretation that would squarely align Medicaid privacy standards with the HIPAA Privacy Rule.

Federal Medicaid law requires state medical assistance plans to provide safeguards limiting the use and disclosure of specific information about applicants and recipients to purposes directly connected with administration of the plans.[35] Under Medicaid regulations, such purposes include establishing eligibility, determining the proper amount of medical assistance, providing services for recipients, and conducting or assisting investigations, prosecutions, or legal proceedings related to plan administration.[36,37]

Other requirements include these:

- Medicaid plans must have criteria that specify the circumstances in which information about applicants and recipients can be released and used.[38] The plans may share information only with entities whose confidentiality standards are as rigorous as the plans' standards.[39]
- With certain exceptions and whenever possible, permission must be obtained from a family or individual before an agency can respond to an information request from an outside source.[40]
- Agencies must have data exchange agreements (similar to HIPAA business associate agreements) in place to exchange data with other agencies.[41]

Like HIPAA, the Medicaid statute provides a basic privacy standard and formal protocols for information disclosures. Unlike HIPAA, it does not appear to address patient consent to disclose personal health information for the purposes of treatment, payment, or health care operations; rather, like FERPA and Part 2, the Medicaid statute appears to rely on the more traditional approach of requiring specific patient consent to disclose personally identifiable information.

State Privacy Laws Governing Treatment for Mental Illness and Substance Use Disorders

As of 2002, all states but Arkansas, and the District of Columbia, had specific statutes related to some aspect of mental health privacy in one or more settings.[42] In *Improving the Quality of Health Care for Mental and Substance-Use Conditions,* the Institute of Medicine categorizes state laws governing the privacy of mental health records into four types, depending on the setting in which the records are found: records in mental hospitals, those in mental health programs, records of patients involuntarily committed to mental institutions, and those of patients receiving mental health treatment of any kind in any setting.[43] In addition, 36 states had laws governing information privacy related to substance use disorders.[44] With the exception of West Virginia's, all of the laws address the privileged legal status of provider/patient communications involving substance abuse or mental health information.

Many states enacted laws before HIPAA. These laws often do not use the same terms and nomenclature as those in the Privacy Rule.

How Federal and State Laws Would Apply in Three Scenarios

This issue brief underscores the tension between the general consent provisions in HIPAA and the specific consent requirements in other federal and state laws. Because of these crucial differences, the release of information about physical conditions for the purposes of patient safety and health care quality might be prohibited in cases involving mental illness and substance use disorders.

How does one reconcile the different standards, given the legal complexity of health information law related to treatment for mental illness and substance use disorders? To promote greater understanding of these issues, the authors, in consultation with experts in the field, have developed several scenarios to illustrate how current law would apply to the exchange of alcohol and substance use disorder information for the purposes of treatment, payment, and health care operations.

SCENARIO ONE

Release of Records for Medical Emergencies

A woman arrives unconscious in the emergency room after a car accident. She has multiple fractures, including a pelvic fracture, and requires surgery. The woman's daughter explains to the emergency room physician that her mother has been prescribed a long-acting opiate antagonist to treat her alcohol dependence. If this is true, the woman may not respond to the normal course of analgesics and could be undertreated for pain caused by the fractures. The physician, who needs

to know exactly what medication she has been taking and how recently it was administered, calls the substance abuse treatment program, which is not a part of the health system that houses the emergency room, to determine the dosage prescribed, other information regarding the prescribed timing of her medication, and her history of compliance with taking medications.

The patient is unconscious and in an emergency situation. Therefore, the stakes are 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.[45] Therefore, HIPAA would not bar disclosure.

If the substance abuse treatment program receives some form of federal funding, which is likely, Part 2 would apply. In medical emergencies, Part 2 allows patient identifying information to be disclosed without patient consent under certain conditions. Disclosures are permitted under 42 C.F.R. § 2.51(a) as follows:

- To medical personnel who need information about a patient; and
- To treat a condition that poses an immediate threat to an individual's health and requires immediate medical intervention.

In this scenario, the substance abuse treatment program could legally disclose patient identifying information to medical personnel, such as the emergency room doctor in this scenario, who need certain information about the patient. The information would enable treatment of a condition that poses an immediate threat to the patient (the pain from multiple fractures) and requires immediate medical intervention. Only information necessary to carry out the purpose of the disclosure could be released.

Part 2 imposes an additional requirement in these circumstances: In the case of an unconscious patient or when time is of the essence, written documentation must be added to the patient record immediately after the disclosure.

