Medication Adherence Technology: Medicine of the Future, Emerging Privacy Concern

Katharine Boshinski Sparks
MEDICATION ADHERENCE TECHNOLOGY:
MEDICINE OF THE FUTURE, EMERGING PRIVACY CONCERN

Katherine Boshinski Sparks*

I. INTRODUCTION

Despite significant advances in medical technology, American doctors face a growing problem: the number of patients who do not take their medication as directed.1 This non-compliant behavior occurs in patients with relatively minor medical issues as well as those with life threatening conditions, and it has become a large and costly problem for American health providers.2 In 2010, the New England Journal of Medicine reported that patient non-compliance costs the healthcare system $100 billion per year in additional hospital stays and results in thousands of preventable deaths.3

Health Information Technology ("Health IT") companies are eager to provide a solution to the problem. Some have developed innovative "smart packaging"4 that alerts the patient's physician when a medicine bottle is opened or a pill is pushed out of the blister pack.5 If no signal is received

* J.D. Candidate, The Catholic University of America, Columbus School of Law, May 2012; B.A., University of Georgia, 2008. The author is grateful for the advice and guidance of Professors Mary Cheh and Clifford Fishman, the love and encouragement of her parents, and the unwavering support of her husband, Jonathan Sparks. The author also wishes to thank the Journal of Contemporary Health Law and Policy editors and staff for their hard work.


2. Id at 1553-54.

3. Id at 1553.


5. Id. A blister pack refers to a particular kind of packaging where the pills are displayed through plastic attached to cardboard or another material. The pills are pushed out through the back of the card. This kind of packaging is particularly effective for
the physician can call the patient to remind him or her about the missed pills. More advanced pill technology is also in development—specifically through the use of ingestible microchips embedded in medication. These microchips are designed to transmit a signal when the medication is ingested or even metabolized.

Although this emerging technology has many beneficial uses, it also poses a serious threat to patient privacy and can constitute invasive medical surveillance. First, this Comment will discuss the recent emergence of medication adherence technology and the privacy issues implicated by its use. Next, this Comment will consider how courts are likely to react to medication adherence technology. Finally, this Comment will discuss several possible legal responses to the privacy concerns raised by medication adherence technology.

II. MEDICATION ADHERENCE

The term "medication adherence", also called medication compliance, indicates how closely a person’s behavior complies with his or her doctor’s treatment instructions. Failure to follow a doctor’s instruction manifests itself in a variety of forms. For example, the patient who never fills the adherence purposes because it is apparent from looking at the pack whether the patient has taken a particular day’s worth of pills. See also William M. Glazer, New Tools for Managing Non-adherence: Providers Recognize the Value of Compliance, but What Can They Feasibly Do About It?, BEHAVIORAL HEALTHCARE (Apr. 1, 2010), http://www.behavioral.net/article/new-tools-managing-non-adherence.


8. Id.


prescription he is given; the patient who fills it but never takes the pills; and the patient who intends to take the pills faithfully but frequently forgets to take them exhibit non-adherent behaviors.\textsuperscript{11}

A. Problems with Non-Adherence

Sometimes referred to as “America’s Other Drug Problem,”\textsuperscript{12} misuse and nonuse of prescription medications is rampant.\textsuperscript{13} It is estimated that 54\% of American adults do not take their medication as instructed.\textsuperscript{14} At the same time, there is abundant evidence that failure to take medication as prescribed can lead to a host of health issues.\textsuperscript{15} According to the New England Healthcare Institute, medication non-adherence is responsible for an estimated $300 billion each year in health care expenditures,\textsuperscript{16} $100 billion of that cost for hospitalizations that could otherwise be prevented by proper medication use.\textsuperscript{17}

Medication adherence is particularly a problem for the elderly population. Surveys indicate that 90\% of elderly Americans take one or more prescription medications per week\textsuperscript{18} and 41\% take five or more a week.\textsuperscript{19} Complicated dosing regimens can increase the difficulties already faced by aging patients, who often suffer from decreased eyesight or mobility.\textsuperscript{20}

\textsuperscript{11} Id.


\textsuperscript{13} See id.

\textsuperscript{14} PHARM. COMMERCE, supra note 10.


\textsuperscript{16} Id.

\textsuperscript{17} Experts Try To Fix Problem of Millions Who Don’t Adhere to Prescriptions, KAISER HEALTH NEWS (May 10, 2010), http://www.kaiserhealthnews.org/Daily-Reports/2010/May/10/Unadherence.aspx.

\textsuperscript{18} CTR. FOR TECH. & AGING, supra note 15, at 5.

\textsuperscript{19} Id.

\textsuperscript{20} Id.
Forgetfulness, confusion, or financial constraints can also make adherence difficult. Whatever the cause of non-compliance, however, statistics show that seniors who do not follow their medication regimens are 76% more likely to suffer a "major decline in total health" than their peers who do.22

Besides the obvious harm to patients' health, non-adherence is problematic for the health industry in general. Pharmaceutical companies, insurance companies, and pharmacies lose potential profit for every pill not purchased as a result of non-adherent behaviors.23 In response, the health care industry is developing Health IT solutions to boost patient compliance.

