Analysis & Perspective

PRIVACY VERSUS FREE SPEECH

The press often reports on abuses in health care, and many stories originate with whistleblowers who supply medical records to prove their tips. However, privacy restrictions in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) make it a felony for the press to obtain these records, much less report about them. Court challenges to HIPAA's limitations on press freedoms are likely, but there are vexing questions of constitutional doctrine, and the outcome is uncertain despite the U.S. Supreme Court's decision this term in *Bartnicki v. Vopper*, protecting the broadcast of a cell phone conversation intercepted by a whistleblower. Hospitals and medical professionals will be among those caught in the crossfire.

HIPAA, *Bartnicki*, and Public Interest In Inherently Private Records

RICHARD D. MARKS

On May 21, 2001, the U.S. Supreme Court ruled in *Bartnicki v. Vopper* that a radio commentator's broadcast of an illegally intercepted cellular telephone call was protected by the First Amendment. The commentator was not the person who intercepted the call, and the court's holding is explicitly limited to the unique facts of the case. Nevertheless, the reasoning of the majority, concurring, and dissenting justices portends profound difficulties for journalists, hospitals, and medical professionals under the Health Insurance Portability and Accountability Act of 1996, aimed at protecting the security and privacy of medical records.

Bartnicki's Facts

In 1992-1993, a labor union representing teachers at a Pennsylvania high school was engaged in contentious contract negotiations with the school board. Two union officials, one using a cell phone, held a conversation that was surreptitiously recorded by a person whose identity remains unknown.[1]

Richard D. Marks is a partner in the Washington, D.C. office of Davis Wright Tremaine LLP. He is chair of the Computer Law Division in the ABA Section of Science & Technology Law, a member of the National Conference of Lawyers and Scientists, and a Director of the Computer Law Association. He is also author of the white paper on HIPAA Certification for the Strategic National Implementation Process of the Workgroup for Electronic Data Interchange (WEDi/SNIP).

In the conversation, the two union officials discussed the difficulties of the negotiations. One remarked: "If they're not gonna move for three percent, we're gonna have to go to their, their homes ... To blow off their front porches, we'll have to do some work on some of those guys."[2]

The head of a local taxpayers' organization opposed to the union's demands testified that he found a tape of the call in his mailbox. He played it for some members of the school board, and later delivered a copy of the tape to a local radio commentator, who broadcast the tape on his public affairs talk show.3

The two union officials filed suit, seeking damages, fees, and costs, under federal and Pennsylvania statutes making illegal the interception of telephone calls (including cellular calls).[4] They argued that the head of the taxpayer's organization who first received the tape and the radio commentator who broadcast it knew or had reason to know that the recording was made illegally.[5]

The Courts Below

The parties filed cross motions for summary judgment in district court. Defendants asserted that they had no role in intercepting the call, and that their disclosure of it was protected by the First Amendment.[6]

The district court held that it is plainly illegal under the federal Electronic Communications Privacy Act, 18 U.S.C. §2510 et seq.,

[1] *Bartnicki v. Vopper*, No. 99-1687 (U.S. May 21, 2001), slip op. at 2; 121 S.Ct. 1753 (2001); 6 ECLR 574, 5/30/01.
[2] *Id*. at 2-3.
[3] *Id*. at 3.
[4] *Id*. at 4.
[5] *Id*. at 3.
[6] *Id*. at 4.

intentionally to disclose the contents of an electronic communication when the person "'know[s] or ha[s] reason to know that the information was obtained' through an illegal interception."[7] The district court also held that the federal and state "statutes were content neutral laws of general applicability," and were not a prior restraint. Therefore, the district court rejected defendants' First Amendment defense. However, the district court granted a motion for an interlocutory appeal, and certified the question of whether imposing liability based on the defendant's actions in turning over the tape and in broadcasting it violated the First Amendment.

The court of appeals, applying an intermediate level of scrutiny to what it viewed as content-neutral statutes, held nevertheless that the federal and Pennsylvania wiretapping acts "deterred significantly more speech than necessary to protect the privacy interests at stake," [8] and so remanded with the direction to grant summary judgment to the defendants.[9]

The Majority Opinion

The Supreme Court, in an opinion by Justice John Paul Stevens, affirmed 6-3. It held that the radio commentator's broadcast of the tape was protected under the First Amendment's "shield [for] speech about matters of public concern."[10]

The court accepted the plaintiffs' assumptions that the interception was intentional and unlawful, and that the defendants had reason to know it was illegal, so that defendants had violated the wiretap statutes. Consequently, the question was whether the statutes as applied violated the First Amendment.[11]

The court, concentrating on the federal act rather than its Pennsylvania counterpart, held that the wiretap prohibitions were content-neutral because they did not depend on the content or the views expressed in the intercepted communications.[12] Still, the court held that the statute's "naked prohibition against disclosure is fairly characterized as a regulation of pure speech,"[13] as distinguished from a regulation of conduct.