Many state laws would also allow disclosures without consent because of the emergency. For example, California law permits disclosure of information about treatment for alcohol and substance use disorders without the patient's written consent to "meet a bona fide emergency."[46]

Compared to other situations, it may be easier to understand and reconcile the different legal standards that apply in this scenario because at every step of the process, when a life is in the balance, overall policy typically favors disclosure to prevent adverse health consequences.

SCENARIO TWO

Communications Relating to Quality Assessments or Outcome Evaluations

The medical director of a county-operated managed care organization wants to compare all of its network providers in terms of the outcomes of patients who have received treatment for mental illness and substance use disorders from them. He asks the providers to send copies of all such service records regarding visits that took place in the previous two years.

As noted earlier, HIPAA generally permits the use and disclosure of protected health information for treatment, payment, and health care operations without the patient's consent. Disclosure for the purpose of health care quality assessment and utilization management may raise more complex issues. Quality assessment and improvement activities, including outcomes evaluation, are considered health care operations under HIPAA.[47] Therefore, HIPAA would allow the network providers to share their records with the medical director for this purpose without having to obtain consent from each patient. The use of such information would be subject to the "minimum necessary" requirement. But as an entity subject to Part 2,

the managed care organization would also be bound by Part 2 and any applicable state laws.

Arguably, the managed care organization has direct control of its provider network pursuant to contractual obligations. Therefore, the Part 2 operational exception would apply and so would the Part 2 audit and evaluation exception.[48] Identifiable information regarding mental health services or substance abuse treatment may be disclosed to persons performing the audit or evaluation on behalf of the following people and organizations:

- 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 that perform a utilization or quality control review; and
- A person the program director determines is qualified to conduct an audit or evaluation.[49]

However, if the physical and behavioral health care were furnished through separate corporate structures, such as a managed care organization and a managed behavioral health organization, the latter could not disclose data to the managed care organization without the specific consent of the patients under its care. In this situation, the overall management of multiple health conditions, as well as utilization review and quality assurance activities, might be significantly impaired.

Part 2 provisions governing the need for specific consent would also prevent a primary care provider from obtaining patient-specific information from a provider specializing in mental illness or addiction treatment, unless the latter was part of the same health care entity that furnished the primary care, such as a community health center with an addiction treatment program.

SCENARIO THREE

Sharing Information About Multiple Disorders and Diagnoses Without Patient Consent

A patient who has alcoholism, diabetes, and depression sees a primary care physician in a community health center for diabetes treatment. During the appointment, the patient tells the doctor that she has begun attending a federally funded program for substance abuse treatment that is a wholly separate entity from the community health center. The doctor asks the treatment program to share the patient's records so he can stay informed about the course of her alcoholism treatment and use the information to help treat her diabetes. The patient is very concerned about the privacy of her medical data and does not consent to have any part of her records shared. She is worried that her employer will learn about her health problems and fire her.

HIPAA would allow the exchange of medical information between the patient's providers without her consent because it would be for the purpose of treatment. While the patient has the right under HIPAA to request that the providers not share information related to her mental illness and alcohol treatment, providers are not required to honor such requests.[50]

However, under Part 2, which is more stringent, the substance abuse treatment facility may not share information in the patient's medical record with the primary care physician or any other provider without the patient's consent. The circumstances in this scenario do not fit squarely into any of Part 2's exceptions or instances in which it does not require consent.

Therefore, if the patient does not consent, the substance abuse treatment facility cannot share her medical record information or any personally identifiable information with her other doctors. This enables the patient to control access to her sensitive health information and may help alleviate her fear that her employer will obtain it. But she may not fully appreciate the fact that if various providers

share such information, it might lead to better care, continuity of care, and holistic treatment.

If this scenario occurred in a state where privacy laws governing mental health information were more stringent than HIPAA and were drafted to be similar to Part 2, any information regarding mental illness or alcohol treatment could not be disclosed without the patient's consent. If this scenario occurred in a state with less stringent laws, the HIPAA standard would apply to mental health information, and the Part 2 standard would apply to alcohol treatment information.

California's law, for example, prohibits disclosure of any information regarding private outpatient treatment by a psychotherapist; its detailed consent requirements are more stringent than those in HIPAA and Part 2.[51] The District of Columbia's law allows patients who are receiving mental health services to voluntarily authorize the disclosure of their records as long as a specific written authorization is executed.[52]

In this more complex scenario, federal and state laws would require the patient's consent before caregivers could share information beneficial to her treatment. But if she does not fully understand the risks and benefits of disclosure, she may not be able to make a truly informed decision regarding consent.

