SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Health Matrix: The Journal of Law-Medicine

Volume 17 | Issue 2

2007

Confidentiality and Privacy in Health Care from the Patient's Perspective: Does HIPPA Help

Ilene N. Moore

Samuel Leason Snyder

Cynthia Miller

Angel Qi An

CONFIDENTIALITY AND PRIVACY IN HEALTH CARE FROM THE PATIENT'S PERSPECTIVE:

DOES HIPAA HELP?

Ilene N. Moore[†], *Samuel Leason Snyder*[††], *Cynthia Miller*[†††], *Angel Qi An*[‡], *Jennifer U. Blackford*[*], *Chuan Zhou*[**], *Gerald B. Hickson*[***]

[†] B.S., State University of New York at Stony Brook (1973); M.D., New York University School of Medicine (1977); J.D., University of California, Berkeley (1989); Assistant Professor of Medical Education and Administration, Assistant Professor of Family Medicine, Center for Patient and Professional Advocacy, Vanderbilt University School of Medicine.

[††] B.S., Georgetown University; Medical Student III, Vanderbilt University School of Medicine.

[†††] B.S., Vanderbilt University; MSSW, University of Tennessee; Research Coordinator, Center for Patient and Professional Advocacy, Vanderbilt University School of Medicine; Social Worker, Clinical Oncology, Vanderbilt Children's Hospital.

[‡] B.S., Peking University (2000); M.S., University of Chicago (2004); Biostatistician, Department of Biostatistics, Vanderbilt University School of Medicine.

[*] B.S., Florida State University (1990); M.S., Vanderbilt University (1994); Ph.D., Vanderbilt University (1998); Assistant Professor of Psychiatry, Vanderbilt University School of Medicine.

[**] B.S., Peking University (1996); M.S., M.S., University of Maryland, Baltimore County (1998, 2000); Ph.D., University of Washington (2003); Assistant Professor of Biostatistics, Vanderbilt University School of Medicine.

[***] B.S., University of Georgia (1973); M.D., Tulane University School of Medicine (1978); Professor of Pediatrics, Associate Dean for Clinical Affairs, Director of the Center for Patient and Professional Advocacy, Director of the VUMC Clinical Risk Reduction and Loss Prevention, Vanderbilt University School of Medicine.

INTRODUCTION

Since April 14, 2003, every U.S. health care recipient is supposed to receive and acknowledge receipt of a HIPAA Form[1] that describes the provider's privacy practices. HIPAA, the Health Portability and Insurance Accountability Act of 1996,[2] as implemented by the Department of Health and Human Services (HHS), requires that the notice include details of how medical information may be used, disclosed, or amended.[3] About half of the people who sign the form do not read it, and of those who say they understand it, about one-third are unable to correctly answer questions about its terms.[4] In all probability, the majority do not appreciate that the notice reflects the federal government's effort to define the boundary between individual privacy and an increasingly complex, information-based health care system.[5]

While the idea of written privacy notices may be new, the idea that patients' medical information is private and entitled to protection from unauthorized disclosure is not. Nor is it novel that there are circumstances that warrant exceptions to the rule of nondisclosure, even in the absence of consent from a patient.[6] Prior to implementation of

---

The authors wish to thank research assistant, Ms. Sumi Rebeiro, for her help with the study discussed in the Article.

[1] *See* EPICTIDE, INC., MEDICAL IDENTITY THEFT CONSUMER STUDY SURVEY RESULTS 11 (2006), http://www.epictide.com/documents/2006-1212-Consumer-Survey.pdf (reporting that about half of the respondents to consumer survey stated that they were asked to sign the form).

[2] *See generally* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA].

[3] OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., OCR GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE, 40-41 (rev. ed. 2003), *available at* http://www.hhs.gov/ocr/hipaa/guidelines/notice.pdf (citing 45 C.F.R. § 164.520(b)). "Covered entities" are health care providers, health plans, and health care clearinghouses who electronically transmit health information for transactions covered under standards adopted by HHS under HIPAA, e.g., electronic billing and fund transfers. 45 C.F.R. § 160.103 (2003). *See also* OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 2 (rev. ed. 2003), *available at* http://www.hhs.gov/ocr/privacysummary.pdf.

[4] *See* EPICTIDE, INC., *supra* note 1, at 11.

[5] While the Federal Privacy Act of 1974 regulates federal agencies or federal contractors that maintain records of personal information about individuals, it does not apply to private or non-governmental entities. *See* Federal Privacy Act of 1974, 5 U.S.C. § 552a (2000). HIPAA fills this gap with respect to individually identifiable health information.

[6] *See* Simonsen v. Swenson 177 N.W. 831, 832 (Neb. 1920) (physician may make reasonable and necessary disclosure to prevent spread of a contagious disease); Bratt v. IBM, 467 N.E.2d 126, 137 (Mass. 1984) (no invasion of privacy where phy-

HIPAA, issues related to privacy and confidentiality in health care were governed by state common law and, in some circumstances, statutory law,[7] which, not surprisingly, produced inconsistent outcomes.[8] HHS's Privacy[9] and Security[10] Rules created national standards for the first time to address how health information may be used[11] and safeguarded[12] and enumerated administrative patient "pri-

---

sician's disclosure of employee's medical information served a valid and substantial interest of the employer); Hoesl v. U.S., 451 F. Supp. 1170, 1176 (N.D. Cal. 1978), *aff'd on other grounds per curiam*, 629 F.2d 586 (9th Cir. 1978) (duties of an examining physician employed to examine employees of the employer run primarily to the employer); Tarasoff v. Regents of the Univ. of Cal., 551 P2d. 334, 353 (Cal. 1976) (finding affirmative duty for psychotherapist who determines that patient poses a serious danger of violence to a third party to warn prospective victim); Horne v. Patton, 287 So. 2d 824, 827-28 (1973); Gammill v. United States, 727 F.2d 950, 953 (10th Cir. 1984) (reporting statute creates no duty to warn third parties).

[7] *See generally* Health Privacy Project, View the Summary of a Specific State, http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat_list.htm (last visited Mar. 29, 2007) (summarizing each state's medical privacy and confidentiality of medical information laws). Some statutes provide that unauthorized disclosure of confidential medical information may be grounds for discipline by a medical board. *See, e.g.*, CAL. BUS. & PROF. CODE § 2263 (West 2003); TENN. CODE ANN. § 63-6-214(b) (2004 & Supp. 2006). The *Tarasoff* decision has been codified in several states. *See, e.g.*, CAL. CIV. CODE § 43.92 (West Supp. 2007); CAL. EVID. CODE §1024 (West 1995 & Supp. 2007) (stating an exception to the general psychotherapist-patient privilege when the patient poses a serious threat of physical violence to himself or others); TENN. CODE ANN. §§ 33-3-206 to -207 (2001 & Supp. 2006); *see generally* Claudia Kachigian & Alan R. Felthous, *Court Responses to* Tarasoff *Statutes*, 32 J. AM. ACAD. PSYCHIATRY L. 263 (2004) (summarizing state *Tarasoff* statutes and court responses).

[8] *Horne*, 287 So. 2d at 827

> [t]hose states which have enacted a doctor-patient testimonial privilege statute have been almost uniform in allowing a cause of action for unauthorized disclosure. . . In reviewing cases from other states which . . . do not have [such a] privilege, the jurisdictions are split about evenly on this issue . . . the sounder legal position recognizes at least a qualified duty on the part of a doctor not to reveal confidences obtained through the doctor-patient relationship . . . . Only two courts have refused to recognize any duty on the part of the physician not to disclose.

(citing Collins v. Howard, 156 F. Supp. 322 (S.D. Ga. 1957); Quarles v. Sutherland, 389 S.W.2d 249 (Tenn. 1965))).

[9] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,461, 82,462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164); finalized in 45 C.F.R. §§ 160, 164.

[10] Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,333, 8,334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164); finalized in 45 C.F.R. §§ 160, 162, 164.

[11] *See* David G. Wirtes, Jr., R. Edwin Lamberth & Joanna Gomez, *An Important Consequence of HIPAA: No More* Ex Parte *Communications Between Defense Attorneys and Plaintiffs' Treating Physicians*, 27 AM. J. TRIAL. ADVOC. 1, 3 (2003) (citation omitted).

vacy rights"[13] related to the information. Significantly, the standards included an expanded range of disclosures that would be permissible without express patient authorization.[14]

Although covered entities were able to anticipate the burdens and benefits the law would impose on clinical functions, business operations, and research,[15] HIPAA's potential impact on patients could not be as easily predicted. Nor was it clear how such impact, if any, could be elucidated. Although literature exploring dimensions of patient dissatisfaction exists, patients' experiences with the privacy and confidentiality aspects of health care have not been as well-defined or quantified. Study of case law may provide some insight into these experiences but is naturally limited only to circumstances that resulted in lawsuits. We are unaware of any research that has used aggregate data collected over a period of years to specifically examine the extent to which patients express concerns that their privacy is compromised or their medical information is not treated confidentially. In addition, while studies show that Americans worry about the safety of their medical information,[16] we do not know of any research that explores whether regulations controlling the flow of medical information are, themselves, a cause of concern for patients and families.

This Article will describe a study conducted by the Vanderbilt University Center for Patient and Professional Advocacy, which was

---

[12] 45 C.F.R. § 164.

[13] 45 C.F.R. § 164.520(b)(1)(iv).

[14] 45 C.F.R. §§ 164.506, 164.512. 45 C.F.R. § 164.520's requirement that patients are notified of "permitted" disclosures rather than asked to consent to them has been a source of controversy. *See, e.g.,* June Mary Zekan Makdisi, *Commercial Use of Protected Health Information Under HIPAA's Privacy Rule: Reasonable Disclosure or Disguised Marketing*, 82 NEB. L. REV. 741, 754 (2004) (Since patients under 45 C.F.R. § 164.520 have no ability to "negotiate[] by the mechanism of informed consent," "permissible disclosures" allowed under HIPAA must approximate the tradeoff of privacy the participating individuals would have agreed to in exchange for the benefits.).

[15] David Armstrong et al., *Potential Impact of the HIPAA Privacy Rule on Data Collection in a Registry of Patients with Acute Coronary Syndrome*, 165 ARCHIVES INTERNAL MED. 1125, 1125-26 (2005); Steven M. Altschuler & F. Lisa Murtha, *HIPAA and Pediatric Gastroenterology Practice in the United States,* 37 J. PEDIATRIC GASTROENTEROLOGY AND NUTRITION 1, 1 (2003); John Barnard & Debbie Fine, *The HIPAA Privacy Rule and Its Impact on Pediatric Research,* 37 J. PEDIATRIC GASTROENTEROLOGY AND NUTRITION 527, 527 (2003); A.L. Denker, *What HIPAA Means for Your Clinical Practice*, 10 SEMIN NURSE MANAG. 85 (2002); Peter Kilbridge, *The Cost of HIPAA Compliance*, 348 NEW ENG. J. MED. 1423, 1423-2415 (2003); A. Craig Eddy, *A Critical Analysis of Health and Human Services' Proposed Health Privacy Regulations in Light of The Health Insurance Privacy and Accountability Act of 1996*, 9 ANNALS HEALTH L. 1, 5, 60 (2000).

[16] *See* EPICTIDE, INC., *supra* note 1, at 11.

designed to investigate several questions pertaining to privacy and confidentiality in health care. We first asked if patients and their families complain about confidentiality and privacy issues. If so, what issues are they concerned about? We then examined which health care personnel are associated with patient/family concerns. Finally, we asked whether there has been any change in patterns of confidentiality- and privacy-related complaints since institutions implemented the Privacy Rule regulations under HIPAA.

On the basis of this study, we propose a revision of the Privacy Rule. The central problem with the Rule is that, while the regulations authorize and facilitate information sharing among health care providers in a manner that takes cognizance of the complex realities of our modern health care system, it fails to give equal weight to individuals' reasonable expectations of privacy. The effect is to permit health care providers and institutions to tread on patient privacy and confidentiality, rather than protect patients from such invasions.

Part I of this Article reviews concepts of confidentiality and privacy in the health care context under state law and briefly discusses the background of HIPAA. Part II describes the Vanderbilt study, which addresses patient and family perceptions of privacy and confidentiality violations. In Part III, we report our results. Part IV provides a discussion of our findings. In Part V, we propose basic revisions of the HIPAA Privacy and Security Rules and administrative recommendations to address privacy and confidentiality issues in the health care context.

I. BACKGROUND

A. Privacy and Confidentiality in Health Care

The physician-patient relationship has long been imbued with a special ethos of confidentiality. This ethos was set out by Hippocrates in 460 BC: "All that may come to my knowledge in the exercise of my profession . . . which ought not to be spread abroad, I will keep secret and will never reveal."[17] The American Medical Association (AMA) has incorporated confidentiality into its Principles of Medical Ethics. Section IV declares that "[a] physician shall respect the rights of patients . . . and shall safeguard patient confidences . . . within the constraints of the law."[18] The AMA Code of Ethics re-emphasizes that

[17] DORLAND'S ILLUSTRATED MEDICAL DICTIONARY 768 (27th ed., W.B. Saunders Co. 1988) (1900).

[18] American Medical Association, Principles of Medical Ethics,

"the information disclosed to a physician . . . is confidential to the greatest possible degree" but recognizes countervailing "ethically and legally justified" exceptions that also demand consideration.[19]

This ethos of confidentiality derives from privacy interests of the patient.[20] Privacy, generally described as "the right to be let alone,"[21] is linked to autonomy, i.e., the ability to control one's destiny and limit others' physical access to one's person or to information about oneself.[22] Privacy is a complex and multifaceted concept which scholars have struggled to tease apart and break down into its elements. Formulations generally incorporate aspects of privacy related to physical and informational access; proprietary use of likeness or personal identity, personhood (includes notions of dignity and individuality), and constitutionally-protected decision-making about intimate relations[23] are readily recognizable in the health care context. The last

---

http://www.ama-assn.org/ama/pub/category/2512.html (last visited Apr. 9, 2007). Judges may take notice of professional codes of ethics, e.g., the AMA Principles of Medical Ethics and Hippocratic Oath, when determining appropriate conduct for physicians related to privacy and confidentiality. *See* Hammonds v. Aetna Casualty and Surety Co., 243 F. Supp. 793, 797 (N.D. Ohio 1965); Doe v. Roe, 400 N.Y.S.2d 668, 674 (1977); Horne v. Patton, 287 S.2d 824, 832; *see also* Hague v. Williams, 181 A.2d 345, 348-49 (N.J. 1962) (rejecting plaintiffs' assertion that ethical codes for confidentiality create an absolute privilege to extrajudicial disclosures).

[19] Language in the AMA Code of Medical Ethics, in addition to formulating ethical principles for conduct, also incorporates language that tracks legal consensus as it evolves. *See, e.g.*, AMA CODE OF ETHICS, E-5.05 (2004) (paraphrasing the *Tarasoff* decision); AMA CODE OF ETHICS, E-5.059 (referring to current-day realities of healthcare delivery to suggest limits of privacy).

[20] The AMA Code of Medical Ethics distinguishes confidentiality from privacy: "[C]onfidentiality . . . [is] information told in confidence or imparted in secret. However[,] . . . patient privacy . . . encompasses information that is concealed from others outside of the patient-physician relationship." AMA CODE OF ETHICS E-5.059.

[21] WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 802 (4th ed. 1971) (citing COOLEY, TORTS 29 (2d ed. 1888); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)).

[22] Lawrence Gostin et al., *Privacy and Security of Health Information in the Emerging Health Care System*, 5 HEALTH MATRIX 1, 21 (1995) ("To respect the privacy of others is to respect their autonomous wishes not to be accessed in some respect—not to be observed or have information about themselves made available to others."); Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 464 (1987) ("'[P]rivacy refers to conditions of restricted access. This usage is in keeping with the popular theoretical definitions of 'privacy as the inaccessibility of persons, their mental states, and information about them to the senses and surveillance devices of others.").