The court rejected as insufficient both interests advanced by the government to justify the statute: first, removing incentives for the interception of private communications and, second, minimizing harm to those whose communications are intercepted.[14] The first reason, discouraging illegal interceptions by punishing innocent recipients' later truthful publication of the intercepted content, was deemed too speculative to overcome the fundamental First Amendment interest in protecting public debate on matters of public concern.[15] The court reached this conclusion by relying on an unbroken line of cases protecting publication of information of public significance that was lawfully obtained by media publishers: "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need ... of the highest order."[16]

The court viewed the government's second asserted justification as by far the stronger of the two.[17] It assumed that minimizing harm to the people involved in private conversations justified penalties for the interceptor's own use of the illegally acquired content.[18] However, as to publication by the radio commentator--who had no role in performing or encouraging the interception of the cell-phone call--that interest was outweighed by the public interest in truthful dissemination of the conversation's content, involving as it did a matter of public interest (school contract negotiations with the union) and the mention of a threat of violence.[19]

The court quoted Warren and Brandeis' statement that "[t]he right of privacy does not prohibit any publication of matter which is of public or general interest."[20] The court noted that "[o]ne of the costs associated with participation in public affairs is an attendant loss of privacy."[21] It emphasized the profound commitment to preserving robust debate on public issues, and to the "'general proposition that freedom of expression upon public questions is secured by the First Amendment.'"[22]

The court explicitly refused to extend its holding beyond the facts of the case, and to answer generally "whether truthful publication may ever be punished consistent with the First Amendment."[23] It noted that the cases leave open the question of whether the state could punish a newspaper that unlawfully acquired information for both the illegal acquisition and the ensuing publication. Thus, its holding was confined to the situation where a commentator "obtained the information ... in a manner lawful in itself but from a source who has obtained it unlawfully."[24]

The Concurrence and Dissent

While joining the court's opinion, Justices Sandra Day O'Connor and Stephen Breyer concurred, in an opinion by Justice Breyer, for the purpose of explaining why the court's holding "does not imply a significantly broader constitutional immunity for the media."[25] Justice Breyer noted that the statutes in question did not forbid receipt of the tape itself, and he argued that "the speaker had little or no *legitimate* interest" in the privacy of the call because of the suggestion of violence, a "wrongful act" in Justice Breyer's view. Justice Breyer views the contents of the particular cell-phone call in question as falling within a privilege allowing reports of threats to public safety.[26] Among the examples he cites in support of this approach is a case holding that the psychiatric privilege is not binding when there is danger to the patient or others.[27] He reinforces this framework with the observation that the union officials involved in

[7] *Id*.
[8] *Id*. at 6.
[9] *Id*.
[10] *Id*. at 20.
[11] *Id*. at 9.
[12] *Id*. at 10.
[13] *Id*. at 11.
[14] *Id*. at 14.
[15] *Id*. at 17.
[16] *Id*. at 12.
[17] *Id*. at 17.
[18] *Id*. at 14.
[19] *Id*. at 18-19.
[20] *Id*. at 19.
[21] *Id*.
[22] *Id*.
[23] *Id*. at 13.
[24] *Id*.
[25] *Bartnicki*, concurring opinion, slip op. at 1.
[26] *Id*. at 4.
[27] *Id*. at 5.

the call "had a lesser interest in privacy than an individual engaged in purely private affairs."[28]

Because of the constraints of the facts surrounding the call and the legal doctrine applied as a result, Justice Breyer observes that the holding is narrow. It does not in his view "create a 'public interest' exception" to general privacy protections.[29] Moreover, Justice Breyer observes that "the Constitution permits legislatures to respond flexibly to the challenges future technology may pose to the individual's interest in basic personal privacy."[30] He sees legislatures revisiting privacy statutes, such as those punishing wiretapping, so that they are better-tailored and, consequently, more effective.[31]

In dissent, Chief Justice William H. Rehnquist, joined by Justices Antonin Scalia and Clarence Thomas, argues that the federal and Pennsylvania wiretap prohibitions are content-neutral because they are based solely on the manner in which the content is acquired (interception of electronic or oral communication).[32] This responds to the need Congress saw to protect privacy from invasions using new technology.[33] He contrasts this with the *Daily Mail* line of cases,[34] each of which involved a statute regulating a particular category of speech about governmentally held information (names of rape victims, juvenile offenders, or judges subject to review for disciplinary proceedings).[35]

Chief Justice Rehnquist argues that the majority placed "an inordinate amount of weight upon the fact that the receipt of an illegally intercepted communication has not been criminalized.[36] Further, he emphasizes that the wiretap prohibitions further the First Amendment interest in not inhibiting private communications.[37] He observes that the court has created an "inviolable" right to broadcast conversations of public importance:

> The Constitution should not protect the involuntary broadcast of personal conversations. Even where the communications involve public figures or concern public matters, the conversations are nonetheless private and worthy of protection. Although public persons may have foregone the right to live their lives screened from public scrutiny in some areas, it does not and should not follow that they also have abandoned their right to have a private conversation without fear of it being intentionally intercepted and knowingly disclosed.[38]