B. Health IT as a Solution for Non-Adherence

To combat the growing problem of non-adherence, health providers are developing some inventive solutions.24 Health IT, specifically technology that can remind patients about their medications, is a possible solution to the problem. In conjunction with health providers, several companies are developing information technologies meant to improve patient adherence.25 Supporters of Health IT claim that it will make a positive improvement in the medical field through its ability to reduce medical errors, such as those caused by inaccurate drug coding or patients forgetting what medications they are taking so the physician can avoid possible negative interactions.26

21. Id.


23. Alexander S. Misono et al., Healthcare Information Technology Interventions to Improve Cardiovascular and Diabetes Medication Adherence, 16 AM. J. OF MANAGED CARE SP82, SP91 (2010).

24. The most immediate solutions include: 1) simplifying medication regimens by decreasing the frequency of doses, 2) speaking with the patient to try to discover why they are not taking the medication consistently—whether this is due to financial problems, personal beliefs about medicine, etc.—and 3) suggesting reminder techniques, such as setting an alarm. CTR. FOR TECH. & AGING, supra note 15, at 14.


26. Daniel J. Gilman & James C. Cooper, There is a Time to Keep Silent and a Time to Speak, the Hard Part Is Knowing Which Is Which: Striking the Balance Between
Additionally, proponents argue that having patient information available electronically will decrease the administrative costs of facilitating communication between healthcare providers. According to one report, "[n]o aspect of Health IT entails as much uncertainty as the magnitude of its potential benefits." One of those benefits is its capability to significantly increase patient adherence.

III. COMPLIANCE TECHNOLOGY: YOUR MEDICINE IS CALLING

A. Adherence Packaging

One of the ways pharmaceutical companies are trying to combat the adherence problem is through pharmaceutical packaging. Clear directions and a simple dosing schedule help make adherence easier for patients. This type of format is used today in many blister packs, which generally include calendars to indicate when pills should be taken. These packs have the added benefit of providing a clear visual for patients to keep track of whether they have taken their pills.

A more recent development in the pharmaceutical packaging industry is the use of electronic packaging. The electronic age is opening up new avenues for promoting adherence with novelties such as blinking pill bottles or text messages that alert patients when it is time to take their medication. The newest electronic packages are even capable of storing information

---


27. Id. at 290.

28. Id. at 291.


30. Id.

31. Id.

32. Id.

33. Matthews, supra note 4.

34. Id.
about the patient’s adherence. \footnote{35}{See, e.g., Joe Dysart, *Take as Directed* a lot Easier with these New Tools, DRUG TOPICS (Aug. 20, 2007), http://drugtopics.modernmedicine.com/drugtopics/Top+News/Take-as-directed-a-lot-easier-with-these-new-tools/ArticleStandard/Article/detail/450125.} For example, some can record the time and date the medication is opened. \footnote{36}{Id. One of the most successful electronic compliance packages thus far is Cerepak®, developed by MeadWestvaco Corporation. By way of a tiny microprocessor, this blister pack records the time and date that each dose is taken. Information about patient compliance can then be uploaded to a computer and examined by the prescribing doctor. *Cerepak® Electronic Compliance Packaging*, MWV, http://www.meadwestvaco.com/HealthcarePackagingSolutions/AdherencePackaging/mwv021872 (last visited Feb. 26, 2012).}

Moreover, many of the designs can electronically transmit the information they gather. \footnote{37}{Matthews, supra note 4.} For example, the “GlowCap,” a product designed by Express Scripts Inc., is an electronic cap for the standard sized pill bottle. \footnote{38}{Id. One of these drugs, which may be ready for general use by 2012, is made by Proteus Biomedical. Novartis AG, one of the largest pharmaceutical companies, recently invested $24 million in the technology. Elizabeth Landau, *Tattletale pills, bottles remind you to take your meds*, CNN HEALTH (Feb. 2, 2010), http://articles.cnn.com/2010-02-02/health/pills.medication.compliance_1_pill-adherence-cell-phone?_s=PM:HEALTH.} Inside the “GlowCap” is a wireless transmitter, which can automatically generate emails to report the patient’s adherence statistics. \footnote{39}{Id.} If the patient does not remember to take their medication, the pill bottle can send emails or text messages to family members and the patient’s doctor. \footnote{40}{Id.}

**B. "Smart" Pill Technology**

Medication adherence technologies continue to become more sophisticated. Although not currently available on the market, \footnote{41}{One of these drugs, which may be ready for general use by 2012, is made by Proteus Biomedical. Novartis AG, one of the largest pharmaceutical companies, recently invested $24 million in the technology. Elizabeth Landau, *Tattletale pills, bottles remind you to take your meds*, CNN HEALTH (Feb. 2, 2010), http://articles.cnn.com/2010-02-02/health/pills.medication.compliance_1_pill-adherence-cell-phone?_s=PM:HEALTH.} microchip equipped pills—once only the purview of science fiction—are now being developed for general use. \footnote{42}{Dillow, supra note 7.} These pills, fitted with a tiny digestible
microchip, will transmit a signal when they are ingested, allowing doctors to remotely monitor patient adherence and collect a digital record of the exact time the medication is taken.