[23] Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 723-24 (1999); *see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1092, 1116-18 (2002) (critiquing various formulations of privacy, suggesting it may be better understood in the context of activities that cause its disruption); Daniel J. So-

often requires contact with the health care system in order to act on those decisions.[24]

Confidentiality is a distinctive aspect of privacy in that it arises only within a special relationship, such as a physician-patient relationship.[25] While anyone may be liable for invading a person's privacy,[26] only those with information derived from the special confidential relationship have a duty to maintain its confidentiality, i.e., to not share it without the person's permission or in the absence of a compelling reason to do so. Thus, confidentiality protects informational privacy interests by requiring recipients of information deemed confidential to restrict access to that information.[27]

While the professional ethos of confidentiality is well-established, the rights-based interests that underlie that ethos generate a demand for legal protection as well. The traditional approach has been to recognize a common law cause of action for invasion of privacy. Of the four branches of this tort identified by William Prosser[28]—intrusion, publicity of private facts, false light, and appropriation—the first two would appear to hold the most promise for protecting privacy rights in the health care context.

Common law has proved to be a flexible means of addressing privacy issues in health care but has left important gaps that ultimately led to federal legislation. The intrusion element of the privacy tort generally refers to a physical invasion of a person's privacy, i.e., into a private space or matter in which the person would have a reasonable expectation of privacy.[29] In the classic medical intrusion cases, plaintiffs discover that third parties present at the time of their care were not medical personnel.[30] The perceived offense arises from expecta-

---

love, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477 (2006) (developing categories of privacy disruptions, including aggregation, identification, secondary use, exclusion, breach of confidentiality, exposure, increased accessibility, intrusion).

[24] Allen, *supra* note 22, at 466.

[25] *E.g.,* Gostin et al., *supra* note 22, at 3.

[26] *See* Judy Zelin, Annotation, *Physician's Tort Liability for Unauthorized Disclosure of Confidential Information About Patient,* 48 A.L.R. 4TH 668, 679 (1986) (citing Humphers v. First Interstate Bank, 696 P.2d 527, 530 (plaintiff could proceed against physician's estate under a breach of confidentiality claim but not an invasion of privacy claim)). *Cf.,* Horne v. Patton, 287 S.2d 824, 830-32 (1973) (allowing claims for both breach of confidentiality and invasion of privacy to go forward).

[27] Allen, *supra* note 22, at 464-65 (describing confidentiality as one type of "information nondisclosure," restricting access to the person).

[28] PROSSER, *supra* note 21, at 804-14.

[29] W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 854-55 (W. Page Keeton ed., 5th ed. 1984)..

[30] *See* De May v. Roberts, 9 N.W. 146 (Mich. 1881) (holding intrusion where non-professional party was present during medical care without the patient's consent);

tions unique to the medical context. The expectations are not that information about one's medical problem won't be known or that one's intimate anatomy will not be physically exposed to others. Rather, it is that a patient expects that anyone who learns about medical problems or views intimate anatomy will be someone who must have that information in order to help. In other words, to the extent necessary for self-benefit, the patient consents to expose physical and medical information to direct care health care personnel but to no others.

Other examples of common intrusions in daily medical encounters may be easily imagined: ancillary health care workers learn of medical details beyond their need to know; partially disrobed patients are placed on stretchers in hallways or behind half-drawn curtains; open patient charts are inadvertently left on nursing station countertops and are able to be read by others. But legal cases of this sort are virtually non-existent. In many cases, patients may not find out about such occurrences or, where they are aware, may consider the type of privacy such occurrences invade to be one they already expect to be compromised in the course of competent medical care. Even if they believe that "this shouldn't happen," patients are not likely to litigate the more mundane intrusions.

The "publicity of private facts" tort seems like it should be a natural fit for unauthorized disclosures of medical information, but most cases fail if its elements are strictly applied. The requirements that the private information is "of no legitimate public interest"[31] and that its disclosure would be "highly offensive" and likely to cause serious mental injury to a reasonable person of "ordinary sensibilities"[32] may be satisfied in many situations, but the broad dissemination[33] requirement poses an obstacle.

Courts often struggle to determine how many persons must have learned of the private facts before reaching the threshold for liability.[34]

Sanchez-Scott v. Alza Pharmaceuticals, 86 Cal.App.4th 365, 368 (2001) (presence of a drug salesman during breast examination by oncologist constituted an intrusion that is "highly offensive to a reasonable person").

[31] DAVID A. ELDER, PRIVACY TORTS § 3.5 (2002).

[32] *Id.* at § 3.6.

[33] *See, e.g.*, Vassiliades v. Garfinckel's, 492 A.2d 580, 585 (D.C. 1985) (finding tortious public disclosure of private facts and breach of fiduciary duty by a plastic surgeon for showing "before" and "after" photos in a shopping mall and on television without attempting to disguise or cover up her identity).

[34] *See* Wayne v. Genesis Med. Ctr., 140 F.3d 1145, 1147, 1149 (8th Cir. 1998) (affirming district court's decision that appellant "failed to demonstrate widespread publicity" when six defendant physicians discussed private facts about her surgery); Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 378 (Colo. 1997) (finding no specific number of persons constitutes a threshold for "publicity" but rather that

They generally find that publication to one or two persons is not sufficient.[35] While there appears to be a trend towards lowering the number of persons required to constitute a "public,"[36] it is rare for courts to find an invasion of privacy for unauthorized disclosure to only one person.[37] Standards generally applicable to irresponsible journalists or gossips are not adequate to protect the privacy of patients for whom the unauthorized disclosure is more commonly made to a very limited audience.

In the medical context, denying a remedy on grounds that a disclosure is not public enough does not adequately take into account the unique nature of medical information or the structure of the encounter in which it is learned. While "private" information is commonly known by an intimate or small circle close to an individual, medical information is often much more sensitive. Medical information involves matters that often would not readily be known by any third party, even friends or intimate relations, absent disclosure by the patient himself. Details about bodily functions, concerns about sexual functioning or sexuality, a history of substance abuse, and battles with troubled thoughts are beyond the commonplace private sphere. Disclosing a highly sensitive private fact without authorization to even one person would then make it "public." Revelation of a diagnosis or prognosis to even a very limited audience may place people at risk of social isolation and very real, albeit illegal, discrimination. Furthermore, sharing medical information with third parties without authorization from the patient assaults an individual's dignity and may be wrongful even in the absence of proof of further damages.[38]

---

the "facts and circumstances of a particular case must be taken into consideration in determining whether the disclosure was sufficiently public so as to support a claim for invasion of privacy"); Briscoe v. Reader's Digest Ass'n, Inc., 4 Cal. 3d 529, 534 (1971) (at stake in the public disclosure tort is the right to define one's circle of intimacy).

[35] *See, e.g.*, McCormick v. England, 494 S.E.2d 431, 438 (S.C. Ct. App. 1997) (citing Rycroft v. Gaddy, 314 S.E.2d 39 (S.C. Ct. App. 1984)) (finding that "[p]ublicity involves disclosure to the public, not just an individual or a small group"; case brought by patient-plaintiff against physician who had provided a letter to divorcing husband that described her medical conditions).

[36] *See* ELDER, *supra* note 31, at § 3.3 (citing Kinsey v. Macur, 107 Cal.App.3d 265, 272 (1980), which held that disclosure of information to twenty or so people was publicity).

[37] *See* ELDER, *supra* note 31, at § 3.3 (discussing holding of McSurely v. McClellan, 753 F.2d 88, 112, 112-13 (cert. denied, 474 U.S. 1005 (1985)), which found the disclosure of an affair to one person, if that person is in a special relationship with the subject of the disclosure, satisfies the requirement of a "public" under the public disclosure of private facts tort).

[38] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L.

Some jurisdictions have attempted to remedy shortcomings of the disclosure tort by recognizing that strict construction of the "publicity" requirement creates an injustice. This gap in the common law has partially been filled by a separate tort, generally designated "breach of confidentiality." Courts which recognize this claim may hold physicians or other health professionals accountable for unauthorized disclosure of private information to even a single individual.[39] This cause of action may be based on common law duties, e.g., the fiduciary relationship or an implied contract not to disclose.[40] In other jurisdictions, similar standards have been established by statute—e.g., confidentiality statutes, privilege statutes, statutes governing professional behavior and licensing[41]—or the state constitution.[42]

While common law breach of confidentiality actions resolve the problems that inhere in the broad dissemination requirement of the publicity clause, they often suffer from other limitations. Confidentiality actions do not lie directly against others not owing the same duty

---

REV. 193, 213 (1890) ("If the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.").

[39] *McCormick*, 494 S.E.2d at 439 (recognizing the tort of breach of confidentiality); *see generally* Alan B. Vickery. *Breach of Confidence: An Emerging Tort*, 82 COLUMB.L.REV. 1426 (1982).

[40] *See* Doe v. Roe, 400 N.Y.S.2d 668, 674 (1977) ("the implied covenant not to disclose whose breach is a contractual violation"); Alexander v. Knight, 25 Pa. D. & C. 2d 649, 655 (C.P. Ct. Phila. County 1957), *aff'd per curiam*, 197 Pa. Super. 79 (Pa. Super. Ct. 1962) ("members of a profession, especially the medical profession, stand in confidential or fiduciary capacity as to their patients"); MacDonald v. Clinger, 446 N.Y.S.2d 801, 805 (N.Y. App. Div. 1982) (court found disclosure by psychiatrist of intimate details revealed to him by his patient to his patient's wife breached the fiduciary duty of confidentiality) *but see* Curry v. Corn, 277 N.Y.S.2d 470,471 (N.Y. Sup. Ct. 1966) (physician not liable for revealing to patient's husband information obtained in the course of her treatment).

[41] *See generally* Health Privacy Project, View the Summary of a Specific State, http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat_list.htm (last visited Mar. 29, 2007) (summarizing each state's medical privacy and confidentiality of medical information laws). Some statutes provide that unauthorized disclosure of confidential medical information may be grounds for discipline by a medical board. *See, e.g.*, CAL. BUS. & PROF. CODE § 2263 (West 2003); TENN. CODE ANN. § 63-6-214(b) (2004 & Supp. 2006). The *Tarasoff* decision has been codified in several states. *See, e.g.*, CAL. CIV. CODE § 43.92 (West Supp. 2007); CAL. EVID. CODE §1024 (West 1995 & Supp. 2007) (stating an exception to the general psychotherapist-patient privilege when the patient poses a serious threat of physical violence to himself or others); TENN. CODE ANN. §§ 33-3-206 to -207 (2001 & Supp. 2006). *See generally* Claudia Kachigian & Alan R. Felthous, *Court Responses to* Tarasoff *Statutes*, 32 J. AM. ACAD. PSYCHIATRY L. 263 (2004) (summarizing state *Tarasoff* statutes and court responses).

[42] CAL. CONST, art. I. § 1.

to patients as physicians.[43] Except where duties of confidentiality are directly established by statute,[44] courts have invoked the relationship to the physician to find liability for breached confidentiality when other employees are involved.[45] Under this theory, courts have found liability where the employee was determined to be acting as the agent of the physician and within the scope of his/her employment.[46]

In the past, few people other than physicians were in a position to harm a patient's interest in his/her medical information. Parties not under physicians' direct supervision were not likely to have access to medical or related financial records, for physicians were the de facto custodian of medical records, and payment did not involve a third party. Today, medical care requires interaction and coordination among many individuals and services.[47] Aspects of care are often delegated or first undertaken by licensed, or even unlicensed, care providers other than physicians. Information is obtained, coded, and processed by employees of the physician or health care system, maintained in paper or electronic form, and transmitted to third party payors. The expanding number of those whose jobs provide them with access to medical information increases the risk that individuals will

---

[43] *See, e.g.*, Knecht v. Vandalia Med. Ctr., Inc., 470 N.E.2d 230, 232-33 (Ohio Ct. App. 1984) (secretary-receptionist's comments to her son at home based on information from hospital record were not within her scope of employment).

[44] *See, e.g.*, Eckhardt v. Charter Hosp., 953 P.2d 722, 727-29 (N.M. App. 1997) (discussing that the New Mexico legislature made it clear through "professional licensing statutes, rules of evidence, and [the] state constitution" that "the duty to safeguard patient confidences extends to therapists and social workers.").

[45] *See, e.g.*, Hobbs v. Lopez, 645 N.E.2d 1261, 1263 (Ohio Ct. App. 1994) (holding a doctor and corporate employer liable for disclosure of confidential information by a nurse acting as the doctor's agent).

[46] Health care entities may assume a duty of confidentiality in reference to medical information by federal or state statute, 210 ILL. COMP. STAT. ANN. 85/6.17(b) (West 2007) (patient's medical information must be protected from inappropriate disclosure), and on behalf of their employees within the scope of their employment, under theories of *respondeat superior* or vicarious liability, Bagent v. Blessing Care Corp., 844 N.E.2d 469, 474-75 (Ill. App. Ct. 2006) (holding the hospital's liability under *respondeat superior* would not be "obviated" when an off-duty hospital employee trained by a hospital to hold medical information confidential fails to maintain confidentiality at "all times and all places"); *see also* Ruth Purtilo & James Sorrell, *The Ethical Dilemmas of a Rural Physician,* 16 HASTINGS CTR. REP., Aug. 1986, at 25 (special challenges arise in a rural community, e.g., physician may choose to not document sensitive medical information recognizing patient's social or familial relationships with other office staff; physicians find it hard to maintain confidentiality "when everybody knows everybody").

[47] *See* Gostin, *supra* note 22, at 2 ("All participants . . . (consumers and patients, health plans, and federal and state regulatory authorities) . . . need access to high quality information for informed decision making.").

act outside the scope of authorization to obtain information they do not legitimately need to perform their work.

The electronic health information systems, in particular, that have proliferated in the past ten to twenty years may be particularly vulnerable to improper or abusive dissemination of health and related personal information, including risk of appropriation of critical unique identifiers and financial information. Vast quantities of medical and other personal information are now stored in cyberspace. This information can be accessed by large numbers of health care workers, both physicians and non-physicians, and transferred in a matter of nanoseconds, posing the risk of inappropriate intrusion into highly sensitive private information.

Courts have extended the common law to provide recourse against employer institutions for plaintiffs claiming injury to privacy interests. Institutions may be held liable for invasions of privacy under theories of respondeat superior, vicarious liability, ostensible agency, and enterprise liability for their employees' or affiliates' acts if private information derived from the medical setting becomes "public" in any sense of the word, i.e., becomes known to those who should not know or is made available for use by others who should not have access to it. Institutions may also be held liable for employees' breaches of confidentiality in jurisdictions with statutory law binding HMOs, other medical corporations, and health and mental health professionals to disclosure rules governing physician-patient relationships.[48]

The appropriation branch of the invasion of privacy tort may also have modern applicability. This tort includes circumstances where a defendant "pirates" a plaintiff's identity (name or likeness) for the purpose of benefit or advantage, such as obtaining credit.[49] Because the unique identifiers developed for conducting financial transactions and taking care of patients are valuable and marketable, appropriating patients' medical identity has become an increasing threat to proprietary privacy interests.[50] Stealing medical identity can cause serious

---

[48] *See, e.g.*, Doe v. Cmty. Health Plan-Kaiser Corp., 268 App.Div.2d 183, 186-87 (N.Y. App. Div. 2000) (holding that New York statutory law binds HMOs, other medical corporations, and health and mental health professionals to disclosure rules governing physician-patient relationships and creates an actionable duty of confidentiality in the common law). Concerns regarding this holding include (1) creating strict liability for corporations for their employees' actions, and (2) "the wisdom of having [a] . . . court create a new legal remedy every time it discovers an unserved need." *Id.* at 188, 190 (Mercure, J., dissenting).

[49] PROSSER, *supra* note 21, at 804-05 (citing Goodyear Tire & Rubber Co. v. Vandergriff, 184 S.E. 452 (Ga. Ct. App. 1936)).