HIPAA's Statutory Scheme

In HIPAA, Congress sought to make the health care system more efficient. Congress mandated a large-scale conversion to electronic patient records and the use of specified standard transactions. Congress's goal is to make electronic data interchange (EDI) possible--and, indeed, required--within the United States for this set of routine health care transactions. Having patient records in electronic form is obviously necessary to this process. However, Congress also was concerned that electronic patient records would be easy for hackers to locate, copy, and publish worldwide, in an instant, via the Internet. HIPAA's privacy and security provisions therefore are designed to protect patients' privacy rights once their health records are converted to electronic form. Congress was aware of widespread public sentiment on patient privacy issues, and of the public's fears of wholesale invasions of the privacy of medical records.[39]

HIPAA requires that hospitals, physicians, health plans, clearinghouses, and other covered entities maintain a high level of privacy and security.[40] There are criminal as well as civil penalties for entities and individuals who breach these new statutory duties.[41]

---

[28] *Id*.
[29] *Id*. at 6.
[30] *Id*.
[31] *Id*. at 7.
[32] *Bartnicki*, dissenting opinion, slip op. at 4.
[33] *Id*. at 2-4.
[34] *Smith v. Daily Mail Publishing Co*., 443 U.S. 97 (1979) (name of juvenile defendant); *Florida Star v. B.J.F*., 491 U.S. 524 (1989) (name of rape victim); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975) (name of rape victim); *Landmark Communications Inc. v. Virginia*, 435 U.S. 829 (1978) (confidential proceedings of state judicial review commission).
[35] *Bartnicki*, dissenting opinion, slip op. at 5.
[36] *Id*. at 8.
[37] *Id*. at 7.
[38] *Id*. at 15.

[39] Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462, 82463-71 (2000), to be codified at 445 C.F.R. pts. 160, 164.

[40] 42 U.S.C. §1320d-2(d) states:
§1320d-2. Standards for information transaction and data elements
(d) Security standards for health information
(1) Security standards
The Secretary shall adopt security standards that--
(A) take into account--
(i) the technical capabilities of record systems used to maintain health information;
(ii) the costs of security measures;
(iii) the need for training persons who have access to health information;
(iv) the value of audit trails in computerized record systems; and
(v) the needs and capabilities of small health care providers and rural health care providers (as such providers are defined by the Secretary); and
(B) ensure that a health care clearinghouse, if it is part of a larger organization, has policies and security procedures which isolate the activities of the health care clearinghouse with respect to processing information in a manner that prevents unauthorized access to such information by such larger organization.
(2) Safeguards
Each person described in section 1320d-1(a) of this title who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--
(A) to ensure the integrity and confidentiality of the information;
(B) to protect against any reasonably anticipated--
(i) threats or hazards to the security or integrity of the information; and
(ii) unauthorized uses or disclosures of the information; and
(C) otherwise to ensure compliance with this part of the officers and employees of such person.

[41] 42 U.S.C.§1320d-6 states:
§1320d-6. Wrongful disclosure of individually identifiable health information
(a) Offense
A person who knowingly and in violation of this part--
(1) uses or causes to be used a unique health identifier;
(2) obtains individually identifiable health information relating to an

HIPAA will be implemented by security regulations that have yet to be published in final form and final privacy regulations which are already published.[42] It will also be attended by ongoing controversy.[43] The regulatory scheme is complicated. For example, the final privacy rules, plus accompanying commentary, require 367 pages in the *Federal Register*.[44] A description of the entire regulatory framework is the province of a book, not this short commentary. Rather, the focus here is on unauthorized access to, and publication of, protected patient records, including records of interest to the press and public, and how, under HIPAA, the courts will treat unauthorized disclosure of these records.[45]

HIPAA's Regulation of Disclosures by Whistleblowers

The press relies on tips and inside information for stories about alleged wrongdoing by hospitals, nursing homes, physicians, or health insurers. Often this inside information may include individually identifiable health records. Tipsters also alert federal or state health or law enforcement agencies to wrongdoing by health care providers and insurers, often in the context of *qui tam* litigation. What of HIPAA's effect on this kind of surreptitious disclosure? Can the hospital that employs the whistleblower be caught in a Kafkaesque scenario where it is liable for a tipster's actions that violate the hospital's own rules and procedures forbidding disclosure? Section 164.502 of the final HIPAA privacy rule[46] contains the general rules for uses and disclosures of protected health information. Subsection (j) is entitled, "Standard: Disclosures by whistleblowers and workforce member crime victims."[47]

The rule declares that a "covered entity"--for example, a hospital, health plan, or health care clearinghouse--is "not considered" to have violated the general rule against unauthorized disclosure of "protected health information" (PHI) if the disclosure comes from a member of the entity's workforce (the whistleblower) who "believes in good faith" that conduct at the covered entity "is unlawful or otherwise violates professional or clinical standards ... or potentially endangers ... the public."[48] The rule applies only if the whistleblower's disclosure is to a health oversight agency, public health authority, health care accreditation organization, or to an attorney retained by or on behalf of the whistleblower to help assess legal options.[49]

Plain Meaning and Legislative History

When HIPAA was working its way through the legislative process in 1995 and 1996, legislators and lobbyists concentrated on the parts of the act dealing with insurance portability and health care fraud and abuse. The introduction of electronic data interchange and its accompanying security and privacy protections received relatively scant attention. For example, there was no mention, much less lengthy or detailed analysis, of whether HIPAA's prohibitions on disclosure of health records might run afoul of the First Amendment, or present First Amendment issues that Congress should attempt to balance against the reasons for privacy protections. Put another way, there are no legislative findings on the questions surrounding the value of press scrutiny of potential wrongdoing or ineptitude in the health care industry, or the need to reconcile the potential adverse effect of press reports on the privacy rights of some patients.