Discussion and Recommendations

This issue brief discusses how key differences in health information privacy standards can affect the manual or electronic sharing of personal information related to treatment for mental illness and substance use disorders. Information that the HIPAA Privacy Rule generally allows to be disclosed for treatment-related purposes is subject to far stricter specific consent standards under Part 2 and other federal and state laws.

The justification for this higher standard—avoidance of stigma, employment discrimination, and exposure to prosecution that could result if highly sensitive information is revealed—is as strong today as when these privacy protections were adopted. Furthermore, much more is now known about the importance of having access to complete and accurate information regarding patients' medical conditions and history, prior treatment, and medications in order to provide safe, high-quality, and effective care.

To help reconcile the tension between full disclosure and patient privacy, the authors recommend three reforms that would improve communication between patients and physicians, and ensure that persons with mental illness or substance use disorders benefit from state-of-the-art information management.

Use Technology to Standardize a Specific-Consent System

The easy transfer of data using electronic data systems increases the potential for privacy violations. But the same technology can also improve the safety and quality of care, particularly for patients who have complex medical needs, because it makes more complete information about a patient's condition and course of treatment more readily available.

Technological tools giving mental health and substance abuse patients a means of providing specific, secure consent to disclose sensitive personal information would foster an appropriate balance between technological benefits and privacy protections. Two examples of such tools are firewalls that could protect information that must be kept private under Part 2, and decision-support pop-ups in electronic data systems to help providers follow the necessary steps for obtaining consent.

Ensure That a Patient's Decision to Withhold Information 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. Far less attention has been paid to

ensuring that patients undergoing treatment for mental illness or substance use disorders are truly informed when they decide to withhold information from other health professionals who treat them.

Fully informed consent hinges on patients' thorough understanding of the risks and benefits associated with information sharing. Withholding consent when caregivers would use personal information only to assure treatment safety and quality carries significant risks. Specific-consent statutes can be overridden in medical emergencies, but an equally great concern may be situations in which important health information is withheld from a patient's primary health care physician or specialist—especially diagnostic information or information about a particular course of therapy related to mental illness or addiction.

A crucial part of patient empowerment is patients' full understanding of how the special privacy shield applies to their mental illness or addiction information. In addition, they must receive impartial and careful counseling about their rights regarding the sharing of such information in certain circumstances.

Strengthen Privacy Enforcement Tools

Patients may become more comfortable with information sharing if they know that penalties for violations of privacy laws are swift and serious. Remedies for unauthorized use of confidential information could include steep penalties, such as significant fines, exclusion from participation in federal or state health care programs, or suspension of licenses for health professionals who disclose information for any purpose other than that covered by a disclosure consent.

Conclusion

Mental health and substance use disorder treatment need not be excluded from the potential benefits and transformational power of technology-enabled health care. And a specific-consent standard need not be a barrier to technological innovation. Through operational design, a commitment to genuine informed consent, and provider accountability, it may be possible to reconcile the important goals of protecting the privacy of personal health information, and that of making such information more readily available for the critical purposes of improving the safety and quality of care for mental illness and substance use disorder patients.

Authors

J. Zoë Beckerman, J.D., M.P.H., associate, Feldesman Tucker Leifer Fidell LLP, Washington, D.C.

Joy Pritts, J.D., research associate professor, Health Policy Institute, Georgetown University, Washington, D.C.

Eric Goplerud, Ph.D., research professor, Department of Health Policy, The George Washington University School of Public Health and Health Services, Washington, D.C.

Jacqueline C. Leifer, J.D., partner, Feldesman Tucker Leifer Fidell LLP, Washington, D.C.

Phyllis A. Borzi, J.D., research professor, Department of Health Policy, The George Washington University School of Public Health Services, Washington, D.C.

Sara Rosenbaum, J.D., 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.

David R. Anderson, M.G.A., senior research scientist, Department of Health Policy, The George Washington University School of Public Health and Health Services, Washington, D.C.

Acknowledgment

The authors would like to thank The Pew Charitable Trusts for their support of the research behind this brief and the journal article on which the brief is based.

About the Foundation

The California HealthCare Foundation, based in Oakland, is an independent philanthropy committed to improving California's health care delivery and financing systems. Formed in 1996, our goal is to ensure that all Californians have access to affordable, quality health care. For more information about the foundation, visit us online at www.chcf.org.