[50] *See* Allen, *supra*, note 23 at 723-24 (discussing "control over names, likenesses and repositories of personal information").

harm to the victim, as inaccuracies in medical records create safety, as well as financial, threats to individuals.[51]

In sum, most of the law related to confidentiality and privacy in health care prior to HIPAA was reactive, not proactive, and tested the boundaries of permissible disclosure on a case by case basis. The doctrines courts developed to protect patients' privacy interests are a testament to the strengths of the common law approach, but the variability and uncertainty of the resulting rules are an emblem of the common law's weaknesses. In the absence of clear guidelines for many situations, difficult to enforce professional ethical standards provided patients' primary protection from unauthorized disclosures. As risks to privacy in the current health care delivery system have become ubiquitous, it is clear that it can be assured only if continuously guarded and routinely observed. Through HIPAA, the federal government has attempted to create safeguards and routine by establishing security standards for electronic transmissions and defining the limits of authority for disclosure in the privacy standards.

B. HIPAA—Patient Rights and Provider Requirements

HIPAA amended the Internal Revenue Code of 1986[52] and Title XI 42 U.S.C. 1301 et seq, Social Security Subchapter XI Part C.[53] The preamble to HIPAA states that the statute is intended "to combat waste, fraud, and abuse in health insurance and health care delivery" and "simplify the administration of health insurance."[54] Subtitle F sought to improve delivery of care under the Medicare and Medicaid programs by establishing "standards and requirements for the electronic transmission of certain health information" needed to develop a "health information system."[55] HIPAA assigns to covered entities[56] a duty to maintain "administrative, technical, and physical safeguards of health information" to preserve its "integrity and confidentiality."[57]

The statute assigned enforcement of Subtitle F to the Department of Health and Human Services (HHS), which proceeded to establish

---

[51] *See generally* PAM DIXON, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU (2006), *available at* http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.

[52] HIPAA pmbl.

[53] 45 C.F.R. § 160.101 (2003) (implementing sections 1171 through 1179 of the Social Security Act).

[54] HIPAA pmbl.

[55] HIPAA § 261.

[56] *See* OFFICE FOR CIVIL RIGHTS, OCR GUIDANCE EXPLAINING SIGNIFICANT ASPECTS OF THE PRIVACY RULE, *supra* note 3, at 41-42.

[57] HIPAA § 1173(d)(2)(A).

standards for the storage and transmission of electronic health data. In carrying out this task, however, HHS officials realized that not only did health care, as an industry, lack standards for adequate storage and transmission of electronic health data,[58] but there were very few prevailing laws or rules that could adequately protect such data.[59] Recognizing the importance of securing the public's confidence[60] in both the privacy and security of health data, HHS promulgated a set of uniform Privacy and Security Rules to establish minimum requirements for appropriate use and protection of health information.[61] Thus, the HIPAA regulations are not the result of a direct Congressional statutory command but arise from a fairly broad interpretation of the statute by the implementing agency.

---

[58] *See* Health Insurance Reform: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organizations, 65 Fed. Reg. 50,312, 50,352 (Aug. 17, 2000) (to be codified at 45 C.F.R. pts. 160, 162) ("[I]t is important to understand current industry practices. . . . A 1993 study . . . estimated that administrative costs comprised 17 percent of total health expenditures. Paperwork inefficiencies are a component of those costs, as are the inefficiencies caused by the more than 400 different data transmission formats currently in use.").

[59] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,764-65 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160, 164) (discussing lack of comprehensive legislation in most states on matters of privacy in health care; most states regulate privacy for only specific areas of health care, e.g., for stigmatizing conditions); *see also* Privacilla.org, HIPAA and the Privacy Torts, http://www.privacilla.org/business/medical/hipaatort.html (last visited Mar. 27, 2007).

[60] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,776; University of Miami: Miller School of Medicine, Privacy/Data Protection Project, http://privacy.med.miami.edu/glossary/xd_admin_simplification.htm (last visited Apr. 2, 2007); Health Insurance Reform: Standards for Electronic Transactions; Announcement of Designated Standard Maintenance Organizations, 65 Fed. Reg. at 50,351 ("As discussed in the proposals, the regulations will provide a consistent and efficient set of rules for the handling and protection of health information. . . . [T]he promulgation of a final privacy standard will enhance public confidence that highly personal and sensitive information is being properly protected, and therefore, it will enhance the public acceptance of increased use of electronic systems. Collectively, the standards that will be promulgated under Title II can be expected to accelerate the growth of electronic transactions and information exchange in health care."); Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. at 82,464 (discussing the "Need for a National Privacy Framework," commenting on the importance of medical privacy, the public's concerns about privacy and the risk of unauthorized dissemination of genetic information, and the impact of interconnected electronic information systems); *see also* Makdisi, *supra* note 14, at 757-58 (stating that the success of federal health care programs hinged on the inclusion of privacy provisions).

[61] *See* 45 C.F.R § 160.203.

The Privacy Rule went into effect October 15, 2002, with a final compliance date of April 14, 2003 for subject health care organizations.[62] In brief, permissible disclosures of "protected health information"[63] fall into two categories, those requiring patient authorization[64] and those not requiring patient authorization.[65] While patient authorization, in general, is required for use or disclosure of health information, the Privacy Rule does not require express patient authorization when made directly to patients or their representatives, when made in the course of treatment, payment, or health care operations, or when made in the public interest. If disclosures are made incidental to an authorized disclosure, they are allowable if "reasonable safeguards" were employed, if the "minimum necessary" was disclosed, and if the institution has policies in place to limit access to protected health information on a "need to know" basis.[66] Patients have the right to an accounting of how their medical information has been shared without their written consent, but institutions may exclude from the accounting all uses or disclosures permitted under the regulations.[67] Patients also have the right to request an amendment to their medical record to counter or clarify information contained within that record.[68] Institutions and providers must inform patients with whom they may file complaints about "HIPAA violations."[69] The regulations authorize covered entities to conduct a broad range of required and permissible

---

[62] 45 C.F.R. § 164.534. "Small health plans" were the only covered entities with a later final compliance date of April 14, 2004. *See also* DHHS Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,249 (Aug. 14, 2002); *cf.* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8,333 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164) (HIPAA's Security Rule requiring adherence with electronic security standards went into effect April 21, 2003 with final compliance dates of April 21, 2005 for most covered entities and April 21, 2006 for small health plans).

[63] 45 C.F.R. § 160.103 ("*Protected Health Information* means individually identifiable health information.").

[64] 45 C.F.R. § 164.508.

[65] 45 C.F.R. §§ 164.506, 164.512.

[66] 45 C.F.R. § 164.502(a)(1)(iii). The Office for Civil Rights provides guidance for incidental uses and disclosures. *See* OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 3, at 5-7.

[67] 45 C.F.R. § 164.528(a)(1) (excluding from accounting uses or disclosures that are related to treatment, payment, and health care operations; incidental to a use or disclosure that is otherwise permitted; previously authorized; for a facility directory; made to families, relatives, or friends involved in patient's care or those involved in payment; or to national security or law enforcement entities).

[68] 45 C.F.R. § 164.526(a) (stating the "right to amend").

[69] 45 C.F.R. § 164.520 (b)(1)(vi) (stating the requirements regarding complaint procedures).

uses and disclosures of protected health information, consistent with HHS's intent to permit "flexibility"[70] to meet their needs.

HIPAA outlines administrative, civil, and criminal penalties for violations of its standards and is enforced by the HHS Office of Civil Rights.[71] HIPAA preempts state law unless the latter is more restrictive than the HIPAA regulations.[72] Although HIPAA does not provide

---

[70] *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,208-09 (Aug. 14, 2002) (to be codified at 45 C.F.R. pt. 160, 164) ("In developing the Privacy Rule, the Department balanced the privacy implications of uses and disclosures for treatment, payment, and health care operations and the need for these core activities to continue. . . [T]he Department's goal is, and has always been, to permit these activities to occur with little or no restriction.").

[71] In the absence of knowing intent to obtain or use individually-identifiable health information in violation of Part C-Administrative Simplification, covered entities face monetary penalties for HIPAA violations. *See* HIPAA § 1176(a) (outlining civil penalties for violating sections of part C). Intentional violation of HIPAA may result in substantial monetary fines as well as criminal sanctions. *See* HIPAA § 1177 (outlining criminal penalties for anyone who knowingly misuses a unique health identifier or obtains or discloses individually-identifiable health information (IIHI)); *see also* HIPAA § 1177; John A. Cogan, Jr., *First-Ever HIPAA Conviction Highlights Differing Views of HIPAA's Civil and Criminal Penalties*, 88 MED. HEALTH R.I. 33, 33-34 (2005), *available at* http://www.health.ri.gov/publications/medhealthri/January05RIMed.pdf; *but see* Heather Hayes, *More Privacy Concerns Are Not Investigated*, GOVERNMENT HEALTH IT, Dec. 18, 2006, http://govhealthit.com/article97136-12-18-06-Web (finding that only one-fourth of more than 23,000 complaints to OCR about alleged HIPAA violations have been investigated); Doreen Z. McQuarrie, *HIPAA Criminal Prosecutions: Few and Far Between*, HEALTH L. PERSP., Feb. 19, 2007, http://www.law.uh.edu/healthlaw/perspectives/2007/(DM)HIPAACrimCharges.pdf (Of the complaints sent to OCR, 366 have been sent to the Department of Justice for enforcement. The Department of Justice has prosecuted only four individuals for criminal offenses under HIPAA, all involving theft of individually identifiable health information for the purpose of financial gain. Author expresses concern that the Office of Legal Counsel of the Department of Justice issued a Memorandum Opinion that puts into question whether "rank and file" employees are subject to criminal sanctions.).

[72] *See* Health Insurance Reform: Standards for Electronic Transactions, 65 Fed. Reg. 50,313; HIPAA Administrative Requirements, 45 C.F.R. §§ 160, 162, 164 (2003); 45 C.F.R. § 160.202 ("*More stringent* means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, 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 this subchapter."); 45 C.F.R. § 160.203; *see also* Giangiulio v. Ingalls Mem'l Hosp., 850 N.E.2d 249, 264 (Ill. App. Ct. 2006) ("HIPAA contains a preemption provision that generally supersedes contrary state law provisions. . . . However, HIPAA does not preempt state laws that are more stringent."); Grace Ko, Note, *Partial Preemption Under the Health Insurance Portability and Accountability Act*, 79 S. CAL. L. REV. 497 (2006) (discussing the issues surrounding HIPAA and state privacy laws).

for a private cause of action,[73] its regulations have been used to provide evidence of standards in state tort actions.[74] Because HIPAA places an affirmative duty on employers to properly train their employees,[75] employees' failure to comply may lend support to plaintiffs' invasion of privacy or breach of confidentiality claims against employers. On the other hand, the scope of permissible disclosures includes an express allowance for incidental disclosures—subject only to judgments that they entailed the "minimum necessary" and that "reasonable safeguards" were employed—and provides a refuge for defendants describing business necessities.

While HIPAA may have provided an impetus for institutions to proactively develop and implement policies and procedures to ensure that health-related information is handled in a consistent and predictable manner, underlying questions remain: Do the regulations successfully establish the correct standards for covered entities to follow? If they do, do institutions properly interpret, apply, and enforce them? The study discussed in this Article may shed some light on these issues.

II. A STUDY OF PRIVACY-RELATED PATIENT COMPLAINTS

The authors conducted a study at the Vanderbilt University Center for Patient and Professional Advocacy to address the following: Do patients and/or their families complain about confidentiality and privacy issues? If so, what specific issues do they complain about? Which health care personnel do they associate with their concerns? Has there been any change in patterns of confidentiality- and privacy-

---

[73] *See, e.g.*, Bagent v. Blessing Care Corp., 844 N.E.2d 469, 472 (Ill. App. Ct. 2006) (citing Univ. of Colo. Hosp. Auth. v. Denver Publ'g Co., 340 F.Supp.2d 1142, 1145 (D.Colo.2004)).

[74] *See, e.g.*, Acosta v. Byrum, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006) ("[P]laintiff cites to HIPAA as evidence of the appropriate standard of care, a necessary element of negligence. Since plaintiff made no HIPAA claim, HIPAA is inapplicable beyond providing evidence of the duty of care owed by [the doctor] with regards to the privacy of plaintiff's medical records."); *see also* Francoise Gilbert, *Emerging Issues in Global AIDS Policy: Preserving Privacy*, 25 WHITTIER L. REV. 273, 297 (2003) (stating that HIPAA could be used to establish standards of performance for covered entities regarding the use or disclosure of medical information through private actions (citing Cal. Civ. Code Ann. § 1798.53 (providing for special and general damages for invasion of privacy by intentional disclosure of information from a state or federal "system of records" as defined in the Federal Privacy Act of 1974, 5 U.S.C. 552(a) (2006)))).

[75] 45 C.F.R. §§ 164.308(a)(5)(i), 164.530(a)(2) (regarding security awareness and training).

related complaints (hereinafter, "privacy-related complaints") since institutions implemented HIPAA's Privacy Rule? Utilizing a database of coded patient complaints previously filed with offices of patient affairs at three geographically distant academic medical institutions, we developed a methodology to extract privacy-related complaints from the patient/family complaint report files and then developed a classification system into which they could be sorted. Finally, because HIPAA and its implementing regulations represent a major transformation of the law governing privacy in the medical context and handling of health care information, we analyzed the data to compare patterns of privacy-related complaints before and after final implementation with HIPAA's Privacy Rule.

A. The Value of Patient Complaints

Several studies have looked into "naming, blaming, claiming" behavior of consumers, including that of health care recipients.[76] Prior research has demonstrated the value of unsolicited patient or family complaint data as an indicator for patient dissatisfaction[77] and that physicians who generate high levels of patient dissatisfaction are at disproportionate risk of malpractice claims.[78] In prior small studies,

---

[76] U.S. OFFICE OF CONSUMER AFFAIRS, CONSUMER COMPLAINT HANDLING IN AMERICA: AN UPDATED STUDY, PART II (1986); *Id*, Executive Summary; ARTHUR BEST, WHEN CONSUMERS COMPLAIN, 57-59 (1981); Arthur Best & Alan R. Andreasen, *Consumer Response to Unsatisfactory Purchases: A Survey of Perceiving Defects, Voicing Complaints, and Obtaining Redress*, 11 LAW & SOC'Y REV. 701, 705, 711, 715-17, 726, 738 (1977); *see generally* William L.F. Felstiner et al., *The Emergence and Transformation of Disputes: Naming, Blaming, Claiming*, 15 LAW & SOC'Y REV. 631 (1981); *see* Marlynn L. May & Daniel B. Stengel, *Who Sues Their Doctors? How Patients Handle Medical Grievances*, 24 LAW & SOC'Y REV. 105, 118 (1990) (discussing the results of a study examining the dispute resolution method of choice between patients and doctors); *see generally* Charles Vincent et al., *Why Do People Sue Doctors? A Study of Patients and Relatives Taking Legal Action*, 343 LANCET 1609 (1994) (examining why patients and their relatives bring malpractice suits).

[77] *See, e.g.*, Gerald B. Hickson et al., *Obstetricians' Prior Malpractice Experience and Patients' Satisfaction with Care*, 272 JAMA 1583, 1583 (1994); Kecia N. Carroll et al., *Characteristics of Families that Complain Following Pediatric Emergency Visits*, 5 AMBULATORY PEDIATRICS 326, 326 (2005).

[78] *See* Gerald B. Hickson et al., *Patient Complaints and Malpractice Risk*, 287 JAMA 2951, 2951 (2002); *see* James W. Pichert et al., *Identifying Medical Center Units with Disproportionate Shares of Patient Complaints*, 25 JOINT COMMISSION J. QUALITY IMPROVEMENT 288, 289 (1999); Ilene N. Moore et al., *Rethinking Peer Review: Detecting and Addressing Medical Malpractice Claims Risk*, 59 VAND. L. REV. 1175, 1197-99 (2006).

patient complaints have included allegations of breached confidentiality or failure to respect patients' dignity.[79]

Patients' confidentiality and privacy concerns are not only a major factor in determining their sense of subjective satisfaction but are also a factor in affecting the quality of their medical care. Patients may withhold information from providers if they do not trust that it will be kept confidential. If patients share incomplete information, physicians' ability to render optimal care may be compromised.[80] In addition, dissatisfied patients more frequently fail to adhere to prescribed therapeutic regimens or drop out from care altogether.[81] If patients observe that a health care setting or worker's demeanor does not reflect respect for their needs, they may have reason to fear that medical information will be inappropriately discussed or disseminated.[82]

In order to address patient and family dissatisfaction, medical institutions frequently establish an office of patient affairs. The offices are given various titles such as Ombudspersons, Patient Relations, and

---

[79] *See* Sally Lloyd-Bostock & Linda Mulcahy, *The Social Psychology of Making and Responding to Hospital Complaints: An Account Model of Complaint Processes,* LAW & POL'Y, 123, 129 (1994) (analysis of 399 formal complaints yielded 713 allegations that included issues of confidentiality (0.4 percent), behavior and attitude (12.8 percent), discrimination (0.3 percent), and not respecting requests about treatment of a corpse (0.3 percent)); *see also* Hickson et al., *supra* note 77, at 1585-87. In a study of non-suing patients' complaints about their physicians, physicians were sorted by malpractice claims history. The patients of those with the highest frequency of claims were three times more likely to complain regarding the human aspects of the care, which indicates a perceived lack of concern or respect for the patient. *Id.*

[80] *See* Lloyd-Bostock & Mulcahy, *supra* note 79, at 138.