This then is the background against which courts might be asked to construe investigative reporting of wrongdoing, in circumstances where the reports are based on protected health information--medical records of identified individuals--obtained by the press in violation of HIPAA. To give this a context, and for purposes of analysis only, here is a hypothetical scenario framed by HIPAA.

Suppose that a hacker illegally penetrates the information systems of a major medical center, downloads a large number of patient records (say, 1,000)[50] , and leaves disks containing the records in the mailbox of a local newspaper reporter. (Using disks, the hacker reasons, prevents law enforcement from tracing an email or similar transmission of the records. A hacker could use a variety of techniques to try to make the transmission anonymous, but our hacker is unwilling to take the small risk that very sophisticated technology, properly applied, could reconstruct the path back to him. The hacker considers the risk of being seen, and identified, when placing the disk in the reporter's mailbox to be much smaller, and therefore acceptable.)

Reviewing the disk, the reporters sees that the records may be interpreted to show a pattern at the medical center of failing to make, or to act early enough upon, diagnoses of serious diseases. In fact, there may be sufficient deficiencies to support seeking an accreditation review of the hospital. The records include the medical files of celebrities and politicians. Among the records are those of the governor and the chief justice of the state's highest court. Test results show that the governor's heart disease is much more serious than has

---

individual; or
(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b) of this section.
(b) Penalties
A person described in subsection (a) of this section shall--
(1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
(2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both.

[42] Final Privacy Rules, (to be codified at 45 C.F.R. pts. 160, 164).
[43] *See, e.g., Legislators Urge Bush Not to Weaken Contested Provisions in Medical Privacy Rule* (9 HCPR 881, 6/4/01).
[44] Final Privacy Rules, *supra* n.42.
[45] Final Privacy Rules, *supra* n.42, at 82464-71.
[46] 45 C.F.R. §164.502.
[47] 45 C.F.R. §164.502(j).
[48] 45 C.F.R. §164.502(j)(1)(i).
[49] 45 C.F.R. §164.502(j)(1)(ii).
[50] This is a realistic number, one that could easily be exceeded by a successful hacker. *See, e.g., Greg Farrell, Medical Records Particularly Vulnerable to ID Theft,* U.S.A. Today, Dec. 13, 2000, at 3B (successful hacker attack obtained thousands of patient records at University of Washington Medical Center); David Wahlberg*, Patient Records Exposed on Web,* The Ann Arbor News, Feb. 10, 1999 (thousands of patient records at University of Michigan Medical Center exposed to public access on Internet); *compare* Julekha Dash, *Health-Care Industry Looks at Security Risks*, ComputerWorld, Aug. 14, 2000 (theft of at least 23 patient records by temporary data-entry clerk at Dana-Farber Cancer Institute).

been described to the public. The chief justice's medical records reveal a diagnosis of cancer, a condition that has not been made public.

Arrest, Search, Seizure

The newspaper publishes the first in a series of articles about these revelations, using the medical records of the governor and chief justice as examples of the hospital's pattern of late diagnoses of serious diseases. Further articles by the same reporter are slated for publication over the next three days. However, on the afternoon of the day when the first article appears, the FBI comes calling. The reporter, editor, and publisher are arrested and led away in handcuffs. Search warrants are executed at the newspaper and the reporter's home and car.

Attempts by the paper to quash the search warrants are unsuccessful. An assistant U.S. attorney successfully argues to a federal magistrate judge that "merely obtaining" individually identifiable medical records without authorization violates 42 U.S.C. §1320d-2, d-6. Moreover, disclosing unique health identifiers and individually identified health information without authorization is per se a violation of the statute. Further, adds the government attorney, the disclosures in this case appear to be acting in concert with a hacker who used false pretenses. Moreover, publication by the newspaper appears to show that disclosure was made, in the words of the statute, "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm."[51] The malice is the hacker's, argues the government, and the commercial advantage and personal gain are inarguably among the newspaper's motivations--the publishers are trying to sell papers.