The possibilities for the technology seem endless. Already, researchers are working on “smart pills” that can detect when they have been metabolized and send a message to the doctor indicating that the medicine has entered the patient’s bloodstream. Additionally, pills that can automatically adjust how much medicine they administer, so as to provide the optimal amount of medication for each particular patient, are also forthcoming.

The adherence technologies currently on store shelves and in development are impressive, and the benefit to patients with adherence problems is considerable. Many lives could be prolonged by improved adherence to medication intended to address chronic and other serious conditions. The technology has great potential to help those that want to take their medication appropriately but have difficulty doing so. Moreover, in an increasingly “wired” world, many people appreciate the convenience of email, text messages, and alarm reminders. While these medical advances could help doctors remotely monitor their patient’s health and improve patient adherence, they may significantly invade patients’ privacy in the process.

43. Id.
44. Id.
45. CTR. FOR TECH. & AGING, supra note 15, at 16.
46. Id.
47. KAISER HEALTH NEWS, supra note 22.
49. Matthews, supra note 4.
IV. THE CURRENT STATE OF PRIVACY LAW

A. What is Privacy?

Although there is general agreement that a right to privacy exists, finding an accurate definition of that right is far more difficult. The first significant call for a privacy right came in 1890. In an article written for the Harvard Law Review, Samuel D. Warren and Louis D. Brandeis urged the U.S. Supreme Court to recognize a fundamental right of privacy to protect "the sacred precincts of private and domestic life" from intrusion by others. Simply put, they argued that privacy is "the right to be let alone." A year later the Supreme Court, in Union Pacific Railroad Company v. Botsford, defined privacy as "the right of every individual to the possession and control of his own person." Other posited definitions for privacy include: 1) the right to control information, 2) an autonomy regarding personal matters, or, more abstractly, 3) "control over when and by whom the various parts of us can be sensed by others."

B. Judicial Protection of Privacy Rights

Although a right to privacy does not appear expressly in the U.S. Constitution, the Supreme Court has recognized privacy as a fundamental right in certain situations. According to the Court, the right can be implied from several provisions of the Bill of Rights, specifically the First, Third,
Fourth, Fifth, and Ninth Amendments. In a line of cases beginning with *Griswold v. Connecticut* in 1965, the Supreme Court has held that privacy against intrusion by the government is a constitutionally protected right.

Supreme Court jurisprudence has primarily concerned two different kinds of privacy. The first is a due process right to make certain personal decisions without the government's intrusion. The second, stated in the Fourth Amendment, is the right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The latter is the Constitutional right primarily implicated by adherence technology.

1. **Fourth Amendment Privacy Jurisprudence**

Fourth Amendment protection is limited to the prevention of searches and seizures by the government, most commonly performed by police. The Amendment's protections are not triggered unless it is demonstrated that there is a "reasonable expectation of privacy" where the privacy breach occurred. For example, the Court has held that a person may have a

---


59. *Id.*; *See also* Eisenstadt v. Baird, 405 U.S. 438 (1972) (holding that there is a right to be free from governmental intrusion into personal matters); Roe v. Wade, 410 U.S. 113, 153 (1973) (holding that "the Constitutional right of privacy is broad enough to encompass woman's decision whether or not to terminate her pregnancy."); Lawrence v. Texas, 539 U.S. 558 (2003) (holding that the Fourteenth Amendment protects personal decisions "relating to marriage, procreation, contraception, family relationships, child rearing, and education"); *Cruzan v. Dir., Missouri Dep't of Health*, 497 U.S. 261 (1990) (holding that there is a constitutionally protected right to refuse medical treatment).


61. *See, e.g.*, Loving v. Virginia, 388 U.S. 1 (1967) (recognizing a right to marry); *Cruzan*, 497 U.S. at 261 (recognizing a right to decide to accept medical treatment); *Griswold*, 381 U.S. at 479 (recognizing a right to decide whether to have children).

62. U.S. CONST. amend. IV.

63. Cheh, *supra* note 60.

reasonable expectation of privacy within his own home,\textsuperscript{65} making a warrantless search of the home generally unreasonable.\textsuperscript{66}

However, the privacy right is no longer protected if the information has been exposed to the public.\textsuperscript{67} Therefore, being in public as opposed to in the home limits the Fourth Amendment's protections.\textsuperscript{68} For example, the Court has held that a driver on a public street does not have a reasonable expectation of privacy regarding the direction or destination of his automobile.\textsuperscript{69} Consent of the person searched also makes a search lawful.\textsuperscript{70}

Injection or forced ingestion of a human with a microchip-equipped pill could be considered an unlawful "search" under the Fourth Amendment because it violates the right of the patient "to be secure in their person."\textsuperscript{71} However, this would only raise a constitutional issue if: (1) the "search" (use of the pill) was not consensual, and (2) the search was conducted by the government. This second requirement severely limits the applicability of the Fourth Amendment to adherence technology because it appears that only patients whose doctors are directly employed by the government and working within the scope of their employment could recover for the invasion of privacy.\textsuperscript{72} Additionally, a patient would have no cause of action against third parties who use the gathered information inappropriately.\textsuperscript{73} Therefore, it will not be effective to rely solely on constitutional guarantees of privacy. In this case, it may be better for aggrieved plaintiffs to invoke the privacy torts instead.