Endnotes

1. U.S. Constitution, amend. 4.
2. Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462 and 82,464 (December 28, 2000). See also Standards for Privacy of Individually Identifiable Health Information, Proposed Rule, 64 Fed. Reg. 59,918 and 60,008 (November 3, 1999).
3. Blumenthal, D., and J.P. Glaser. "Information technology comes to medicine." *New England Journal of Medicine* 2007;356(24): 2527–2534.
4. 45 C.F.R. §§ 160.102(a) and 164.500.
5. 45 C.F.R. §§ 164.502(b) and 164.508.
6. *Ibid.*
7. 45 C.F.R. § 164.512.
8. 42 U.S.C. § 1320d-5. Penalties are more severe for wrongful disclosure: fines of not more than $50,000, imprisonment, or both.
9. U.S. Department of Health and Human Services. Compliance and Enforcement: Numbers at a Glance Archive (www.hhs.gov/ocr/privacy/enforcement/numbersglance.html).
10. 45 C.F.R. § 160.202.
11. 45 C.F.R. § 164.512(a).
12. P.L. 104-191 § 264(c)(2).
13. 42 U.S.C. § 1130d-7(b) and 45 C.F.R. § 160.203(c).
14. 42 U.S.C. § 1130d-7(c) and 45 C.F.R. § 160.203(d).
15. Kamoie, B., and P. Borzi. "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.
16. 42 C.F.R. §§§ 2.3(a), 2.12(b), and 2.12(c).
17. 42 C.F.R. § 2.11.
18. *Ibid.*
19. 42 C.F.R. §§ 2.3 (b)(3) and 2.4.
20. 42 C.F.R. § 2.12(d).
21. Kamoie and Borzi, *supra* note 44, at 17. *See also* 42 C.F.R. § 2.11 *et seq.*
22. 42 C.F.R. § 2.11. 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 are his primary functions and he is identified specifically as that type of provider.
23. 42 C.F.R. § 2.11
24. 42 C.F.R. § 2.13(a).
25. 42 C.F.R. subpart D, "Disclosures without Patient Consent."
26. 42 C.F.R. §§ 2.52(b) and 2.53(d).
27. 20 U.S.C. § 1232g.
28. *Disability Rights Wisconsin, Inc., v. Wisconsin Department of Public Instruction,* 463 F. 3d 719, 730 (7th Cir. 2006).
29. *Kestenbaum v. Michigan State University,* 294 N.W. 2d 228, 231 (1980); 120 Cong. Rec. 39,858 and 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); and Daggett, L. "Bucking up Buckley I: Making the Federal Student Records Statute work." *Catholic Law Review* 1997;46: 617–670.
30. 20 U.S.C. § 1232g(d).
31. 34 C.F.R. § 99.1.

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

33. The most current analysis of FERPA and HIPAA is a study of the Virginia Tech shootings and the care that assailant Seung-Hui Cho received, the information that was disclosed or kept confidential, and the decisions that his university and health care providers made throughout his college tenure; Virginia Tech Review Panel. The Virginia Tech Review Panel Report, August 2007 (www.vtreviewpanel.org/report/index.html). The panel cited the reach of HIPAA and FERPA, and how perceptions of these privacy laws plus fears about noncompliance often cause entities to default to nondisclosure, even when they can legally make disclosures; *Ibid.* at 40. The secrecy shrouding Cho's care neither helped him get proper treatment nor helped integrate him into society.

34. 42 U.S.C. § 1396a(a)(7).

35. *Ibid;* 42 C.F.R. § 431.205.

36. 42 C.F.R. §§ 431.300 – 431.307.

37. 42 C.F.R. § 431.302.

38. 42 C.F.R. § 431.306(a).

39. 42 C.F.R. § 431.306(b).

40. 42 C.F.R. § 431.306(d).

41. 42 C.F.R. § 431.306(f).

42. Pritts, J., A. Choy, L. Emmart, and others. *The State of Health Privacy,* 2d edition. Health Privacy Project. 2002 (www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm, ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf, and ihcrp.georgetown.edu/privacy/pdfs/statereport2.pdf).

43. Jost, T.S. "Constraints on Sharing Mental Health and Substance Use Treatment Information Imposed by Federal and State Medical Record Privacy Laws," Appendix B in *Improving the Quality of Health Care for Mental and Substance Use Conditions, supra* note 6.

44. Choy, Emmart, and others. *The State of Health Privacy,* 2d edition.

45. *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).

46. California Health & Safety Code § 11845.5.

47. 45 C.F.R. § 164.501.

48. 42 C.F.R. § 2.12(c)(3).

49. 42 C.F.R. § 2.53.

50. 45 C.F.R. § 164.522.

51. California Civil Code § 56.104(d).

52. D.C. Code Ann. §§ 7-1202.01 and 7-1202.02.