[81] Sheryle Whitcher-Alagna, *Receiving Medical Help: A Psychosocial Perspective on Patient Reactions, in* 3 NEW DIRECTIONS IN HELPING: APPLIED PERSPECTIVES ON HELP-SEEKING AND -RECEIVING 131, 135-36, 140 (Arie Nadler et al. eds., 1983) (discussing studies demonstrating that dissatisfied patients more likely are noncompliant, fail to keep appointments, drop out of treatment, reject physician recommendations, or turn to non-medical healers); MARIE HAUG & BEBE LAVIN, CONSUMERISM IN MEDICINE: CHALLENGING PHYSICIAN AUTHORITY 25 (1983) ("[T]he compliance concept is based on assumptions about the doctor-patient relationship that are not congruent with a consumerist perspective. . . . The doctor may not communicate effectively, . . . failing to hear or take into account what the patient is trying to say."); Dana Gelb Safran et al., *Switching Doctors: Predictors of Voluntary Disenrollment from a Primary Physician's Practice,* 50 J. FAM. PRAC. 130, 132-33 (2001) (noting that with increasing patient dissatisfaction, voluntary disenrollment from the physician's practice increases).

[82] David Barlas et al., *Comparison of the Auditory and Visual Privacy of Emergency Department Treatment Areas with Curtains Versus Those with Solid Walls,* 38 ANNALS EMERG. MED. 135, 137 (2001) (some patients stated they "probably" or "definitely" withheld part of their medical history because of privacy concerns).

Patient Assistance. Because patients or surrogate family members (hereinafter, "patients") frequently lodge complaints against individual health care workers or discuss other concerns related to their medical care experiences, patient affairs personnel play key roles in service recovery. They listen to patients and record patient concerns in complaint report summaries, documenting, when possible, the identification of associated individuals and units. Where appropriate, patient affairs staff may initiate fact-finding on behalf of complainants and provide follow-up communication.[83] Patient affairs staff help other personnel, including physicians, develop action plans to address patient-related issues and mediate among involved parties to clear up miscommunications and misunderstandings.

Since the mid-1990s, the Center for Patient and Professional Advocacy has worked with growing numbers of patient affairs departments from a diverse group of U.S. medical centers to collect and analyze patient complaints in the Patient Advocates Reporting System.[84] Coders review and extract all individual complaints contained within the complaint reports, sorting them among six broad categories (physician communication, physician concern for patient, care and treatment, access and availability, environment, and billing) and thirty-five subcategories.[85] Each report may contain multiple complaints—for example, the same patient may complain about parking, a rude staff member, and a hospital bill—all of which are coded and entered into a central database.

---

[83] As of September 9, 2005, the Centers for Medicare and Medicaid Services (CMS) has mandated that several categories of patient complaints be handled as grievances. Health care institutions are required to adopt policy and procedures that ensure that patients are informed of contact persons to whom they may communicate their concerns both within the institution and the pertinent state agencies. *See* Ctrs. for Medicare and Medicaid Services, 42 C.F.R. § 482.13 (2000), Medicare and Medicaid Programs; Hospital
Conditions of Participation Patients' Rights; Interim Final Rule, *available at* http://www.cms.hhs.gov/transmittals/downloads/R17SOM.pdf.

[84] Relationships governed by Business Affiliate Agreements (BAAs) in compliance with HIPAA and institutional peer review and/or quality improvement statutes under state law.

[85] Gerald B. Hickson et al., *Development of an Early Identification and Response Model of Malpractice Prevention* 60 L. & CONTEMP. PROBS. 7, 13-14 (1997).

B. Methods

1. Study Sites

The study used data originating at three geographically distant academic medical centers in the U.S. The data included complaints from patients in inpatient, outpatient, and emergency department settings. Approval for the project was obtained from each center's Institutional Review Board or Committee for the Protection of Human Subjects.

2. Data Source and Coding System

We searched the PARS[SM] complaint database to extract a subset of complaints that involved privacy or confidentiality concerns and to develop a taxonomy for classifying sub-types of these complaints. We then used an iterative process to inspect the complaints, sort them into different types, and assign categories. The coding scheme development consisted of two phases. First, we reviewed sample complaint phrases from one hundred complete complaint narratives. Coding categories were created by grouping similar complaints together and then creating complaint categories. To ensure that the developed coding scheme was reliable, the coding scheme was taught to a second individual who classified the complaint phrases. The coding scheme was then modified to ensure reliable coding. Seven general categories and eighteen subcategories ultimately emerged. Coders made no judgment as to the accuracy of patient assertions or the interpretation of events underlying the complaints.

To test inter-rater reliability, two coders independently coded identical sets of reports, making five judgments about each complaint: type of "violation/burden," type of protected health information involved, whether complainant found behavior offensive, whether HIPAA was mentioned, and who was complained about. Kappa statistics for measuring inter-rater reliability for the five judgments were 0.88, 0.75, 1.0, 0.88, and 0.81, respectively. Values demonstrate good agreement between coders.

3. Study Periods

April 14, 2003 was the final date for covered entities to comply with the HIPAA Privacy Rule.[86] The first observation period covered the three years before (April 1, 2000–March 31, 2003), and the second

[86] 45 C.F.R. § 164.500 *et seq.* (2006).

observation period covered the two years after (May 1, 2003–April 30, 2005). Durations of the observation periods differed for two reasons. The first was our desire to include as much data as possible and correct for the different durations statistically. The second reason was that if there were fewer privacy-related complaints in the first observation period, lengthening the duration of the observation period would likely yield more observable and reliable data.

4. Statistical Analysis

Descriptive statistics using means, proportions, and differences are presented. Chi-square tests were used to assess the shift in complaint distributions between two observation periods, across different complaint categories, and different personnel groups. Similar comparisons were conducted on the aggregate scale with all three institutions combined. The analyses were intended to be exploratory. A P-value less than 0.05 was considered statistically significant.

III. RESULTS

A. Do Patients File Privacy-Related Complaints?

Patients and families filed complaints related to matters of privacy and confidentiality at all study institutions. (Table 1) When filing complaints, patients and families used terms such as "confidentiality" and "privacy" interchangeably; we dub these complaints, collectively, "privacy-related complaints." Privacy-related complaints comprised 0.4 to 2.3 percent of all complaint reports recorded by the medical centers over the five-year target period.

Table 1

Frequency of Reports with Privacy-Related Complaints (PRC reports)

Pre- and Post-Final Compliance Date with HIPAA Privacy Rule

Institution 1	Pre Count	Post Count	P Value	Relative Change
PRC reports	54	102		
PRC reports per year	18	51		
Total complaint reports	3079	3976		
PRC reports/1000 complaint reports	17.5	25.7	**0.027**	46.3%
PRC reports/million RVUs	4.4	10.6		140.9%
Institution 2				
PRC reports	49	42		
PRC reports per year	16.3	21		
Total complaint reports	4920	3177		
PRC reports/1000 reports	10	13.2	0.211	32.7%
Institution 3				
PRC reports	28	70		
PRC reports per year	9.3	35		
Total OPA reports	5327	3093		
PRC reports/1000 reports	5.3	22.6	**<0.001**	330.6%
Aggregate				
PRC reports	131	214		
PRC reports per year	43.7	107		
Total complaint reports	13326	10246		
PRC reports/1000 reports	9.8	20.9	**<0.001**	112.5%

Pre: 3 years of data from 4/1/00 to 3/31/03
Post: 2 years of data from 5/1/03 to 4/30/05
Relative Change: (Post - Pre)/Pre *100%
P Value is calculated under the null hypothesis that the ratio of PRC reports in relation to all OPA reports is the same in both Pre and Post study periods
RVUs: relative value units, a proxy for workload
(RVUs available for Institution 1 only)

B. Can Privacy-Related Complaints Be Classified?

The process of collecting and sorting privacy-related complaints resulted in seven overall categories of complaints: environmental disclosures, inappropriate disclosures, incidental disclosures, too sensitive information, willful disclosures, privacy policy compliance issue, and dissatisfaction with privacy policy. Table 2 in the Appendix provides examples for each category. The first five categories reflect patients' perceptions that their confidentiality and/or privacy expectations were or could be violated and the last two, their beliefs that institutional policy or procedure related to confidentiality and/or privacy was not followed or created burdens.

Pooling results for all institutions over both observation periods, incidental and willful disclosures were the most common complaints, followed by environmental disclosures and dissatisfaction with institutions' privacy policies. (Table 3)

Table 3

Distribution of Privacy-Related Complaints Pre- and Post-Final Implementation Date for HIPAA Privacy Rule

	Institution 1			*Institution 2*		
	Pre count (%)	Post count (%)	Absolute Change (Post - Pre)	Pre count (%)	Post count (%)	Absolute Change (Post - Pre)
"VIOLATIONS"						
Disclosures						
environmental	10 (15.2)	16 (13.6)	-1.60%	5 (9.6)	5 (11.1)	1.5%
inappropriate	6 (9.1)	13 (11.0)	1.90%	8 (15.4)	4 (8.9)	-6.5%
incidental	24 (36.4)	34 (28.8)	-7.60%	18 (34.6)	17 (37.8)	3.2%
willful disclosures	16 (24.2)	31 (26.3)	2.00%	10 (19.2)	10 (22.2)	3.0%
Too sensitive information	1 (1.5)	10 (8.5)	7.00%	10 (19.2)	1 (2.2)	-17.0%
"POLICY-RELATED"						
Privacy policy compliance	3 (4.5)	1 (0.8)	-3.70%	0 (0.0)	0 (0.0)	0.0%
Dissatisfaction with policy	6 (9.1)	13 (11.0)	1.90%	1 (1.9)	8 (17.8)	15.9%
TOTAL	**69 (100)**	**118 (100)**		**52 (100)**	**45 (100)**	

	Institution 3			*Aggregate*		
	Pre count (%)	Post count (%)	Absolute Change (Post - Pre)	Pre count (%)	Post count (%)	Absolute Change (Post - Pre)
"VIOLATIONS"						
Disclosures						
environmental	13 (44.8)	13 (16.7)	-28.2%	28 (19.0)	34 (14.1)	-4.9%
inappropriate	2 (6.9)	7 (9.0)	2.1%	16 (10.9)	24 (10.0)	-0.9%
incidental	3 (10.3)	21 (26.9)	16.6%	45 (30.6)	72 (29.9)	-0.7%
willful disclosures	7 (24.1)	20 (25.6)	1.5%	33 (22.4)	61 (25.3)	2.9%
Too sensitive information	0 (0.00)	1 (1.3)	1.3%	11 (7.5)	12 (5.0)	-2.5%
"POLICY-RELATED"						
Privacy policy compliance	0 (0.0)	0 (0.00)	0.0%	3 (2.0)	1 (0.4)	-1.6%
Dissatisfaction with policy	4 (13.8)	16 (20.5)	6.7%	11 (7.5)	37(15.4)	7.9%
TOTAL	**29 (100)**	**78 (100)**		**147 (100)**	**241(100)**	

Pre: 3 years of data from 4/1/00 to 3/31/03
Post: 2 years of data from 5/1/03 to 4/30/05

C. Which Personnel Are Most Commonly Associated with Privacy-Related Complaints?

Attending and resident physicians were designated "physicians" in the study. All staff categories other than attending and resident physicians were represented under the "non-physician" heading: nurses, receptionists, administrative assistants, housekeepers, technicians, laboratory personnel, etc. We also included under this subheading privacy-related complaints that did not specify personnel but referred to privacy infringements for which "reasonable safeguards" could be applied. Examples of such complaints include references to shared rooms or certain communication methods, such as misdirected telephone calls, faxes, and letters. Overall, physicians were mentioned in twenty percent of privacy-related complaint reports at all institutions. (Table 4)

Table 4

Distribution of Personnel Involved in Privacy-Related Complaints Pre- and Post-Final Compliance Date with HIPAA Privacy Rule

Personnel	Total	Pre	Post	Absolute Change in Percentage
	Count (%)	Count(%)	Count(%)	(Post - Pre)
Institution 1				
physician	39 (20.3)	12 (18.2)	27 (22.9)	4.7%
nonphysician	153 (79.7)	54 (81.8)	91 (77.1)	-4.7%
Total	*192 (100)*	*66 (100)*	*118 (100)*	
Institution 2				
physician	13 (13.3)	7 (13.5)	6 (13.3)	-0.1%
nonphysician	85 (86.7)	45 (86.5)	39 (86.7)	0.1%
Total	*98 (100)*	*52 (100)*	*45 (100)*	
Institution 3				
physician	27 (24.3)	14 (48.3)	13 (16.7)	-31.6%
nonphysician	84 (75.7)	15 (51.7)	65 (83.3)	31.6%
Total	*111 (100)*	*29 (100)*	*78 (100)*	
Aggregate				
physician	79 (19.7)	33 (22.4)	46 (19.1)	-3.4%
nonphysician	322 (80.3)	114 (77.6)	195 (80.9)	3.4%
Total	*401 (100)*	*147 (100)*	*241 (100)*	

Total: 5 years of data from 4/1/00 to 4/30/05
Pre: 3 years of data from 4/1/00 to 3/31/03
Post: 2 years of data from 5/1/03 to 4/30/05

D. Were There Differences in Findings Between the Two Observation Periods?

Privacy-related complaint reports increased in frequency during the second observation period for all institutions. (Table 1) The proportion of privacy-related complaint reports per 1,000 complaint reports increased significantly for two of the institutions (Institution 1 (18 vs. 26, $p = 0.027$) and Institution 3 (5 vs. 23, $p < 0.001$)) but not Institution 2 (10 vs. 13, $p = 0.21$)).

We had access to relative value units (RVU)[87] data for Institution 1, which served as a proxy for service volume. The RVU data allowed us to normalize the report count for the workload. The number of pri-

[87] RVU is an acronym commonly used within the health care industry. WILLIAM C. HSIAO ET AL., A NATIONAL STUDY OF RESOURCE-BASED RELATIVE VALUE SCALES FOR PHYSICIAN SERVICES: PHASE III FINAL REPORT TO THE HEALTH CARE FINANCING ADMINISTRATION 215 (Harvard School of Public Health ed. 1992).

vacy-related complaint reports per million RVUs more than doubled (4.4 and 10.6, respectively), while the workload volume increased by twenty-one percent from the first to the second observation period.

Table 3 illustrates the distributions of privacy-related reports across seven complaint categories. In the aggregate, there was no significant change in the distribution of complaint categories ($p = 0.14$), but there were some specific changes in distribution at individual institutions between the two observation periods. The distribution of these complaints did not change significantly between the two observation periods for Institution 1 ($p = 0.30$). The observed decrease in allegations that "too sensitive information" was solicited or documented and the increase in "dissatisfaction with policy" complaints at Institution 2 ($p = 0.014$) were statistically significant. "Environmental" violation complaints decreased and "incidental" violation complaints increased at Institution 3 but did not reach statistical significance ($p = 0.06$). "Willful disclosure" allegations did not change for any institution.