\textsuperscript{67} Katz, 389 U.S. at 360.


\textsuperscript{70} Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (noting that the Fourth Amendment is not violated if consent is given).

\textsuperscript{71} U.S. CONST. amend. IV.

\textsuperscript{72} Ferguson v. City of Charleston, 532 U.S. 67, 76 (2001) (holding that employees at a state hospital are government actors for purposes of the Fourth Amendment).

2. Privacy Torts

Historically, privacy protection unrelated to government action was achieved through Common Law torts.\textsuperscript{74} Unlike the Fourth Amendment right, state law privacy torts control third party behavior.\textsuperscript{75} First enumerated after the publication of Warren and Brandeis’ article, the Second Restatement of Torts now recognizes four distinct causes of action that protect different privacy rights. They are: (1) intrusion on seclusion, (2) publication of private facts, (3) false light, and (4) misappropriation.\textsuperscript{76}

The two privacy torts most relevant for purposes of this paper are intrusion on seclusion and publication of private facts.\textsuperscript{77} First, the intrusion tort imposes liability for intentionally intruding “physically or otherwise upon the solitude . . . of another or his private affairs or concerns.”\textsuperscript{78} In order to win a civil lawsuit based on this theory, the plaintiff must prove that the intrusion would be “highly offensive to a reasonable person.”\textsuperscript{79} Some types of adherence technology—in particular the microchip equipped pills—would likely meet this threshold requirement of being “highly offensive.” Other types of adherence technology could intrude upon the patient’s solitude if use of the medication was compulsory. Deciding whether to take the medication is inherently a personal concern of the patient.\textsuperscript{80} Many people would undoubtedly find the intrusion to be highly offensive—who really wants their doctor to know when they expel the microchip?

\textsuperscript{74} See Scott Jon Shagin, \textit{The Prosser Privacy Torts in a Digital Age}, \textsc{New Jersey Lawyer, the Magazine}, 251-APR N.J. Law 9 (2008).

\textsuperscript{75} See \textit{Katz v. United States}, 389 U.S. 347, 347 (1967) (observing that privacy protection against third parties is left to state law).


\textsuperscript{77} The false light tort will not adequately protect medical information privacy because truth is a defense to the claim. The private records that need to be protected are truly the patient’s medical status. \textit{Id}. Additionally, the misappropriation tort only applies to embarrassing information about public figures so it would not protect the privacy of the general public. \textit{Id}. at 557.

\textsuperscript{78} \textsc{Restatement (Second) of Torts § 652B} (1977).

\textsuperscript{79} \textit{Id}.

\textsuperscript{80} \textit{Id}.
The second tort, publication of private facts, applies to information that is not "of legitimate concern to the public." It requires that the publicized information be of the kind that would be "highly offensive to a reasonable person." However, the tort is limited in scope to those facts that are made public. If private facts are not widely circulated, recovery may not be available.

In addition to the state privacy torts just discussed, Congress has created federal laws that protect privacy rights as well. Whether these laws will make recovery possible for plaintiffs is addressed below.

C. Legislating Privacy Rights

Originally, privacy laws were enforced by the states. The states administered tort protections through their judiciaries and frequently enacted statutes that enhance the protection given by the tort remedies. More recently, however, the federal government has taken a larger role in the protection of privacy. Federal legislation has the potential to provide a


82. Id.

83. Id. at § 652D cmt. A. William L. Prosser's well-known article in the California Law Review describes the four kinds of privacy torts. Regarding publication of private facts, Professor Prosser discusses the essential requirement that the facts be sufficiently publicized. He states:

"It is an invasion of the right to publish in a newspaper that the plaintiff does not pay his debts . . . but it has been agreed that it is no invasion to communicate that fact to the plaintiff's employer, or to another individual, or even to a small group, unless there is some . . . trust or confidential relation which will afford an independent basis for relief."

Thus, while a doctor cannot publicize a patient's medical information without the patient's consent, an ordinary citizen has no such professional duty of confidentiality. So long as the disclosure does not pass the threshold of "publication", the harmed patient will have no remedy in tort against them. William L. Prosser, Privacy, 48 Calif. L. Rev. 383, 393-394 (1960).


85. Id.
strong national standard for privacy protection, but current federal law appears to be insufficient because it provides few remedies for the person harmed. In some cases, federal law even preempts state law that would have provided a remedy to the injured.