Indictment

Soon, indictments of the reporter, editor, and publisher follow. They all are charged under 42 U.S.C. §1320d-2, d-6, and, if convicted of all charges, face a maximum of 10 years in prison and a fine of $250,000 each.[52] Moreover, the chief executive and the chief of information systems of the hospital also are indicted under the same sections of the statute, but for lesser offenses, so that each faces the possibility of a year in prison and a $50,000 fine.[53]

Class Action and Downstream Lawsuits

Shortly after the indictments become public, a class action is filed on state law negligence and invasion of privacy grounds against the hospital, its chief executive officer, chief information officer, and board of trustees. The hospital's principal computer system vendors are also listed as defendants, on the theory (as explained in the complaint) that they furnished medical record computer systems that lacked adequate security features to satisfy HIPAA's standard of care. The complaint alleges that the hospital, its officers, directors, and employees (and its systems vendors) failed to implement the standard of care for security and privacy demanded by HIPAA. The suit seeks damages for the patients' emotional distress as well as damages for loss of employment and inability to buy insurance, alleged specifically on behalf of several members of the class who suffered these consequences after the public release of their medical records.

Two weeks go by, and the newspaper is sued by the hospital and the other defendants in the class action. The plaintiffs' theory is that the publisher, editors, and reporters at the paper acted negligently (under the standard of care mandated by HIPAA) in not safeguarding the medical records once they realized what had been given to them by the hacker, and in fact then conspired with the hacker to commit the intentional tort of invasion of privacy. The suit is joined some time later by a number of the patients whose identified medical records the paper published, also seeking relief on invasion of privacy grounds. The governor is among these plaintiffs.

Constitutional Doctrine and Legislative Intent

How do these facts fare under a *Bartnicki* analysis?

Perhaps the starting point is that HIPAA makes it a crime knowingly to "use," or "cause to be used" a unique health identifier; to "obtain" individually identifiable health information; or to "disclose" that information to another person.[54] HIPAA thus presents the "still-open question"[55] that the court in *Bartnicki* specifically stated it was avoiding: Whether Congress can constitutionally make criminal the "mere" obtaining of illegally intercepted content.[56]

A related question is whether Congress made sufficient findings before passing HIPAA to support this criminal prohibition. A third question, one closer to *Bartnicki's* facts, is whether publication of the medical records, which were obtained by the newspaper without proper authorization under HIPAA--and therefore obtained and possessed illegally--is also a criminal act.[57]

There is apparently no legislative history about how Congress viewed the balance between the press's robust reporting of alleged wrongdoing in the health care system and preservation of the near-absolute privacy of patients' medical records. An unbiased reader of HIPAA's legislative history might conclude that Congress's view of this balance can only be inferred (though the inference may be strong). Similarly, there is no legislative history illuminating Congress's view about the First Amendment value of reporting public figures' medical records, and how that should be balanced against public figures' privacy interests. Apparently, these questions were not considered in the legislative process that produced HIPAA.

Courts may infer from reading HIPAA, and especially 42 U.S.C. §§1320d-2, 1320d-6, that Congress obviously intended to, and did,

---

[51] 42 U.S.C. §1320d-6 (b)(3).

[52] *See* 42 U.S.C. §1320d-6 (b)(3). The indictment charges intent to use the medical records for commercial advantage and personal gain.

[53] *See* 42 U.S.C. §1320d-6 (b)(1). The indictment charges disclosure of individually identifiable health information to another person through the hospital's (and its officers' and directors') knowing failure to implement the safeguards required under 42 U.S.C. §1320d-2 (d)(2) ("ensure" against "any reasonably anticipated ... threats or hazards" to security, integrity, and unauthorized uses or disclosures of an individual's medical records).

[54] 42 U.S.C. §1320d-6 (a).

[55] *Bartnicki*, slip op. at 13.

[56] Section 1320d-6 (a)(2) makes it a criminal offense for a person "knowingly and in violation of this part" to "obtain[] individually identifiable health information relating to an individual." (Emphasis added.) As the court in *Bartnicki* emphasized, it has yet to face a case where a statute "proscribe[d] receipt" of information. Slip op. at 10 (citing *Florida Star v. B.J.F.*, 491 U.S. 524, 536 (1989)).

[57] Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on a defect in a chain? Slip op. at 13.

treat *all* individually identifiable medical records as a special category of information. That is, Congress identified a class of speech defined solely by its content. (Whether this category is content-neutral for purposes of constitutional adjudication is of course a separate question.) Further, Congress intended to protect all the information in this special category with a high level of security and with detailed privacy restrictions. Will courts require more support for these propositions when the congressional intent and rationale are so clear from the face of the statute, and when concerns for privacy generally, and medical record privacy in particular, are so easy to document?

Public Interest, Private Records

Does HIPAA create an exception to the thrust of *Times v. Sullivan*?[58] Is there now a HIPAA-imposed rule that the medical records of public figures lie in the same category as the medical records of the general public, so that all of these records are entitled to HIPAA's strong protections against disclosure (unless the disclosure is made, or specifically authorized by, the patient)? This is a threshold question before the trial court as it considers the criminal liability of the newspaper and its publisher, editor, and reporter who "obtained" the disk and, upon realizing what it contained, failed to safeguard its contents and to turn it over to the police immediately.[59]

One of the difficulties facing the trial and appellate courts in analyzing this issue is the lack of any congressional hearings or debate on the role of the press in continuing to report on the health care system. Without evidence in the legislative history that Congress considered the important balance between free press values and patients' privacy interests when it enacted HIPAA, will courts be willing to impose the plain language of HIPAA on how the press can, or must, deal with individually identifiable health records that come into its possession from whistleblowers (supposed do-gooders) or wrongdoers? Will courts see a justification for imposing a different rule for patients who are public figures, under a *Times v. Sullivan* rationale? Do the medical circumstances of the public figure, or the circumstances under which the press "obtains" the medical records, allow or require courts to enforce HIPAA differently? Conversely, does the lack of legislative history for all these issues demand a uniform imposition of HIPAA's high security and privacy standards--and uniform penalties for failing to adhere to them?