Table 4 illustrates the results for distribution of complaints across two personnel groupings: non-physicians and physicians. Non-physicians accounted for the majority of complaints (fifty-three to eighty-seven percent) in both periods. For Institution 1 ($p = 0.20$) and Institution 2 ($p = 0.63$), the contribution of each personnel grouping to privacy-related complaints remained roughly the same for the two observation periods. For Institution 3, the proportion of complaints associated with non-physicians relative to physicians increased significantly between the observation periods. Aggregate data for the three institutions showed a significant shift in the distribution of personnel grouping associated with privacy-related complaints over the two observation periods ($p = 0.02$).

IV. DISCUSSION

Our study's findings are as follows: (a) patients and families reported privacy-related complaints to offices of patient affairs; (b) reports generated on the basis of these expressed concerns could be reliably coded and aggregated into privacy-related complaint categories; (c) physicians generated twenty percent of the privacy-related complaints; (d) each study institution displayed a unique distribution of complaint types; (e) some complaint categories appeared more frequently in complaint reports; and (f) patients filed more privacy-related complaints in the second observation period compared with the first. Our discussion will comment on these findings.

A. Privacy-Related Complaints

The study demonstrated that patients and/or their families do file complaints with offices of patient affairs about their perceptions of how institutions handle matters of privacy and confidentiality. Several privacy interests were represented in the complaints, including physical, informational, proprietary, and personhood (dignity) interests. Sometimes patients perceived serious violations of their privacy by physical intrusion, both into spaces over which they thought they should have control and their person:

> [Husband] had clearly stated that no one with the last name of ['Smith'] should visit or know of her location, yet the staff personally escorted Mr. [Smith] to her room.
> The nurse showed [his burns] to [another woman,] exposing his private area.

Patients complained of infringements on informational privacy interests where strangers and acquaintances alike could hear, see, or were otherwise provided with details of illnesses, test results, treatments, and personal data:

> The nurses are always discussing patients in the hall, and everyone can hear. I can tell you everything about the other patients there. I know everybody's business, and they know mine."
> Dr. XX came to the waiting room . . . [I]n the presence of the other gentleman . . . the reference to "remune" and "clinical trials" indicated . . . [patient] is being treated for AIDS.
> [D]oor left open throughout [my] visit. . . . should be closed for privacy.

Patients often expressed concern that, without their permission, information was disclosed, left on answering machines, mailed, faxed, or otherwise transmitted to other providers or family members, or areas where others would have access:

> Patient upset . . . fax sent from her doctor's office . . . to fax machine . . . in area used by others.

They were equally alarmed to learn other patients' medical information by overhearing, being handed, or receiving information via mail or fax; they began to worry where their own information might be:

> She overheard Dr. X telling husband of a patient her prognosis in a crowded waiting room. . . . [S]he was appalled. . . . [that the] doctor discussed the patient's procedure and told him about her breast cancer.
> He picked up his films, and there were x-rays for 7 other patients in the jacket. . . . [with] patients' names, dates of birth, and social security numbers.
> The lab results she received in the mail . . . were not hers.
> He received another patient's records. Other patient was in for HIV test.

Patients were disturbed by observations that health care personnel were careless with medical information and took few precautions to protect it:

> [He] left a report of all of his other patients in [the] room and did not retrieve it until hours later.
> She learned a lot about the patients in the nearby beds because she could overhear conversations.

Conversely, patients found at times that their intent to disclose or receive information was thwarted by health care personnel:

> [N]urses are scared of giving away personal information due to HIPPA [sic].

Patients or families, in telling their stories, sometimes revealed a sense of what can only be described as an assault upon their or their loved ones' dignity, i.e., a lack of respect for them as persons. For example, according to one parent of adopted children,

> Dr. X asserted . . . that both of the parents had been alcoholics . . . as the boys played at our feet. I don't know yet what I will tell them about their birth parents, but I reserve the right to tell them when I choose and what I choose. . . . Two residents were invited to observe the physical. [My son] is easily embarrassed and was further subjected to Dr. X pointing out to the residents such characteristics as how he held his arms, how he ran, his gait, etc. [My son] was clearly humiliated[,] and so was I. I told Dr. X I didn't think he needed such a large audience during this physical.

Patients also expressed grave concerns about risk of appropriation of personal financial data and unique identifiers, a type of proprietary privacy interest. They worried that such information would be or had been stolen and converted to the control of others. Fear or reports of

identity theft, including medical identity theft, was a recurring theme in the privacy-related complaint reports:

> His brother was in an auto accident and used his name in order to [receive several thousand dollars worth of] medical care. . . . [A]s a result, Mr. XX has very bad credit.
> He had complained about seeing patients' personal information thrown in the regular trash. He was worried about identity theft.

B. Classifying Complaints: How to Recognize the "Tip of the Iceberg"

The coding system we developed yielded classifications into which privacy-related complaints could readily and reliably be sorted. While the absolute number of reports for each observation study period is small, they merit consideration for two reasons: first, the information they convey signifies a much higher likely incidence of similar events, and, second, complaints may be associated with legal risk.

Background studies about consumer dissatisfaction in all commercial areas indicate that, while many may be unhappy, few take action to let the vendor or offender know of their dissatisfaction.[88] Fewer still initiate an informal or formal complaint. An even smaller number follow through on litigation. Studies in the health care context have demonstrated that for every patient who voices or files a formal complaint, many more patients with similar experiences do not.[89] Each complaint, therefore, represents the "tip of the iceberg."

As for legal risk, previous studies show that physicians who generate higher rates of seemingly unrelated patient complaints have an

---

[88] *See* BEST, *supra* note 76, at 114-30.

[89] Ellen Annandale & Kate Hunt, *Accounts of Disagreements with Doctors*, 46 SOC. SCI. MED. 119, 125 (1998) ("[O]f the 307 disagreement episodes reported, just four led to any formal action being taken beyond seeking a second opinion and changing doctors as already noted."); *cf.* Mark Schlesinger et al., *Voices Unheard: Barriers to Expressing Dissatisfaction to Health Plans*, 80 MILLBANK Q. 709, 717 (2002) (citing 1988 study that found "as few as 11 percent of American patients complain about the problems that they experience"); Linda Mulcahy & Jonathan Q. Tritter, *Pathways, Pyramids and Icebergs? Mapping the Links Between Dissatisfaction and Complaints*, 20 SOC. HEALTH & ILLNESS. 825, 835 (1998) (stating that thirty-eight percent of surveyed householders had expressed specific dissatisfaction with health care to formal networks); JUDITH ALLSOP & LINDA MULCAHY, ADVERSE EVENTS, COMPLAINTS AND CLINICAL NEGLIGENCE CLAIMS: WHAT DO WE KNOW? 14 (U.K. Dep't of Health ed., 2002) (citing 1997 MORI survey in which thirty-two percent of dissatisfied patients voiced complaints).

associated increased likelihood of being sued in the event of an adverse medical outcome.[90] Privacy-related complaints may be of particular importance, for when compared with other types of seemingly unrelated patient complaints such as rudeness or long waits, they uniquely refer to matters which themselves may bear direct legal consequences.

C. Categories of Personnel and Privacy-Related Complaints

The findings suggest that non-physicians were most often associated with privacy-related complaints. However, physicians were mentioned in a sizeable portion of the complaints (twenty percent) and were associated with some of the more egregious complaints. We propose several reasons for the predominance of non-physicians in the complaints. First, access to information and information-processing, unlike treatment, is not restricted to medically-trained personnel. Second, non-physicians represented a collective aggregate of different groups of personnel. Third, because non-physician personnel make up the majority of employees within medical institutions, it is not surprising that they would be associated with a larger share of complaints than physicians. Fourth, non-physicians' vulnerability for privacy-related complaints may be related to the physical work environment as well as their job functions. They often are positioned in common work spaces with visible computer screens and fax machines, which, without adequate safeguards, pose risk for disclosure. They may spend time in clinical settings that pose privacy challenges and require special effort to compensate for visual and aural access to patients. Job functions commonly involve processing or transferring health information. We suspect that both groups, physicians and non-physicians, may not receive adequate training to be able to reflexively or consciously incorporate principles for protecting privacy in all situations. Overall, there was a significant shift in the distribution of complaints towards non-physicians from the earlier to the later observation period. The reasons for this are not clear and merit further study.

D. HIPAA and Privacy-Related Complaints

Two interesting observations involving comparison of the first and second study periods emerged from the study. First, the proportion of patient complaints that reflect privacy-related issues appears to have increased concurrently with institutions' efforts to comply with HIPAA requirements. For all of the study institutions, up to three

[90] *See generally* Hickson et al., *supra* note 78.

times more privacy-related complaint reports were filed in the second observation period than in the first. Analysis of privacy-related complaint reports relative to volume at Institution 1 revealed a greater increase in these reports than could be accounted for by patient volume alone.

Second, the distribution profile of complaint categories for Institutions 1 and 3, as well as the aggregate distribution profile, did not change significantly from the first to second study period. For both study periods, complaints about incidental disclosures, followed by willful disclosures, dominated over all other types of complaints.

What might be the reasons for these observations? If HIPAA created uniform standards to protect medical privacy, why did patients file more complaints about privacy issues in the second study period than the first? And why did complaints about willful disclosures (for the most occurring as part of normal business operations) and incidental disclosures (disclosures to unintended recipients) continue to be so prominent? After all, the required privacy notices alert patients that information will be shared for treatment, payment, business operations. In addition, the regulations apply restrictions on use and disclosure to prevent, or at least lessen the risk of, incidental disclosures. Health care professionals and medical institutions in compliance with HIPAA, then, should be communicating and transferring information in appropriate settings, under appropriate circumstances, and in an appropriate manner. They should, therefore, no longer receive complaints about privacy or confidentiality breaches.

We did not find this to be the case. Instead we found an increase in the proportion of privacy-related complaint reports relative to all patient complaint reports and noted, in particular, the persistence of incidental and willful disclosure complaints. We propose several potential explanations for these findings. The first possibility is that confidentiality and privacy issues in medical care may have gained more saliency through dissemination of HIPAA-related information. To begin with, some patients and families may have learned of their rights under HIPAA through general publicity in the period around April 13, 2003, the deadline for most covered entities to comply with the Privacy Rule. Others may have been alerted by reading institutions' privacy practices notices. Even patients who did not read the notices may at least have had their attention drawn to the issue by the HIPAA acknowledgment form. Finally, saliency could have also been a factor for patient affairs personnel whose awareness or knowledge of HIPAA may have inspired them to more diligently record these types of complaints. Thus, both patients and patient affairs personnel may have been particularly sensitized to privacy and confidentiality matters.

A second hypothesis might be that, although the three institutions studied here presumably consider themselves to be fully HIPAA-compliant, they are not.[91] A third hypothesis, which may or may not be related to the second, is that health care workers continue to invade patients' privacy and, without authorization, disclose or use health and related personal information. While there may be circumstances of disclosure that suggest suspect motivations, presumably most instances involve well-intentioned individuals acting in a manner consistent with what they believe to be in their patients' best interests[92] or their institutions' policy:

> She learned that Dr. XX accepted her [as a patient]. . . . [S]he understood from her psychiatrist that no other staff would have access to her psychiatry records. . . . Dr. XX knew all about her psychiatric medications. . . . [T]he only way he could have known was to look at her records from her psychiatrist. . . . [S]he is not angry but is very sad that this happened.

A fourth possible reason for the increase in privacy-related complaints in the second observation period is suggested by our comparison of RVU data with complaint rates. Increased volume may increase pressures and demands on health care staff and medical institutions, making it more difficult for them to protect patients' privacy and medical information confidentiality at all times.

---

[91] *See, e.g.*, Joseph Goedert, *Keeping Up with HIPAA Compliance*, HEALTH DATA MGMT., Dec. 2006, http://healthdatamanagement.com/HDMSearchResultsDetails.cfm?articleId=14367; PHOENIX HEALTH SYSTEMS, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, U.S. HEALTHCARE INDUSTRY HIPAA COMPLIANCE SURVEY RESULTS 2-4 (2006), *available at* http://www.himss.org/ASP/ContentRedirector.asp?ContentId=65641 (reporting that fifty-five percent of Providers and seventy-two percent of Payers have implemented Security standards; twenty percent of Providers and fourteen percent of Payers are non-compliant with Privacy regulations; among "compliant" organizations, "establishing Business Associate Agreements, monitoring internal Privacy compliance, and maintaining an accounting of disclosures" are areas of least compliance; "organizational constraints" and problems integrating "new systems and process" are cited as barriers to compliance).

[92] Kathleen Shoaff, *Professors Discuss Effectiveness of Patient Confidentiality Law*, THE DAILY ATHENAEUM, Nov. 1, 2006, http://www.da.wvu.edu/new/show_article.php?&story_id=24613&archive_date=11-01-2006 (discussing how physicians disclose medical information to family members without the patient's permission if they believe disclosure is in the best interest of the patient).

We propose a final hypothesis. Perhaps patients' concerns actually derive from the design of HIPAA itself. Our findings in the study raise the question as to whether the HIPAA regulations, as currently drafted and interpreted, capture patients' expectations of what privacy in the health care setting should entail.[93] The issues involve HIPAA's concepts of medical privacy, permissible disclosures, limits on disclosure, and the role of the notice of privacy practices.

Given the origin of HIPAA and its implementing regulations, consider whether full compliance would necessarily eliminate complaints about privacy and confidentiality violations. Because Congress's primary intent in enacting HIPAA was to facilitate business transactions, the privacy protections in the regulations issued by HHS represent something of an afterthought. HHS realized that to retain the public's confidence in the face of easier information exchange for business purposes it needed to explicitly address medical privacy. It did so but in an odd way. While re-conceptualizing the meaning of medical privacy through the regulations, HHS did not attempt to define privacy as a substantive or set of substantive interests. Instead, it established the meaning of medical privacy through the creation of a procedure by which privacy interests could be overcome.

The HIPAA regulations pay a lot of attention to informational privacy interests but very little to other privacy interests. Of particular concern is HIPAA's failure to positively influence respectful behavior among health care workers, hindering the effective delivery of health care that HIPAA is supposed to promote. To illustrate:

> She felt her case was discussed in the hall and her name was trashed in front of the surgeons; her son was hurt and no one showed any compassion, and some even laughed. . . . [I]f they had gone to a room, she may have been able to discuss very serious things that she was worried about in regards to her son.
>
> Such assertions do more than share individuals' hurt feelings; they demonstrate how a lack of regard for their dignity and

---

[93] *See, e.g.*, Joseph Conn, *HIPAA, 10 Years After*, MODERN HEALTHCARE Aug. 7, 2006, at 26, 28 (discussing ongoing litigation against former HHS Secretary Tommy Thompson raising Fourth and Fifth Amendment constitutional challenges to the final Privacy Rule's "notice" language that replaced "consent" language); Jennifer Stansbury, *Medical Identity Theft Survey Reveals Consumers Are Concerned About the Privacy and Protection of Their Medical Records*, EPICTIDE, INC., Dec. 12, 2006, http://www.epictide.com/subpages/Medical_Identity_Theft_Survey.asp.

> need for privacy impairs their ability to communicate with physicians, to the detriment of themselves or their loved ones.

The regulations, on the other hand, do define confidentiality, albeit in a curious manner. HHS does not portray confidentiality as a feature of information that precludes it from being shared except with authorization from the person about whom it pertains or for other compelling reasons. Rather, under HHS's version, the property of information called "confidentiality" is that a non-authorized person or process cannot gain access to it. This definition of confidentiality does not specify who is authorized to authorize.[94] Ultimately, it is the Privacy Rule, not the patient, that grants authorization for access to medical information in most instances.

The regulations grant authorization by listing categories of persons and entities authorized to have access to information and the activities and processes for which they may use the information.[95] While patients retain the authority to prohibit disclosures not otherwise excepted,[96] the list of exceptions is so extensive as to eviscerate any common understanding of what it means to be in control of one's medical information. In some cases, patients complained of behaviors or disclosures which are, in fact, allowed by HIPAA[97]:

> Patient states he is angry because Dr. XX violated his confidentiality by calling Dr. YY without his permission.
> Patient's father was upset about [the vendor the medical center uses to provide durable medical equipment] having his information.