The federal law most germane to the issue of health privacy is the Health Insurance Portability and Accountability Act ("HIPAA"), passed by Congress in 1996. This law went into full effect in 2003, and provides that entities covered by HIPAA must make electronic health information secure, ensure that the information is disclosed properly, and limit the number of people who have access to patient records. HIPAA does not preempt stronger protections in state law. However, like many federal privacy laws, although HIPAA provides for broad administrative agency enforcement, it does not provide a remedy for individuals whose personal information is compromised.

V. PRIVACY CONCERNS WITH ADHERENCE TECHNOLOGY

Health IT presents significant privacy concerns. Some patients might object to private health information being transmitted, collected, and shared. Medication that itself "tattle-tales" to family, caregivers, or other health providers, can undermine personal autonomy and broadcast very personal matters to others. The American legal system has traditionally protected

86. Id.

87. Id.

88. Id. at 15.

89. HIPAA recognizes the following as proper disclosures: 1) disclosure to the patient, 2) disclosure for payment, treatment, or healthcare needs, 3) disclosure with patient consent, and 4) disclosure based on an agreement. Michelle C. Pierre, Note, New Technology, Old Issues: The All-Digital Hospital and Medical Information Privacy, 56 Rutgers L. Rev. 541, 551-552 (2004).


91. De Armond, supra note 84, at 16.

personal medical decisions by competent adults. When and if to take medications is a personal matter traditionally protected by the right to privacy.

A citizen’s right to privacy is particularly important in the medical context. Doctors, nurses, and other caregivers have a legal and ethical obligation to maintain the confidentiality of information supplied by their patients. Americans must trust that their private medical information is protected when they talk to their doctor. Without this security, some patients may withhold essential information from their healthcare provider fearing that the information will not remain private, and in doing so, risk improper prescriptions and treatment.

93. Cruzan v. Dir., Missouri Dep’t of Health, 497 U.S. 261, 262 (1990) (holding that there is a constitutionally protected right to refuse medical treatment); Vacco v. Quill, 521 U.S. 793, 805 (1997) (noting that the “overwhelming majority of state legislatures” distinguish between allowing a patient to refuse treatment (which is legal) and physician-assisted suicide (which is not)); Washington v. Harper 494 U.S. 210, 221-22 (holding that a prisoner possesses “a significant liberty interest in avoiding the unwanted administration of anti-psychotic drugs under the Due Process Clause of the Fourteenth Amendment”).

94. Cruzan, 497 U.S. at 262.


97. AMA Code of Medical Ethics, supra note 96.


99. Id.
The recent explosion of Health IT has made confidentiality increasingly more difficult to guarantee. The ease of gathering and transmitting medical data allows more people access to health information.\(^{100}\) As Health IT use increases, courts will likely see more litigation concerning medical privacy that has been compromised.\(^{101}\)

VI. PREDICTING JUDICIAL AND LEGISLATIVE RESPONSES TO HEALTH IT BY ANALOGIZING TO OTHER CONTEMPORARY HEALTH INFORMATION TECHNOLOGIES

As of now, the courts have not had occasion to consider adherence technology, so the judicial response to its privacy implications is uncertain. Until the particular issue of adherence technology is challenged in the courts, it is helpful to look to other high profile information technology areas, in particular Electronic Health Records and Radio Frequency Identification Technology, to hypothesize what the judicial response may be.

A. Electronic Health Records and the Potential for Privacy Violations

Historically, patient medical records were written documents kept in the physician's office.\(^{102}\) To access them, it was necessary to obtain the record in person.\(^{103}\) Today, the widespread use of electronic health records means that many doctors, pharmacists, and insurance providers have unscreened access to an individual's medical record.\(^{104}\) Patients' personal health information can be transferred online in seconds leading to possible privacy encroachment.\(^{105}\)


102. Id. at 1184.

103. Terry & Francis, supra note 100, at 705.

104. BONNIE F. FREMGEN, MEDICAL LAW AND ETHICS 223 (3d ed. 2009).

105. Pierre, supra note 89, at 547.
1. **Electronic Health Record Technology**

There are many benefits to using electronic health records rather than traditional paper records. Electronic records facilitate communication between multiple providers, alert physicians when they prescribe incompatible medications, and prevent medical errors as a result of unclear handwriting. There is also evidence that the use of electronic records can save healthcare providers a significant amount of money.

Still, one of the largest drawbacks to electronic patient records is the significant privacy concerns they create. Electronic records are more difficult to protect than their paper counterparts. Confidential patient information can be hacked or inadvertently sent to the wrong person. Records can be accessed by individuals who are “snooping” public figures, even though they may have no professional medical interest in the information. Moreover, there is an issue concerning who owns these medical records because the owner has control over how and when the records can be accessed by others. In most states, the physician or hospital owns the patient records they create, although patients may decide who else receives access to them through written authorization.

---

106. Terry & Francis, *supra* note 100, at 683.


111. Terry & Francis, *supra* note 100, at 706.

112. *Id.* at 705-06.