Strict Scrutiny

Some of this analysis may be expressed in terms of whether "strict scrutiny" is the appropriate test for courts to use in testing HIPAA.[60] If so, courts may demand specific, careful legislative findings to buttress imposition of criminal sanctions for merely obtaining protected patient records, where the press, as a passive recipient, has no role in acquiring the information. Of course, whether the press's subsequent use and disclosure of protected health information so received converts its role from passive to active, and therefore criminal, is also part of the mix.

The press will argue that HIPAA's criminal framework is just the kind of "naked prohibition against disclosures ... fairly characterized as a regulation of pure speech,"[61] requiring imposition of "strict," rather than "intermediate," scrutiny.[62] They will also argue that strict scrutiny is required because 42 U.S.C. §1320d-6(a) is a "flat ban against unauthorized speech about medical records.[63] Whether strict or intermediate scrutiny is appropriate depends in part on whether HIPAA's prohibition against unauthorized use or disclosure of medical records is categorized as "content neutral." In *Bartnicki*, the court held that the federal and Pennsylvania wiretap statutes in question both were content neutral because their application did not depend on the contents of the intercepted conversations.[64] (*Bartnicki* did not involve the flat-ban issue.)

HIPAA's prohibitions of course are directed at records defined by their content. There is a careful, content-based definition in the statute of "individually identifiable health information,"[65] and the final privacy rule also defines "protected health information" based on its content.[66] The definitions may be described as "content neutral" only in the sense that they do not depend on whether the information is long or short, comprehensive or partial, or on whether the medical news might be considered routine or exceptional, good or bad.

Narrow Tailoring

This article is not the place to examine the various analytical paths to different definitions of "content neutral." Suffice it to say that helpful analogs to the problems of singling out medical records for unique treatment under the First Amendment may be the definitional issues surrounding classified information,[67] commercial speech, and obscenity and indecency. These doctrinal paths probably lead to the question of whether HIPAA's prohibition against the unauthorized use or disclosure of patients' medical records is "narrowly tailored" to

---

[58] *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) (imposing the "actual malice" standard under the First Amendment to protect and encourage reporting about "public officials"). For development of the *Times v. Sullivan* doctrine and its extension to "public figures," see generally *Milkovich v. Lorain Journal Co*., 497 U.S. 1 (1990).

[59] The final privacy rule, 45 C.F.R. §164.502(j)(1)(ii)(B) states that a "covered entity" is not considered to have violated the rule's confidentiality restrictions if there is disclosure by a whistleblower to (among other choices) an attorney retained by the whistleblower to advise about legal options. Attorneys in this situations should note that nothing in the statute exempts them from 42 U.S.C. §1320d-6 (a)(2), making the obtaining of individually identifiable health information subject to the criminal penalties in 42 U.S.C. §1320d-6 (b).

[60] *Cf. Bartnicki*, concurring opinion, slip op. at 2.

[61] *Bartnicki*, slip. op.. at 11.

[62] *See Bartnicki*, slip op. at 6.

[63] *See R.A.V. v. City of St. Paul, Minn.,* 505 U.S. 357, 381 (1992) (holding facially unconstitutional city's bias-motivated crime ordinance, on grounds that "it prohibits otherwise permitted speech solely on the basis of the subjects the speech addresses," and declining to reach the issue of overbreadth (see supra n.77)).

[64] Slip op. at 10-11.

[65] 42. U.S.C. §1320d (6).

[66] Final Privacy Rules, 65 Fed. Reg. at 82496-97.

[67] *Compare Snepp v. U.S.,* 444 U.S. 507 (1980) (per curiam) (upholding validity of secrecy agreement required for employment by the Central Intelligence Agency), with *New York Times Co. v. U.S.*, 403 U.S. 713 (1971) (per curiam) (the "Pentagon Papers" case) .

effect the legitimate privacy interests that Congress is seeking to protect.

That, in turn, leads back to whether Congress made sufficient findings to enable a useful analysis of the sufficiency of its tailoring of HIPAA to meet Congress's specific goals. There will be great temptation for courts simply to assess Congress's goals from the plain meaning of HIPAA's statutory language, and hold that the obvious privacy interests in everybody's medical records sustains the definitions--which a court of this mind would classify as "appropriately narrow"--of individually identifiable health information, and its permissible uses and disclosures.