Or they revealed through their comments a belief that there were no prohibitions on sharing information:

> Patient stated the way he understood the information he received, [the medical center] can just release his information to whomever it pleases.

Despite such misunderstandings, the regulations do specify three cautionary restrictions on covered entities' use or disclosure of information; the "minimum necessary"[98] information may be shared with

---

[94] *See* 45 C.F.R. § 164.304 (2006).

[95] § 164.502; § 164.512.

[96] § 164.502; § 164.508(a).

[97] *See generally Less than 25% of Medical Privacy Complaints Merit HHS Investigation, Melamedia Seminar Reveals*, BUSINESS WIRE, Dec. 13, 2006.

[98] 45 C.F.R. § 164.502(b) (2006); § 164.514(d).

those who "need access"[99] in order to do their jobs, as long as "reasonable safeguards"[100] against unauthorized disclosure are utilized in doing so. Patients' expressions demonstrated an instinctive recognition that disclosures, or requests for information, should be tailored to require the "minimum necessary" to be provided to those with a bona fide need:

> The [secretaries ask] personal questions regarding the appointment. Why do you want to see the doctor? What's the problem? . . . He feels they are not medical personnel and that it is none of their business. . . . [O]ne [employee] hung up on him because he refused to tell her.

In practice, adherence to these restrictions is not simple. First, it takes a certain level of skill to be able to consistently distinguish what is necessary from what is desired and what the minimum would be to meet that need. It requires training and judgment and may be prone to error. Furthermore, health care providers' perceptions of minimum necessary do not always match those of patients':

> The Breast Center and return address were on the outside of the envelope, and her female carrier asked if she was OK. [Patient] believes the return address information was a breach of her right to confidentiality.

Presumably, had this patient been given a choice, she would have requested that communications come in an unmarked envelope.

Finally, it is not apparent that any form of policing would be able to adequately enforce these limiting criteria. The high percentage of complaints about incidental disclosures demonstrates that they have not diminished despite HIPAA. Many instances are likely to take place without witnesses, in the form of misdirected faxes and letters, or without the awareness of the patient that others are within viewing or hearing distance. The failure of the regulations to promote respect for physical and personhood privacy interests may further impair attempts to achieve compliance with minimum necessary, need to know, and safeguard standards.

Patients have a right to notice of covered entities' privacy practices under the regulations.[101] Covered entities are required to provide patients with notice of the latitude of disclosure granted them by the

---

[99] § 164.514(d)(2)(i)(A).
[100] § 164.530(c).
[101] § 164.520(a)(1).

regulations. While required to give at least one example of disclosures for each of "treatment, payment, health care operations,"[102] the regulations do not require covered entities to give examples that illustrate disclosures a patient might not readily anticipate.[103] While patients assume that their physicians and nurses will have access to their medical record, health care institutions typically do not specifically describe the range of personnel, both within and outside the institution, who may have access to the information for health care operations, treatment, and payment. This is particularly true in the case of outsourced services governed by business associate agreements. The covered entity may have confidence in the integrity of the business partner. However, patients, whose information is being shared, may not feel the same way. They may complain, for example, about telephone or paper surveys that refer to the time, date, provider, and clinic location of their patient visit.

Although not a required element of the privacy notice, covered entities sometimes insert information about providing an opportunity for patients to agree or object to specific uses, in this case, disclosure to those involved in their care or payment for that care.[104] By including this statement in the privacy notice, delivery of the notice provides an opportunity in advance for patients to agree or object. The regulations, however, do not require covered entities to emphasize to patients that they have the right to re-consider whether they wish to agree or object at each medical encounter, nor do they insist that covered entities make it convenient for patients to do so.

Despite HHS's "intent" that notices of privacy practices promote discussions between patients and care providers "related to the use and disclosure of protected health information about him or her,"[105]

---

[102] § 164.520(b)(1)(ii)(A).

[103] *See* Makdisi, *supra* note 14, at 759 (citation omitted) (While covered entities are required to "provide 'sufficiently detailed' descriptions of uses and disclosures that are permissible under [45 C.F.R. § 164.534 (2001)] . . . [e]ntities may. . . utilize innocuous examples that may mask more controversial uses and disclosures."). In fact, 45 C.F.R. § 164.520(b)(1)(ii)(D) does not require an example in its "sufficient detail[ed]" description, whereas § 164.520(b)(1)(ii)(A) pertaining to "treatment, payment and health care operations" does.

[104] 45 C.F.R. § 164.510.

[105] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,210 (Aug. 14, 2002) (to be codified at 45 C.F.R. pt. 160, 164) ("The Department also understands that the opportunity to discuss privacy practices and concerns is an important component of privacy, and that the confidential relationship between a patient and a health care provider includes the patient's ability to be involved in discussions and decisions related to the use and disclosure of protected health information about him or her."). The authors are unaware of any research demonstrating that the privacy notices have this type of salutary effect.

they have instead been a common source of unresolved confusion. In general, especially at larger institutions, front desk staff are delegated the task of giving patients a copy of the notice of the institution's privacy practices and asking them to sign the acknowledgment that they have received a copy of the notice. It is unlikely that all front desk personnel or even medical providers are truly qualified to answer questions about the interpretation of the general description of permitted uses of information in the privacy notice. Patients with questions, therefore, must choose between delaying their visit in order to pursue a conversation with an institution's attorney or privacy officer, or seeing their doctor on schedule. Most likely, they will choose to "participate in the exchange of privacy for health care."[106]

In short, HIPAA is guilty of duplicity. While purporting to provide something that people value,[107] it actually prioritizes the health care team's function over individuals' preferences and shields health care workers and institutions from liability for disclosures related to those functions.[108] The privacy rights it establishes do little to control use or disclosure of medical information and do nothing to promote physical or personal privacy for patients. Furthermore, the long business-oriented list of carve-outs permitting uses and disclosures of information predictably may be at odds with patients' legitimate expectations of how their medical information will be handled. Patients' "privacy rights" under the regulations describe procedural rights, not substantive rights. Without the existence of substantive privacy rights, investigations of HIPAA violations boil down to an inquiry of: first, whether the covered entity provided an opportunity for individuals to avail themselves of their "rights," and, second, whether the covered entity was operating within the limits of its broad authority to decide how to use and disclose health information.[109] There are no standards

---

[106] *Restricting Disclosure Under the HIPAA Privacy* Rule, HEALTH LAW WEEK, Feb. 18, 2005, at 34 (discussing Makdisi, *supra* note 14, at 754).

[107] *See* 45 C.F.R. § 164.520(c); http://www.hhs.gov/ocr/privacysummary.pdf at 13-17 (describing requirements for what is to be included in the institution's privacy notice although privacy is not required to be defined).

[108] *See id.*, "Permitted Uses and Disclosure" at 4-6 (leaving it in the hands of "covered entities [to] rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.")'; 45 C.F.R. § 164.502(a)(1); § 164.506.

[109] 45 C.F.R § 164.520(a)(1) (right to notice of privacy practices); § 164.522(b) (right to receive health information by alternative means); § 164.522(a)(1) (right to request restriction of uses and disclosures), but covered entities are not required to agree to a restriction; § 164.522(a)(1)(i); § 164.526(a) (right to amend), which is actually a right to request an amendment that the covered entity may deny for a variety of reasons; § 164.528 (right to accounting) subject to, at covered entities' discretion, exclusion of all permissible and authorized uses and disclosures; § 164.524

for judging if either procedural irregularities or "permissible" disclosures had an impact on individuals' privacy interests.

In Part V, we will submit some suggestions for modification of the Privacy Rule and steps that administrators can take to better meet patients' expectations for respecting privacy and maintaining confidentiality within the health care context.

We acknowledge several limitations of this study. The first relates to selection of the complaint reports containing privacy-related complaints. Keywords were selected to optimize the balance between retrieving all relevant reports and avoiding an excessive number of non-relevant ones. Adding keywords led to the return of diminishing numbers of useful reports. Our analysis was based on comparing proportions of privacy-related complaint reports for both study periods, so exclusion of other potentially useful keywords should not affect our results.

Thirteen of 102 complaint reports in Table 1 were found using HIPAA and its common spelling variants (collectively, "HIPAA") and did not contain another keyword; these complaints were filed in the second study period and were relatively evenly distributed across coding categories. While we recognize that use of "HIPAA" would more likely occur in the second observation period, we submit that patients may instead have found "HIPAA" to provide an efficient way to easily telegraph messages that would have been otherwise expressed prior to the law's adoption. The presence of "HIPAA" in patient complaints also suggests that complaint-capturing systems do successfully identify HIPAA-related complaints, i.e., patients do pay attention to HIPAA. They may assert rights that in fact exist under the regulations but often assert perceived, but nonexistent, rights. Even if privacy-related complaint reports found exclusively through searching for "HIPAA" were removed from the study, however, the number of privacy-related complaints reports filed would still reflect an increase from the first observation period to the second.

Another potential limitation is that the interval between the effective date of the Privacy Rule of HIPAA (October 2002) and the final compliance date (April 14, 2003) may have affected our results. As preparations were made for final compliance, widespread media publicity and health facility efforts informed patients of the change in federal law.[110] While April 14, 2003 may not represent a sharp line to

(right of access to protected health information except for patients seeking psychotherapy notes).

[110] *E.g.*, Elaine Wilner, *Q & A, Lauren Steinfeld, From Intrusive Surveillance to Identity Theft to Junk E-mail, Privacy Is Under Attack. It's Her Job to Mount a Defense*, PENN CURRENT, Feb. 27, 2003, *available at*

indicate when patients did or did not know about HIPAA, comparing complaint patterns before and after the final compliance date, nevertheless, yields useful information.

Distribution patterns of reported confidentiality- and privacy-related violations provide insight into one important aspect of an institution's unique risk profile, but they should be interpreted cautiously and within context. Instances of inappropriate disclosures by health care workers may be less discoverable by patients and, therefore, evoke fewer complaints than more easily discovered undesired disclosures, such as incidental or willful ones. Patterns of complaints may also reflect patients' assessments of context. "Environmental" lack of privacy, such as experienced in a semi-private room or curtained cubicle in an emergency department, may not differ from some patients' expectations.[111] A "willful" disclosure to a patient's employer, however, is unexpected and sufficiently distasteful to motivate a complaint. Conversely, as illustrated earlier, some complaints may reflect patients' erroneous beliefs that certain disclosures are legally impermissible, and, therefore, some patients may overstate the frequency of true infringements.

Finally, institutions' differing complaint capture systems might have affected the results. While results for each medical center varied, complaint category distribution patterns were similar, supporting the notion that a variety of complaint capture systems may be effectively utilized to analyze privacy-related complaints.

V. RECOMMENDATIONS

Despite potential limitations, the study findings merit some consideration and suggest that institutions and providers should not assume that HIPAA has eliminated or diminished patient concerns about the way they treat privacy interests. In this section, we will suggest regulatory reforms and private administrative initiatives that might better serve those interests.

---

http://www.upenn.edu/pennnews/current/2003/022703/cover.html; Aparna Surendran, *Lawsuit Filed Against New Health Privacy Rule*, PHILADELPHIA INQUIRER, Apr. 1, 2003; R. Pear, *House Republicans Urge Bush to Ease Health Care Rules*, N.Y. TIMES, May 11, 2001; Cal. Healthcare Found., *Janlori Goldman Discusses Privacy on 'Morning Edition,'* CAL. HEALTHLINE, May 15, 2001; Buster Olney, *Baseball: Law May Forbid Leagues to Say If Player Is Hurt*, N.Y. TIMES, June 11, 2002; Jennifer Steinhauer, *Money & Medicine: Patient: Know Thy Rights*, N.Y. TIMES, June 4, 2000.

[111] *See,* Barlas et al., *supra* note 82, at 138.

A. Legal Reforms

The purpose of HIPAA's Privacy Rule, according to HHS, is to allow "the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being."[112] Clearly, HIPAA's premise was that the public good would be better served through efficiencies in information flow. The study supports the idea that, rather than raising the bar, the Privacy Rule may have created a more casual approach to the issue of protecting patients' privacy interests and, in some cases, may have caused harm to those interests.

It is to the credit of the drafters of HIPAA and its implementing regulations that they considered and attempted to do something to address foreseeable public resistance to the idea of low-barrier information sharing in order to achieve the goal of increased efficiency in management of the health care system. However, we believe that the HIPAA regulations do not take adequate cognizance of people's legitimate expectations in the area of privacy and confidentiality in health care. HIPAA currently provides to patients only meager control over the flow of health information compared to that granted to covered entities. The inclusion of standards such as "reasonable safeguards," disclosure of the "minimum necessary" information, and ascertaining the need for employees' need for access, hint at some limitations on disclosure, but HHS did not go far enough to assuage worries that have, in fact, become real. We see a need for further legislative action or administrative clarification of the privacy standards.[113]

---

[112] OFFICE FOR CIVIL RIGHTS, SUMMARY OF THE HIPAA PRIVACY RULE, *supra* note 3, at 1.

[113] The complex, time-consuming, and interest-group ridden process of enacting or amending federal legislation need not be undertaken in order to implement the changes we recommend; the statutory authority already exists. HHS is fully authorized to enact regulations that adequately protect the privacy and dignity of patients in American society. Revised standards of this nature would fit comfortably with HHS's discretion under the prevailing *Chevron* doctrine. *See* Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 865-66 (1984). The existing regulations are already a fairly expansive interpretation of the statute. Revised standards that balance patients' privacy interests more evenly against the business needs of the healthcare providers would not be any more expansive. *See generally* Cynthia R. Farina, *Statutory Interpretation and the Balance of Power in the Administrative State*, 89 COLUM. L. REV. 452 (1989) (discussing the interaction between courts and agencies following *Chevron*); *see* Jonathan T. Molot, *The Judicial Perspective in the Administrative State: Reconciling Modern Doctrines of Deference with the Judiciary's Structural Role*, 53 STAN. L. REV. 1, 99 (2000); *see generally* Peter L. Strauss, *One Hundred Fifty Cases Per Year: Some Implications of the Supreme Court's Limited Resources*

First and foremost, the regulations need an affirmative definition of privacy. Remarkably, the present Privacy Rule contains no such definition. The value of defining privacy goes beyond the increased clarity that would result, although such an increase would certainly be welcome. By defining privacy, the regulations will establish a normative tone and moral authority that is essential in this area. No set of rules can possibly cover all the situations implicating patient privacy that arise in medical treatment nor can any agency address all instances of violations. To provide the protection that patients need, HHS must obtain voluntary compliance, and that means that it must articulate a norm that health care providers and personnel can understand and follow. Declaration of substantive privacy rights within HIPAA would send a powerful message to both health care providers and institutions to remind them of the essence of the context in which they easily conduct treatment, payment, and health care operations. The regulations should reflect standards of civility, respect, and dignity that patients in our society expect or have a right to expect. We recognize that such standards may be hard to develop and harder to enforce. However, if not articulated, voluntary efforts are not likely to result in the needed level of consistent, across the-board performance.

Second, modification of the regulations should include procedural components to ensure implementation of substantive privacy standards. Where the regulations are vague, institutions and individuals may behave in a manner that will accommodate their greatest convenience. General changes in the overall orientation of the HHS regulations would include fuller development of the "minimum necessary," "need to know," and "reasonable safeguards" standards to make clearer its meaning and application to a wide range of clinical situations. Most importantly, the regulations should require educational programs for health care personnel that address, not only the mechanics of the regulations, but also philosophical concepts shaping the delicate balance of business needs and all aspects of patient privacy. This may prepare health care workers to more flexibly address varying circumstances and take into account matters of physical and personal privacy. The procedural regulations should require institutions, on a local level, to develop policies and procedures and training programs consistent with more patient-centered applications of the regulations.

---

for Judicial Review of Agency Action, 87 COLUM. L REV. 1093 (1987) (analyzing a burdened Supreme Court's ability to shape the law, as in *Chevron*); *see* Cass R. Sunstein, *Law and Administration After* Chevron, 90 COLUM. L. REV. 2071, 2084 (1990) (discussing *Chevron* and its principle of deference).