114. FREMGEN, *supra* note 104, at 211; *see also* Estate of Finkle, 395 N.Y.S.2d 343, 344 (1977) (“[T]he vast majority of states hold ‘that medical records are the property of the physician or the hospital and not the property of the patient.’”); Paul V. Stearns, *Access to and Cost of Reproduction of Patient Medical Records: A Comparison of State*
2. Judicial Decisions Affecting Electronic Records

Judicial decisions on the subject of medical record ownership are inconsistent. This confusion is partially a result of the 1977 Supreme Court holding in *Whalen v. Roe*.\(^{115}\) In *Whalen*, the Court seemed to announce a right to information privacy, saying, "[t]he cases sometimes characterized as protecting ‘privacy’ have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."\(^{116}\) Despite this language, which appears to recognize a Constitutional right to information privacy, the Court has not addressed the issue further in the thirty years since the decision in *Whalen*.\(^{117}\) Without additional guidance from the Supreme Court, lower courts have had to interpret the meaning of information privacy on their own,\(^{118}\) and most of those courts have held that the Constitution protects information privacy.\(^{119}\)

---


\(^{118}\) Brief for American Civil Liberties Union, *supra* note 115, at 8.

\(^{119}\) See, *e.g.*, *In Re Crawford*, 194 F.3d 954, 958 (1999) (saying that the right to information privacy “is firmly established”); Seaton v. Mayberg, 610 F.3d 530, 537 (2010) (recognizing and expanding the information privacy right found in *Whalen*); Ramie v. City of Hedwig Village, Tex., 765 F.2d 490, 492 (1985) (recognizing the information privacy right set out by the Supreme Court in *Whalen*). *But see* Am. Fed’n of Gov’t Empls., AFL-CIO v. Dep’t of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (noting that the D.C. Circuit does not recognize a constitutionally protected right to information privacy); Bloch v. Ribar, 156 F.3d 673, 684 (6th Cir. 1998) (holding that information privacy is only protected when another fundamental liberty interest is involved).
The Supreme Court had the opportunity to address the confusion in 2010 with its ruling in *NASA v. Nelson*.\(^{120}\) In *Nelson*, the Court was asked to consider the constitutionality of certain questions in a government background check required of all federal contractors working for NASA.\(^ {121}\) The Court chose to decide the case narrowly on its facts, saying that the background check was within the government’s right as an employer, and avoided making a broad constitutional ruling on information privacy.\(^ {122}\) For now at least, lower courts will continue to decide cases of information privacy without the Supreme Court’s guidance.

It is likely that the use of electronic medical records will continue to be an important issue, as use of the technology is growing. By way of illustration, consider the actions of the Obama administration, which allotted $36 billion in federal stimulus money to facilitate the increased use of electronic medical records.\(^ {123}\) Intended to assist communications between multiple providers, the significant amount of federal funding indicates that electronic health records are here to stay.\(^ {124}\) In addition to considering the judicial response to electronic patient health records, and in an effort to better predict the court’s response to cutting edge Health IT, the judiciary’s response to Radio Frequency Identification technologies merits analysis as well.

**B. Radio Frequency Identification Technology**

Radio Frequency Identification ("RFID") is an electronic identification system that uses microchips to identify tagged items.\(^ {125}\) Like the UPC bar

---


121. *Id.*


124. *Id.*

codes\textsuperscript{126} found on everyday items but with more data storing capabilities, RFID systems have been in use since the Second World War.\textsuperscript{127} Today RFID is used in many areas including inventory control, shipment tracking, and building security.\textsuperscript{128} During the 1990s, RFIDs were implanted in more than fifty million of the world’s domestic pets so that lost pets could be identified and returned to their owners.\textsuperscript{129}

Today, the technology is FDA-approved for implantation in humans.\textsuperscript{130} VeriChip Corporation, the maker of the approved RFIDs, has made most of its sales abroad—for example, the Mexican Attorney General and his staff have all been injected with RFIDs to allow them to access high security areas.\textsuperscript{131} Now, a new campaign by VeriChip is encouraging implantation in “high-risk” Americans, particularly the elderly suffering from Alzheimer’s and children who are in danger of being kidnapped.\textsuperscript{132} Besides the possibility of protecting “high-risk” people,\textsuperscript{133} other benefits of RFID systems include the ability to manage assets, provide data for electronic records systems, and prevent the distribution of counterfeit medications.\textsuperscript{134} Despite these benefits, the use of RFIDs in humans pose both health and