Public figures will argue that their medical records are entitled under HIPAA to exactly the same protection as anybody else's. (There is no exception in HIPAA permitting less confidentiality for the medical records of political office holders, celebrities, or anyone else, and no mention in HIPAA's legislative history of consideration of any exception of this kind.) Under this view, the public release of officeholders' medical records should be allowed only if the patient authorizes their release because of a public relations, political, or a similarly personal calculus, and not because of an exception (or loophole) created by judges. After all, as the preamble to HIPAA's final privacy rules states, the willingness of any patient to enter into a frank exchange of information with doctors depends on the patient's assurance that the information will be disclosed only to those who need to know it for purposes of diagnosis and treatment (and payment for the care). Nothing in a public figure's status diminishes those privacy interests, nor the First Amendment interest in encouraging the *private* speech between patient and caregiver.[68]

A separate set of questions attends the issue of whether civil and criminal liability is appropriately imposed upon the hospital and its officers and directors for the disclosure of medical records released through the whistleblower's actions. Recall that the Final Privacy Rules specifically declare that a "covered entity" will not be held liable for a disclosure in these circumstances.[69]

Doubts About the Whistleblower Rule

However, the class-action plaintiffs (the people whose medical records were disclosed by the newspaper) will argue that the whistleblower rule adopted by the secretary is contrary to HIPAA, and in any event guides only HHS's enforcement of civil penalties under the Final Privacy Rules. They will argue that the whistleblower rule is not a limitation on enforcement of HIPAA's criminal penalties by the Department of Justice, nor on tort, contract, and other state and federal causes of action available to civil plaintiffs (such as violation of state and federal consumer protection laws).

Moreover, it is not at all clear that the courts will sustain the exemption for a covered entity's liability under the Final Privacy Rule when a whistleblower causes the breach of confidentiality. Nothing in the plain language of Section 1320d-2 (d)(2)--or any other section of HIPAA or its legislative history--offers any basis for this exception. Consequently, plaintiffs in court cases who also complain to HHS and seek enforcement action are likely to challenge Section 164.504 (j) and seek its invalidation. Their argument will be that the exception is facially inconsistent with the plain language of Section 1320d-2 (d)(2). They will point out that a covered entity's internal security threats are foreseeable, and, indeed, that it is well known in the security industry that the greatest threats are internal. Therefore, a whistleblower threat falls squarely within Section 1320d-2 (d)(2)'s requirement that a covered entity maintain safeguards to "ensure" the integrity and confidentiality of medical records and "protect against any reasonably anticipated ... threats or hazards ... and ... unauthorized uses."[70]

Because of this facial inconsistency, HHS's interpretation of the statute as expressed in Section 164.504(j) of the Final Privacy Rule, may not be entitled to *Chevron* deference.[71] The first step in a *Chevron* analysis is to ask "whether Congress has directly spoken to the precise question at issue."[72] If it has, the matter ends because courts and agencies (including executive departments) "must give effect to the unambiguously expressed intent of Congress."[73] Only if the court finds "that the statute is silent or ambiguous with respect to the precise question at issue,"[74] does the court proceed to the second *Chevron* step of asking whether the agency has construed the statute permissibly. Only in the second step is the agency's interpretation due "substantial deference."[75]

Whether or not the rule is ever invalidated, its usefulness for hospitals and other covered entities is in great doubt in civil suits under state law. The hospital in our hypothetical example may seek a ruling of law (or, later, a jury instruction), based on this part of the privacy rule, that the hospital cannot be found negligent for failure to supervise the whistleblower, or for failure to prevent the whistleblower from hacking the hospital's systems. Its theory would be that Section 164.504(j) exempts hospitals from HHS sanction in this circumstance, and that courts should adopt the same approach. That will be a hard sell under state tort law. After all, the very issue to be tried is whether the hospital's conduct is negligent. Under all these circumstances, courts are likely to find that they owe little if any deference to the Secretary's interpretation.

Technology, Public Issues, and Fundamental Rights

The flat ban on press coverage of health issues that lurks in HIPAA may well be vulnerable to constitutional challenge. However, the road in this kind litigation is often long,[76] and the risks in the interim are real. Any reporter who is thinking about a story that draws support from surreptitiously obtained medical records, any editor and publisher faced with the opportunities and obligations that a story like this carries, and any lawyer called upon to give pre-publication advice, faces risks far graver than before. The uncertainties are enormous.

The constitutional analysis of free-press privacy issues in light of HIPAA is beset with proliferating issues. Initially, juries may decide some of the more important constitutional questions, at least in the first instance. They may do so in cases where plaintiffs have suffered

---

[68] *Bartnicki*, dissent, slip. op. at 7.

[69] Final Privacy Rules, 65 Fed. Reg. at 82504-05; 45 C.F.R. §164.504 (j).

[70] 45 C.F.R §1320d-2 (d)(2).

[71] *Chevron U.S.A. v Natural Resources Defense Council Inc*., 467 U.S. 837 (1984).

[72] *Id*. at 842; *see e.g., U.S. Telecom. Assn. V. F.C.C.,* 277 F.3d 450, 457 (D.C. Cir. 2000).