In addition to these general changes in the overall orientation of the HHS regulations, there are a number of specific changes that would contribute to the protection of patients' privacy. These include supplementary regulations governing physical intrusion, notice to patients, opportunities for patients to agree or object to certain disclosures, restrictions on sharing information with those involved in payment for care, restrictions on institutional uses or disclosure of information, and expanded accountability to patients of uses and disclosures of health information.

1. Supplementary Regulations Governing Physical Intrusion

The HIPAA regulations focus on informational privacy rather than physical privacy. Privacy, however, should take into account physical privacy interests, that is, individuals' control over others' ability to see, hear, and touch them. While patients may have received notice of both the nature of the institution and the fact that information will be shared with those involved in their care, such notice may not adequately prepare them for how privacy in its broadest sense may be compromised in the course of medical care. The regulations should make clear that the principles of "minimum necessary," "reasonable safeguards," and "need for know" apply as readily to physical privacy as they do to informational privacy.

Consider a sample complaint about a medical encounter from one of the academic medical centers in the study. Patients who seek services at academic medical facilities are given notice that, as an educational institution, students and residents are part of the health care team and may participate in the patient's medical care. Generally, patients understand and accept that students or residents must be exposed to clinical care so that they may eventually practice medicine independently. Patients, however, do not always understand beforehand what an exam will entail nor are they necessarily able to anticipate how the presence of additional parties may impact their experience of a particular exam. Sometimes they are not asked at the time of the exam if they would agree or object to the presence of trainees. Patients may become emotionally distraught over difficult clinical encounters, especially when witnessed by others who passively observe. In this complaint, the patient stated:

> No one asked her permission or advised her that a student would be conducting the exam. . . . [T]he examination was extremely painful. . . . [S]he feels humiliated because there were four people in the room during her exam, none of whom did anything to intervene and help her during the procedure. She expressed a great deal of anger that no one asked her

> permission to have so many people in the room. . . . Ms. XX compared this experience to being raped with an audience present.

The patient's autonomy and physical privacy were violated: she asserts that she was not asked for permission to have individuals present during the exam; she was not informed ahead of time of a material fact about the ensuing exam, i.e., that a student would be Conducting it; and she likened the exam to a physical invasion ("rape") with observers. Adequately trained personnel who understood substantive privacy concepts would likely have handled the situation in a way to avoid creating distress for the patient. They might have engaged with her to create expectation and agreement on how to meet her medical needs, maintain an atmosphere of dignity and respect in which the patient could communicate her preferences, and balance the learning needs of the students.

Other types of occurrences during care intrude on patients' physical privacy:

> She put the 'Bathing' sign on the outside of her door so that she can have some privacy while she showers, dries off, and dresses. Nurses, care partners, staff who pick up meal trays, persons who clean the room, etc. have either looked in the blinds or walked in the room while the sign was up. . . . [It is] very embarrassing when the dietary person enters to pick up the tray or the cleaning person comes in to pick up the trash while she is dressing. . . . She does not understand why staff disregard the sign.

Should business needs really take precedence over patients' preferences in these circumstances?

As mentioned earlier, HHS neither defines privacy nor elaborates substantive privacy rights or standards in the regulations, but we believe it ought to. We recommend that any definition of privacy incorporate references to physical and person(hood) privacy interests. Currently "protected health information" covers only individually identifiable health information capable of being transmitted or maintained in electronic or other forms or media.[114] The definition must encompass verbal disclosure as a form of information transmission (sound waves) through a medium (air, telephone) in order for the regulations to make any sense. Why then should the regulations not be further interpreted or modified to clearly include the notion that vis-

[114] 45 C.F.R. § 160.103 (2006).

ual, aural, or tactile access to a person transmits information about that individual through the sensory system as a medium? We would suggest, therefore, that additional rules need to be developed that strengthen and support limitations on disclosure. One set of rules could devise minimum functional privacy standards, such as specifications for rooms and other stalls and cubicles where patient care takes place.[115] Another set could carefully illustrate the application of the principles of "minimum necessary" and "reasonable safeguards" and what it means for "persons or classes of persons" to "need access" in varying contexts involving multiple privacy interests.

2. Clearer Notice to Patients

Health care institutions should be required to provide more specific information to patients about personnel and business associates, within and outside the institution, who may have access to their medical and personal information for health care operations, treatment, and payment purposes. In particular, patients need notice of frequent information sharing activity that would not be intuitively evident (such as outsourced patient satisfaction surveys) before receiving care and offered an opportunity to opt out. One way that covered entities can address the information gap is to provide a Frequently Asked Questions (FAQ) sheet with the Privacy Notice.[116]

In the event that substantive privacy rights are adopted by HHS, institutions ought to adopt similar language into privacy notices. Not only might this serve to foster a respectful care environment, but it may also empower patients to assert control when they perceive infringements on those rights.

---

[115] One option is to mandate that all new construction take these standards into account, including re-modeling, similar to what has been required under the Americans with Disabilities Act of 1984. *See* 34 C.F.R. § 104.23 (2006) ("New Construction . . . (c)(1) Effective as of January 18, 1991, design, construction, or alteration of buildings in conformance with sections 3-8 of the Uniform Federal Accessibility Standards (UFAS) (Appendix A to 41 CFR Subpart 101-19.6) shall be deemed to comply with the requirements of this section with respect to those buildings.").

[116] HIPAA does not currently require covered entities to provide adolescents with a Notice of Privacy Practices. Varying by jurisdiction, adolescents are able to consent to care for HIV/AIDS care, psychiatric, sexually transmitted infections, and other reproductive health issues (with varying limits on their ability to receive a therapeutic abortion without parental notification). We would also recommend that HHS specify that they are to be provided with the same notice as other patients.

3. The Opportunity to Agree or Object

Portions of the regulations that afford patients some degree of control over disclosure are drafted vaguely enough that covered entities may, whether intentional or not, deny patients opportunities to exercise that control. One example is the Privacy Rule's articulation of "[u]ses and disclosures requiring an opportunity for the individual to agree or to object" to such use or disclosure of protected health information.[117]

At present, the opportunity to agree, prohibit, or restrict applies only to two circumstances: maintaining patient information in a facility directory and disclosure to others involved in the individual's care or payment. The first circumstance should be straightforward, but some of the complaints we reviewed demonstrated institutions' failure to comply with patients' instructions to not be included in a directory. There is an internal contradiction within the regulations that may account for this. Under section 164.510(a), individuals are to be given an opportunity to agree or object to a facility's use of protected health information in a facility directory. Section 164.522(a)(1)(B)(v) then removes any obligation of the institution to restrict that use, even if it had already agreed to restrict it.[118] The lack of clarity in the regulations may reinforce administrators' presumptions about allowed uses and disclosures of personal information.

As for the second circumstance, the rule is vague and allows institutions to expand their disclosure practices beyond the scope of patients' reasonable expectations. The Rule does not say when the opportunity to agree or object must occur, except that it must be "in advance" of the disclosure.[119] An institution could assert in its privacy notice, for example, that it may share information with others involved in patients' care, including family and friends, and that it will "allow" the patient to tell the institution whom they would like to be involved. Patients may not understand the potential significance of this type of notice. Health personnel may draw an inference from their institution's privacy notice that patients who have acknowledged its receipt have been provided with the required advance opportunity to

---

[117] 45 C.F.R. § 164.510 (2006).

[118] 45 C.F.R. § 164.522 (2006) ("A restriction agreed to by a covered entity under paragraph (a) of this section, is not effective under this subpart to prevent uses or disclosures permitted or required under . . . § 164.510(a).").

[119] § 164.510 ("Uses and disclosures requiring an opportunity for the individual to agree or to object: A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section.").

object or to designate whom they want involved and that, in the absence of taking either action, they have agreed to future disclosures by professionals using their judgment. Practitioners may also fail to affirmatively ask patients whom they want involved, believing that the privacy notice shifts the burden to the patients to tell them. Complaints of the following type may well be related to such an interpretation by health care personnel:

> [A] nurse came into her room to tell her that her brother called to ask about her. Later she learned from her mother that her brother received all of the information on her condition.

Physicians, in particular, may demonstrate a different, but related, interpretation of the opportunity to agree or object rule. When making hospital rounds, some physicians may, as a matter of course, chat with patients about non-medical matters when others are present. While they may intend this as an opportunity for patients to agree or object to the presence of their visitor(s) during the medical disclosures about to follow, patients may be waiting for, and expect, the physician to ask visitors to leave so they may speak privately. If the physician does not take the initiative, many patients will remain silent and not express their preference to talk alone, hesitating to overtly exclude others who may very much wish to remain.

Other health care personnel may also fail to properly provide the patient with an opportunity to agree or object. Not only might they fail to ask others to leave before asking personal questions or sharing sensitive medical information, but they may not consider that medical conditions sometimes impair patients' ability to be cognizant of or to voice objections to the presence of others:

> An employee came into her room and began asking questions. . . . [The patient] is diabetic[,] and her blood sugar was very low. . . . [S]he didn't realize her in-laws were in the room. . . . [W]hen she answered the question regarding miscarriages, her in-laws heard the answer, and it has caused problems in her personal life. . . . [T]he employee should have asked [them] to leave before asking those types of questions.

Section 164.510(b)(2)(i)-(iii)[120] of the HIPAA regulations does the most harm in this regard. It gives providers three options that they can regard as authorization to make a disclosure with the patient present: (i) the patient "agreed," (ii) the patient has the opportunity to

[120] § 164.510 ("Uses and disclosures with the individual present.").

object but did not, and (iii) the professional could judge from the circumstances that the individual did not object. Significantly, there is no mention that these options are to be considered in order, as a hierarchy for determining if patients have agreed to disclosure. On the face of the section, all options are equivalent, and that allows health care providers to infer from the circumstances that patients have not objected;[121] in the described situations, they may well make that inference. Particularly in the first circumstance involving the physician on his rounds, is it any wonder that the doctor might remain silent and judge from the circumstances that the individual did not object? We recommend that section 164.510(b) be modified to instruct providers to make best efforts to first obtain express consent from the patient for disclosures in the presence of others or for disclosures to others when the patient is not going to be present.

4. Restrictions on Sharing Information with Those Involved in Payment For Care

The privacy regulations allow institutions and providers to share information with family and friends involved in payment for the patients' care without stating any limitation on these disclosures. Significantly, the regulations define a familiar word, "payment," in a new way. According to section 164.501, "payment" means "the activities undertaken," not only by someone who is responsible for payment, but also by those who seek to obtain reimbursement.[122] Under section 164.502, the "covered entity," i.e., health care provider or health plan, may share protected health information for the purpose of "payment."[123] Assume for a moment that an institution or provider in good faith routinely provides to payor third parties what in their estimation is "the minimum necessary"[124] medical information to make the bill

---

[121] § 164.510(b)(2)(iii).

[122] 45 C.F.R. § 164.501; *see also,* O'Brien v. Cunard, 28 N.E. 266, 266 (1891) (physician not liable for battery or negligence when he vaccinated woman who raised her arm during a mass immunization. "If the plaintiff's behavior was such as to indicate consent on her part, he was justified in his act, whatever her unexpressed feelings may have been. In determining whether she consented, he could be guided only by her overt acts and the manifestations of her feelings."). *Cunard* is often cited for the proposition silence implies consent (*see, e.g.,* Prosser, *supra* note 21, at 101; Danuta Mendelson, Ph.D., LL.M., *Historical Evolution and Modern Implications of Concepts of Consent to, and Refusal of, Medical Treatment in the Law of Trespass*, 17 J. LEGAL MED. 1, 33 & note 55 (1996)). However, actors should be held liable where consent is readily verifiable but not sought. *See* James A. Henderson Jr., *Process Constraints in Tort,* 67 CORNELL L. REV. 901, 913 (1982).

[123] 45 C.F.R. § 164.502 (2006).

[124] § 164.502.

understandable. Covered entities are not obligated to specify in advance, i.e., give notice to patients, the types of specific medical information that will be disclosed under this provision nor an explanation for its need. Should they have to explain, it would likely become clear that the level of detail on bills has been determined to be most efficient for payment operations so that few phone calls or letters will follow asking for justification of charges. Because the "minimum necessary" may include names of tests, procedures performed, specialty clinic names, and names of providers, those responsible for payment may be able to infer significant medical information from billing charges. Patients who rely on others to pay their bills, if not made aware in advance of elements that will be included in billing information, will be deprived of an opportunity to make other payment arrangements should they object to the level of detail. We, therefore, recommend that the HIPAA regulations require privacy notices to specifically list the type of information the institution or provider puts on its bills. In addition, we suggest that covered entities offer patients options for details on bills.

5. Restrictions on Incidental Uses or Disclosures of Information

Another key issue relates to the HIPAA regulations' acceptance that incidental uses or disclosures will occur in the course of performing another permitted or required use or disclosure. Covered entities are required to have "appropriate administrative, technical and physical safeguards" against unauthorized intentional or unintentional disclosures or uses[125] and to train staff "as necessary and appropriate"[126] "with respect to protected health information."[127] The corollary of this section is that as long as covered entities take reasonable measures to safeguard intended disclosures or uses, incidental uses or disclosures do not violate the Privacy Rule. As an example, a physician wishes to share news with a patient about her condition. He requests permission to speak in the presence of her spouse, talks with them in a private area, and keeps his voice low as he speaks. If it turns out that another person, hidden from view, was present in the room and did not make his presence known, one could conclude that the physician followed "reasonable safeguards" to maintain the privacy of his patient and would not be liable for the disclosure to the third party.

Hospital personnel, however, commonly find themselves working in unforgiving circumstances: overcrowded environments with thin

[125] § 164.530.
[126] § 164.530(b).
[127] § 164.530(b)(1).

walls and thin curtains; many co-workers; multiple users accessing the same paper and electronic records; caring for more than one patient to a room. What personnel sometimes do not recognize is that environments which challenge their ability to protect privacy should instead be regarded as circumstances requiring them to take additional precautions against privacy infringements. Unfortunately, once precautions against disclosure are inconsistently and haphazardly applied, inconsistent and haphazard precautions become the norm. Ambulatory settings provide fewer excuses, yet similarly careless behaviors may carry over to that arena. From our study it appears that outcomes at institutions that consider themselves fully HIPAA-compliant do not always support that assertion, at least with respect to safeguarding non-electronic health information. The lack of specificity in the regulations for safeguards other than those applicable to electronic transmissions may be partially at fault for these failures to protect patient privacy. We suggest that the regulations should be expanded to specifically create behavioral, functional, and environmental standards for the purpose of eliminating incidental infringements on protected health and related personal information.

6. Accounting

Although patients have a right to an accounting of disclosures, the list of uses and disclosures excused from inclusion[128] forecloses any type of meaningful accounting. We question HHS's decision to not require covered entities to provide a complete list of disclosures. If, as a society, we feel comfortable that the benefit of making such disclosures convenient for covered entities outweighs the value of obtaining consent from patients in each instance, should the quid pro quo not be to require a complete accounting upon reasonable request from a patient?

Section 164.528(a)(1)(iii) excuses incidental uses or disclosures of health information from being included in an accounting if, with respect to the intended use or disclosure,[129] administrative, technical, and physical safeguards were in place,[130] the "minimum necessary" was revealed,[131] and the covered entity limits employees' access on a need to know basis.[132] There are several problems with excusing known incidental uses or disclosures from an accounting. First, if, as

---

[128] 45 C.F.R. § 164.528.
[129] § 164.502(a)(1)(iii).
[130] § 164.530(c)(1)-(2).
[131] § 164.502(b); § 164.514(d)(3).
[132] § 164.514(d)(2)(i)-(ii).

we argue above, reports of intended uses or disclosures of information should be provided to patients, it stands to reason that unintended ones must also be included. Second, unintended uses or disclosures, while perhaps not the result of negligence, still represent a communication that should not have happened and about which the patient is entitled to know. Third, patients should not have to engage in a dispute with covered entities that assert that all intended uses or disclosures were restricted to the appropriate parameters; they should instead be given the information they seek.

The sad truth is that it may be impossible for most institutions to track or fully determine how many individuals may have viewed or heard detailed private medical information outside of the "minimum necessary," "need to know," or "reasonable safeguards" standards, precluding a complete accounting in any case. Realistically, other than inadvertent electronic transmissions to unfamiliar destinations, very few disclosures by the institution would fall outside of the regulations' boundaries and, therefore, be noted in an accounting under the current standards.