\begin{thebibliography}{9}
\bibitem{126} UPC codes, also known as bar codes, are vertical black and white stripe patterns that appear on many consumer items. The bar code is read by a scanner which can identify the data contained in the code. \textit{Bar Code Frequently Asked Questions (FAQ): Q. What is a bar code?}, ASS’N FOR AUTOMATIC IDENTIFICATION AND MOBILITY, http://www.aimglobal.org/technologies/barcode/bcfaqs.asp (last visited Feb. 25, 2012).
\bibitem{127} RFID technology was first developed during World War II. The British used RFIDs to identify their own aircraft. Currid, \textit{supra} note 125, at 360.
\bibitem{129} Id.
\bibitem{130} Currid, \textit{supra} note 125, at 361.
\bibitem{131} Id.
\bibitem{132} Id.
\bibitem{133} Id.
\end{thebibliography}
privacy risks. The FDA has cautioned that some RFID systems could interfere with pacemakers and other electronic health devices.\textsuperscript{135} Additionally, it has been widely reported that the implantable chips can cause cancer and that both VeriChip and FDA officials overlooked testing on lab rats that demonstrated this risk.\textsuperscript{136} Privacy concerns with RFIDs focus primarily on the chips' power "to enhance the effectiveness of surveillance—by governments . . . and by private parties both legitimate and criminal."\textsuperscript{137} RFID chips can function as a surveillance system because each chip has a unique code.\textsuperscript{138} For example, if a customer purchases sunglasses with a RFID chip inside for store inventory purposes, that chip effectively could later be used to track the location of the person wearing the sunglasses.\textsuperscript{139} Even more alarming for privacy advocates, RFID technology has been inserted in all new U.S. passports since 2007.\textsuperscript{140} As a result, the government can identify Americans abroad based on the locations of their passports.\textsuperscript{141}

Chips implanted in humans magnify the surveillance risk. While human RFID chips are not currently programmed to track the whereabouts of their "host," scientists are able to use the same kind of technology to track animal

\begin{itemize}
\item 135. \textit{Id.}
\item 136. Pagnattaro, \textit{supra} note 128, at 245.
\item 138. \textit{Id.}
\item 139. \textit{Id.}
\end{itemize}
migrate. Thus, the technology is available if someone wanted to track individual humans.

Still, there are some ways to limit the tracking capabilities of RFID tags. Beginning in August 2010, Wal-Mart stores began tagging clothing with RFIDs to prevent shoplifting. To minimize potential privacy concerns, Wal-Mart attaches the tags to removable labels so that customers can remove the RFIDs after they purchase the item. European retail stores that use the technology generally remove the RFID enhanced tags at the register. Nevertheless, while the tags can be removed, they cannot be turned off and remain traceable.

As of today, regulation of the technology has occurred almost exclusively at the state level. So far, fifteen states have passed RFID legislation. Wisconsin was the first state to completely ban the microchipping of humans. Other states have taken a more moderate approach; for example, North Dakota passed a law that prevents required microchipping of humans but allows microchipping if it is voluntary. California chose to put

142. Currid, supra note 125, at 364.

143. Id.


145. Id.

146. Id.

147. Id.

148. Currid, supra note 125, at 365.


150. Pagnattaro, supra note 128, at 247-249.

151. Id.
limitations on various ways the chips could be used, including a ban on employer-directed microchipping of their employees.152

VII. POSSIBLE JUDICIAL AND LEGISLATIVE RESPONSES TO ADHERENCE TECHNOLOGIES

Because of the potential privacy threats associated with adherence technology, the legal system needs to find the most effective ways to protect patient privacy, while still allowing the use of adherence technology and its many benefits. Legal responses could include a strict approach to traditional consent law,153 legislation to define parameters for adherence technology use,154 improved electronic record privacy regulations,155 and a clear position from the judiciary regarding the scope of the right to information privacy.156

A. Informed Consent Law: The Role of Doctors and Health Professionals

In legal terms, informed consent means that a person “allows something to happen with full knowledge” of the risks and the possible alternatives to the course of action.157 A patient’s informed consent is required before a doctor may take certain actions or malpractice liability can result.158

In the adherence technology arena, informed consent is essential and could be strengthened and reinforced through federal legislation providing for an explicit opt-in approach to the use of adherence technology. Physicians would have to provide patients with documentation indicating the potential privacy risks implicit in the technology and setting out the steps

152. Id.
154. Id.
155. Pierre, supra note 89, at 552 (commenting that “HIPAA only begins to fill the void in existing legislation for protecting medical information privacy”).
156. Brief for American Civil Liberties Union, supra note 115, at 9.
157. BLACK’S LAW DICTIONARY 346 (9th ed. 2009).
taken to minimize those risks, including, for example: their system for data storage, the accessibility of their electronic information, and how the information is transferred to insurance companies and other providers.\textsuperscript{159} Moreover, it is likely that medicines with built-in adherence technology will be more expensive than traditional medications. Patients need to be fully informed about this additional cost in order to make an informed decision about whether to use adherence technology.

It is necessary to emphasize that patients must be completely informed in order to consent to the technology.\textsuperscript{160} Although it may be difficult to explain some of the more complicated concepts—how a digestible microchip works, for instance—health care providers have an ethical duty to keep patients informed.\textsuperscript{161}

\textbf{B. Potential Legislative Action}

In addition to the legislative initiatives regarding informed consent, additional legislation could enhance privacy protection. As mentioned above, federal laws have historically had little effect on medical privacy;\textsuperscript{162} instead Congress has allowed individual states to determine the optimal level of privacy necessary for its citizens' medical records.\textsuperscript{163} However, many states have conflicting laws, making the state-based protection of electronic records that are transferred across state lines particularly difficult.\textsuperscript{164} Because health providers often need to send electronic records interstate, federal legislation becomes the most effective way to police those records.