[73] *Chevron* at 842-43; *see U.S. Telecom*, 277 F.3d at 457.

[74] *U.S. Telecom*, 277 F.3d at 457.

[75] *Id*. at 457-58.

[76] *See, e.g., Community-Serv. Broad. of Mid-America, Inc. v. F.C.C*., 593 F.2d 1102 (D.C. Cir. 1978)(section of Communications Act held invalid on First Amendment and equal protection grounds).

kinds of harm with enormous emotional appeal--there but for the grace of fortune go I (and my medical records, now public on the Internet, for all, including employer and insurance company, to see). These are the kinds of cases where juries may want to send messages. In settings like this, the long-term value of preserving robust, critical reporting by the press is not easy for jurors to see. That may be all the more true because so much technology is available to make enterprise security better. The fact that the technology is by no means fail-safe, is expensive to deploy, and is not yet engineered for health care uses may not give juries much pause.

It may be too early to handicap a declaratory judgment attack against HIPAA's muzzling of the press. Much will depend on how the case is brought--on its facts, and on how the record is developed (related but distinct elements). Yet the intention here is not to be pessimistic. Congress, in its sincere attempts to anticipate the potential loss of loss of privacy once medical records are converted to digital form, went too far in parts of HIPAA. Courts--and soon enough the U.S. Supreme Court--may be asked to ameliorate the overbreadth.[77]

HIPAA's statutory language evinces Congress's judgment that medical records are inherently private, without regard to circumstances, unless the patients themselves authorize release. Even then, the release need not be general or public. Under the statute and the HIPAA privacy regulations, medical records can be authorized for release for very specific purposes only. In those situations, the privacy and security of the records for all other disclosures and uses must still remain intact.

Because Congress's goals are so apparent, the absence of a well-developed legislative record to explicate them may not matter in many of the press cases arising under HIPAA. Courts will be able to enforce the statute and its complicated implementing regulations--or rely on HIPAA as a reference to establish duties of care under state law--with little hindrance. In other words, in many--but not all--of these cases, HIPAA (whether attacked on its face or as applied) may survive strict scrutiny, in part because courts will rule that the statute (sometimes alone, sometimes as implemented through HHS's regulations, sometimes as a reference point for state tort-law theories) is sufficiently narrowly tailored to cover the facts at issue.[78] Where along the spectrum of public interest this rationale may weaken, and where the tailoring may no longer be sufficient, probably will be developed in a manner akin to the evolution of the *Times v. Sullivan* constitutional privilege.

When the privacy rights created under HIPAA clash with First Amendment press rights, the job before the courts will not be easy. Here Congress is facing direct, established limitations on its powers, though the extent and shape of those limits will not be clear early in HIPAA's litigation history. Will judges insist on a better legislative record before they are willing to read HIPAA as criminalizing the press's receipt or use of individuals' medical records in reporting news and uncovering wrongdoing (questions closely related to what is left open in *Bartnicki*)? Will it matter how the press uses these records? That is, will First Amendment protection hinge on the content of the reporting? Will First Amendment protection for press reporting of medical histories translate into an extension of the *Times v. Sullivan* privilege for revealing certain medical records in which the public has a "legitimate" interest? Will there be different rules for public figures who are not public officials, when medical records are at issue? Or might the courts conclude that even public officials, or public figures generally, are entitled to absolute privacy, or something close to it, for their medical records? For now, reporters and editors can only guess at the boundaries, and part of the price for misjudgment may be criminal prosecution.

Conclusion

HIPAA is designed to accelerate the spread of digital technology in the name of efficiency in health care, and to protect against new threats resulting directly from the employment of digital technology. Ironically, HIPAA will have major unintended effects as well. It paints a bullseye on hospitals, physician practices, and other enterprises in the health care system. Hackers' attention will be drawn to medical records, and the challenges of stealing them, as never before. The allure of harm and havoc, the danger of raised stakes--these will be part of HIPAA, too. For some time to come, hackers probably have the edge. Will they use it? And who bears the most risk from their attempts?

HIPAA will set in motion new challenges to fundamental rights and to the constitutional doctrines designed to protect them. What right does the press have to uncover and report problems in the health system, when the coverage inevitably deprives some people of their right to the privacy of their medical records? How well can courts resolve these clashes? Can Congress be convinced that HIPAA needs revision even before it is fully implemented?

As legislatures react to the startling new benefits and threats of digital technology--seeking to promote the good and bottle-up the bad--courts will face seemingly endless challenges in fitting established doctrine to new, technologically driven social patterns. The HIPAA saga, an exemplar, has just begun.

---

[77] The word is used in the sense of the U.S. Supreme Court's overbreadth doctrine. *See Broaderick v. Oklahoma*, 413 U.S. 601 (1973); see generally Tribe, American Constitutional Law 1022-29 (2d ed. 1988).

[78] *But see US West Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied sub nom. Competition Policy Inst. v. US West Inc.*, 120 S.Ct. 2215 (2000) (FCC order requiring opt-in regime for marketing of consumer information invalidated on grounds that privacy protections created burden on free speech and were not narrowly tailored).