We would recommend, therefore, the following revisions to the HIPAA regulations. First, health care workers should be required to report incidental uses or disclosures of health information to the institution's privacy office. Second, covered entities should fully account for all intended and incidental uses and disclosures of health information. Finally, accounting lists of uses and disclosures should be made easily available to patients upon request and at reasonable cost.

In sum, we believe that patients would be willing to accept a wide range of preauthorized disclosures if they could be assured that their privacy interests were taken seriously and that procedures were developed to protect them. This would require that all staff and providers: take seriously the vulnerability of patients' privacy in the health care context and act in a respectful and professional manner; understand their duty to limit disclosures to those with a need to know and to supply only the minimum necessary; and continually and scrupulously employ safeguards against incidental disclosure by being aware and adapting to the environment to minimize visual, aural, and physical exposure. Finally, accountability would need to be transparent, i.e., full accounting for uses and disclosures of health and personal information would need to be made available to patients.

B. Administrative Actions

A number of our findings also point toward recommendations that can be addressed to hospital administrators even if the HIPAA regulations are not revised. The concepts of privacy, confidentiality, and

dignity that date back to ancient Greece and engender widespread support in our own society provide sufficient normative force to successfully use less formal means to encourage administrators to focus on changing providers' and institutions' behavior. For health care institutions, private standard setting institutions, such as the Joint Commission for Accreditation of Healthcare Organizations (JCAHO)[133] and the Accreditation Association for Ambulatory Healthcare (AAAAHC)[134] may provide one type of support needed to foster change in focus and priority.[135]

Our first finding is that patients and their families filed privacy-related complaints with offices of patient affairs during the observation periods before and after implementation of the HIPAA Privacy Rule. By recognizing that every complaint represents the "tip of the iceberg," hospital leaders can gauge the magnitude of the problem and focus efforts to address these concerns. Because under-reporting exists, our first recommendation is for organizations to seriously evaluate each complaint and take appropriate action, especially if complaint reports cluster around certain locations or individuals.[136]

Our second finding is that privacy-related complaints can be reliably coded and classified. Analysis of these complaints enables institutions to identify patterns of unauthorized or impermissible disclosures associated with privacy policies. By sorting privacy-related complaints into subcategories and comparing trends in frequency of occurrence over time, administrators may learn about issues of particular importance at their facility. As an illustration, consider

---

[133] The JCAHO, an independent, not-for-profit organization, accredits close to 15,000 health care organizations in the United States. The Joint Commission, Facts About The Joint Commission, http://www.jointcommission.org/AboutUs/joint_commission_facts.htm (last visited Apr. 21, 2007). JCAHO's institutional accreditation is widely accepted and desired. *Id.* Institutions that comply with JCAHO's standards have obtained a nationally recognized measurement of quality. *Id.*

[134] The AAAHC currently accredits 2700 ambulatory care organizations. http://www.aaahc.org/eweb/dynamicpage.aspx?site=aaahc_site&webcode=home.

[135] *See* Robert D. Cooter, *Decentralized Law for a Complex Economy: The Structural Approach to Adjudicating the New Law Merchant*, 144 U. PA. L. REV. 1643, 1649–50 (1996) (explaining how norms generated within civil society become informally codified by private institutions and serve as standards for the relevant parties and how norms may be incorporated into the legal system by serving as sources of common law decisions or templates for positive enactments by statute or regulation).

[136] *See* James.W. Pichert et al., *Using Patient Complaints to Communicate Concerns to Colleagues, in* ACADEMIC COMPENSATION AND PRODUCTION REPORT 16, 16-19 (Med. Group Mgmt. Ass'n ed. (2004)) (discussing a model that the authors have found helpful to facilitate desired changes in behavior).

that only Institution 2 demonstrated a significant increase in privacy policy-related expressions of dissatisfaction. Following up this finding with a review of complaint reports might reveal, for example, that patients express concerns that they will not receive care unless they sign "HIPAA" forms or that staff inappropriately invoke, misapply, or do not understand HIPAA:

> Her husband was not allowed in the back with her[,] which he used to be. She was wondering what changed. Someone told her HIPAA. . . . [S]he stated that that didn't make sense. HIPAA doesn't have anything to do with it.

Administrators could use this information to try to find out the source of the perception; they may ask, for example, whether the reports accurately reflect what is happening? If so, are there underlying factors for the behavior, such as unmet educational needs, unclear policies and procedures, or questions of interpretation?

We recommend that organizations develop a plan to look for and respond to confidentiality and privacy issues. Coding, aggregating, and analyzing patient complaints have the potential to provide an early warning system for finding aspects of care and service that need improvement.[137] In addition, institutions that fail to take steps to identify and correct deficient policies or unacceptable behaviors or practices may place themselves and their employees at risk for legal consequences. Patient complaints about unauthorized disclosure or inappropriate use of their information may be the harbinger for claims under state law and civil and criminal sanctions under HIPAA.

Our third finding was that all health care personnel were associated with privacy-related complaints, including physicians in twenty percent of the cases. Institutional leaders have several tools at their disposal to decrease the incidence of privacy-related violations. Among these are carefully crafted and enforced policies and procedures that address issues of privacy and confidentiality, appropriate training and re-training, and assessments of job processes and work environments, which include making changes where needed. Physical and administrative supports must be in place to help health care personnel do the right things to protect patients' privacy and the confidentiality of their medical information. Monitoring patient complaint files for privacy-related complaints can help administrators determine if further training or modification of workplace environment and

---

[137] *See* Moore et al., *supra* note 78, at 1205-06 (analysis of patient complaint data may be more sensitive than traditional methods of peer review to proactively detect physicians' risk for medical malpractice claims).

workflow, or other action, is needed to deal with individual health care personnel who continue to engage in behavior that threatens privacy interests.

The HIPAA regulations require that health care personnel receive training.[138] We recommend that the trainings provided by institutions specifically emphasize why confidentiality and privacy are important and emphasize the need to maintain vigilance at all times to prevent breaches of confidentiality and protect privacy.[139] Redacted complaint reports might be used as part of such an educational program. Administrators should provide periodic retraining for all employees, physician and non-physician, with a particular focus on those individuals repeatedly associated with privacy-related complaints.

Once institutions begin to monitor and analyze patient complaints, they may identify individuals and units that generate a pattern of higher levels of privacy-related complaints than their peers. We would suggest that institutions consider implementing intervention programs that focus on individual outliers. Prior studies demonstrate the effectiveness of peer-based models to create desired changes in physician behavior.[140] Peer-based models have also been used to intervene with physicians generating disproportionate levels of patient dissatisfaction, and subsequent improvement in their patient complaint profiles has resulted.[141] Institutions that implement a program to notify outliers of their status should provide follow-up at regular intervals.

Our fourth finding, that privacy-related complaints were more prevalent after implementation of HIPAA's Privacy Rule, serves as a reminder to institutions that regulatory schemes do not necessarily solve local issues. They may represent the government's effort to achieve national priorities, but, as illustrated in this Article, they may imperfectly accomplish those goals. It is up to the administration of each facility, institution, and provider to independently assess the val-

---

[138] 45 C.F.R. § 164.530(b)(1) (2006); § 164.308(a)(5).

[139] In demonstrating the institution's commitment to maintain its patients' dignity and the individual staff member's role in fulfilling that mission, institutions might illustrate, for example, appropriate methods for "draping" patients and providing medical care in other ways that protect privacy, both visually and aurally.

[140] Wayne A. Ray et al., *Persistence of Improvement in Antibiotic Prescribing in Office Practice*. 253 JAMA 1174 (1985); *see, e.g.*, Stephen B. Soumerai & Jerry Avorn, *Principles of Educational Outreach ('Academic Detailing') to Improve Clinical Decision Making*, 263 JAMA 549, 549-50 (1990); James Mason et al., *When Is It Cost-Effective to Change the Behavior of Health Professionals?* 286 JAMA 2988 (2001); JOHN M. EISENBERG, DOCTORS' DECISIONS AND THE COST OF MEDICAL CARE: THE REASONS FOR DOCTORS' PRACTICE PATTERNS AND WAYS TO CHANGE THEM 104-08 (1986).

[141] Moore et al., *supra* note 78, at 1203.

ues of the organization, its customers, and its workforce and to create commonsense, workable, and enforceable local policies and procedures that protect and reinforce those values.

We wish to emphasize that private behavior of this nature can also be encouraged by HHS, even under its existing regulations, through the new public governance approaches of cooperative enforcement.[142] Privacy compliance officers at each institution should be involved in the analysis of each privacy-related complaint at an institution. A full root cause analysis should include a determination of the extent to which the offender's interpretation of what is allowable under the law contributed to the incident of which the patient is complaining. Privacy compliance officers are well situated to engage in reciprocal communication with regulators. Compliance officers can help regulators gain insight into aspects of the regulations that remain unclear, are misunderstood, or do not seem to adequately protect patients' interests, while regulators can inform compliance officers how the regulations have been judicially and administratively interpreted.

VI. CONCLUSION

Confidentiality and privacy concerns related to health care long pre-date the implementation of HIPAA. Our study described in this Article demonstrates that patients perceive and voice concerns about the way physicians, other health care personnel, and institutions handle confidentiality and privacy matters. While HIPAA attempted to establish a uniform, nationwide "floor" for protection of health information, the study demonstrates that implementation of the HIPAA Privacy Rule did not eliminate patient perceptions of threats to privacy and mishandling of confidential information in the medical care milieu.

The types of concerns patients express may be sorted into categories. Non-physicians were more commonly associated with privacy-related complaints than were attending or resident physicians. The

---

[142] *See, e.g.*, IAN AYRES & JON BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE (Oxford University Press 1992) (discussing alternative methods of creating government regulation); Michael Dorf, *Legal Indeterminacy and Institutional Design*, 78 N.Y.U. L. REV. 875 (2003) (discussing the ways in which institutions of government can collaborate to reduce the domain of legal indeterminacy); Jody Freeman, *Collaborative Governance and the Administrative State*, 45 UCLA L. REV. 1 (1997) (arguing that collaborative governance is superior to adversarial institutions); Richard H. Pildes & Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U. CHI. L. REV. 1 (1995) (discussing a variety of options for improving government efficiency); Louise G. Trubek, *New Governance and Soft Law in Health Care Reform*, 3 IND. HEALTH L. REV. 139 (2006).

increase in the proportion of privacy-related complaints relative to all complaint reports between the first and second observation periods for the institutions studied suggests that, compared to the pre-HIPAA period, these issues may now be of even more concern. The problem, in our view, is that the regulations in their existing form fail to take account of, or operationalize, patients' general and legitimate expectations of privacy in medical treatment settings.

Based on the findings of this study, we recommend a number of specific changes to the HIPAA regulations that would contribute to the protection of patients' privacy. These include supplementary regulations governing physical intrusion, clearer notice to patients, providing patients with an opportunity to agree or object to certain disclosures, restrictions on sharing information with those involved in payment for care, restrictions on institutional uses or disclosure of information, and expanded accountability to patients of uses and disclosures of health information.

Finally, we suggest that HHS could encourage private standard setting to promote changes in institutions' and providers' behavior through a public governance approach of cooperative enforcement. We believe it is imperative for administrators to look for areas in which their organizations fail to meet patients' reasonable privacy expectations and outline steps they may take to better satisfy these expectations.

Appendix
Table 2
CLASSIFICATION OF UNSOLICITED PATIENT/FAMILY COMPLAINTS CONCERNING CONFIDENTIALITY/PRIVACY-RELATED ISSUES

Environmental causes of disclosure: physical environment does not safeguard privacy or protected health information

1. **Lack of adequate safeguards:** PHI on computer screens, message boards, forms left in view; non-secured files.

"[I]nfo was out in the open for everyone to review." "[T]he chart was laying on the counter."

2. **Lack of physical privacy, exposure of the patient**:

"Patient upset that his roommate's physicians came into the room to insert chest tube and proceeded without providing privacy for either patient." "She was on the table with her legs in stirrups and in walks a social worker and students; she does not want to see anyone but her nurse and doctor."

Inappropriate disclosures: intentional disclosure clearly not within acceptable boundaries

3. **Identity theft:** resulted from a disclosure that took place at the medical center:

"[H]is personal info is printed on labels and passed around everywhere. . . . He is worried about identity theft."

4. **Impermissible disclosure:** individuals not directly involved in care viewed patient's medical record without legitimate cause, gossiped with people who are not treating health care providers, or disclosed information through illegitimate channels:

"Her ex's girlfriend who works for the medical center has accessed her medical record." "A nurse . . . told staff and other people outside of the Hospital about [patient's] emergency department visits."

Incidental disclosures: health care workers disclosed information to unintended recipients

5. **Mishandled/misdirected document or communication:** phone call, fax, or letter threatened confidentiality:

"Patient stated that she received another patient's test results in the mail." "He requested his medical records and received a page of someone else's." "She was handed another patient's biopsy report."

6. **Conversations between patient and HCP were overheard**:

"A male friend of mine was waiting with me to drive me home. The nurse said right in front of him, '[A]nd here is your prescription for your yeast infection.' I wished the floor would have opened up and swallowed me."

7. **Overheard staff conversation about a patient:** staff members discussed patient PHI; may include joke telling or disparaging remarks:

"She heard the nurse tell the next shift nurse that the patient was faking pain."

Too sensitive information: more private details than necessary are requested or documented

8. **Too much information requested or documented:** information was requested that complainant does not wish to provide, or does not see a need for, or more information than necessary was included in medical records:

"She saw in the chart, 'single/lesbian.' She said that this has nothing to do with her medically[,] and she feels violated."

Willful disclosures: disclosure made in the course of business

9. **Treatment-related disclosure where PHI is sent to another HCP or treatment-related covered entity**:

"Patient is upset that her bone density test results were sent to her family doctor without her knowledge or consent."

10. **Health care business operations-related disclosure:** occurred in the course of billing, reporting to a government agency, or other administrative function:

"I am a little confused on how they can charge me without me signing any release or hippa [sic] papers?"

11. **Notification of friends and family, disclosure to friends, family, and other personal associates of the patient:**

"She was very angry to find out that Dr. XXX had spoken to her mother over 5 times, and she needed him to know that if he did not stop doing that and breaking HIPPA (sic) that she would get a restraining order on him."

12. **Disclosure to employer or coworkers**:

"He believed that his records were confidential, but his employer said he received a copy of the records. He wants to know why they were released and who they were released to."

13. **Disclosure to a business entity not related to the patient's treatment:** business entity sought to market to the patient or otherwise use the patient's PHI in a way not directly related to the patient's medical treatment:

"Husband states they signed privacy notice in Admitting, yet several outside vendors called them at home to solicit their business, telling him they got the patient and newborn information from a hospital employee."

14. **Making information available to inquirers via patient directory**:

"Wife is very angry about a violation of her husband's privacy. She says that . . . he asked that he not appear on the hospital patient directory."

Privacy policy compliance issue*: *privacy policy is not properly complied with

15. **Refusal to provide access to—or a copy of—-the patient's medical records, or does not permit the patient to amend records:** provider not in compliance with privacy policy, for example, by refusing to furnish the patient's medical record or to permit him to correct errors:

"[S]taff member came up to her and told her she was not supposed to have the record, and snatched it from the patient."

16. **Inadequate documentation available**: hospital's written privacy policy or appropriate confidentiality-related documentation for notification or authorization unavailable:

"She asked for a form to sign saying the staff could discuss his medical issues and was told we do not have such a form; she

feels that with all the HIPAA laws we should have a form."

Dissatisfaction with privacy policy: privacy policy imposes burdens

17. Privacy policy obstructs access to information: used as excuse to not fulfill request:

"I feel let down and all because laws became an excuse to block all communication—not just prohibited disclosure. The community deserves better."

18. Problems with paperwork: too many forms to sign, or, in the case of HIPAA, patient refuses to sign a privacy notice:

"The clinic wanted her to sign the privacy information policy (HIPAA). She refused to sign."