\begin{itemize}
\item[159.] Kristen E. Edmundson, \textit{Global Positioning System Implants: Must Consumer Privacy be Lost in Order for People to be Found?}, 38 IND. L. REV. 207, 234 (2005).
\item[160.] See Moore, \textit{supra} note 50, at 166.
\item[162.] See \textit{supra} Part III.C.
\item[163.] Pierre, \textit{supra} note 89, at 557.
\end{itemize}
because it avoids the high costs associated with ensuring compliance with the laws of many different states.\textsuperscript{165}

Like Electronic Health Records and RFIDs, adherence technology creates a need for increased security. Congress has already taken an important step to protect patient privacy protection by including medical privacy initiatives in the American Recovery and Reinvestment Act.\textsuperscript{166} The Act included provisions that strengthen HIPAA privacy rules and increase the fines that the Department of Health and Human Services can levy against healthcare providers for noncompliance.\textsuperscript{167} However, given that adherence technology is in the early stages of development, it is unlikely that the privacy concerns connected with its implementation were considered adequately at the time that the legislation was passed; technology changes quickly while the legislative process can be slow. Thus, HIPAA will continue to require updating in order to address technology advances.

At the same time, individual states can pass legislation to provide many of the same protections as HIPAA. Based on their police powers, states could make their laws stricter than HIPAA and oversee the enforcement of those privacy protections.\textsuperscript{168} For example, California’s newly enacted privacy law is a good model for legislation that punishes those who access medical information without authorization.\textsuperscript{169} California’s law requires that health providers protect patient records from unlawful access and enumerates a

\begin{flushleft}
\textsuperscript{165} As mentioned earlier, federal law has preempted many state privacy laws. When broadening privacy legislation, total preemption should be avoided if possible because state laws are the only ones providing remedies for individual plaintiffs. See De Armond, \textit{supra} note 84.

\textsuperscript{166} Kirsten Ruzic Wild, \textit{The Evolution of HIPAA: The Only Constant is Change}, 12 \textit{J. HEALTH CARE COMPLIANCE} 33 (2010).


\textsuperscript{169} Two California laws which went into effect on January 1, 2009, significantly increased the penalties for medical record “snooping.” The new laws also require that healthcare providers notify patients if their private medical information has been improperly accessed. Edgar D. Bueno, \textit{New California Law Clamps Down on Unauthorized Viewing of Medical Records}, 10 \textit{PRIVACY AND INFO. L. REP.} 6 (2009).
\end{flushleft}
series of penalties for providers who allow confidential medical information to be breached.\textsuperscript{170}

Finally, in order to keep patient’s health records private, federal restrictions on mandatory use of the technology are needed. For example, Congress can forbid the use of adherence promoting technology as a prerequisite for insurance coverage, employment, or school admission. Mandatory use of adherence technology would effectively nullify laws requiring informed consent and result in patients only consenting because they have no other choice.\textsuperscript{171} Additionally, Congress can pass legislation requiring pharmaceutical companies to continue producing some pharmaceuticals without adherence technology, so that patients who do not want to use the technology may opt-out. Patients are not truly consenting if their only option for receiving the benefits of a drug is to submit to adherence technology. Finally, individuals who cannot readily assert their rights or truly exercise informed consent—in particular the elderly, mentally incompetent patients, and children—should not be forced to use adherence technology.\textsuperscript{172}

C. Potential Judicial Action

Without specific legislation or an explicit contract term to interpret, the judiciary will not be able to do much to prevent the misuse of medical information technology. Still, courts will likely be asked to examine more cases addressing Health IT and medical privacy as the use of the technology grows. Americans have come to expect a certain level of privacy in their lives and breaches of medical privacy will likely result in novel litigation involving legal arguments which apply privacy law to Health IT.\textsuperscript{173}

In order to best protect patients, the Supreme Court should specifically address the right of information privacy when the opportunity presents itself. Some privacy scholars have argued that the Court should reexamine, and reaffirm its declaration in \textit{Whalen v. Roe}, recognizing information privacy as


\textsuperscript{171} Moore, supra note 50, at 166.

\textsuperscript{172} Currid, supra note 125, at 383.

\textsuperscript{173} Harris, supra note 101, at 1187.
a fundamental right.\textsuperscript{174} This would allow patients better control over their personal medical information, making recovery easier when a breach occurs and encouraging health providers to handle confidential information more carefully.

VIII. CONCLUSION

Adherence technology has the potential to improve the health of Americans who have difficulty taking their medication properly. "America’s Other Drug Problem" is a serious public help issue and some pharmaceutical companies are attempting to solve the problem.\textsuperscript{175} Besides helping patients follow prescription regimens, Health IT may also reduce medical errors, foster communication between a patient’s multiple health providers, and make administrative tasks easier.\textsuperscript{176}

And yet, Americans should be wary of any technology that makes highly sensitive information about their health more readily available. Already Electronic Health Records and RFIDs are becoming commonplace\textsuperscript{177} and according to industry projections, pharmaceutical packaging demand will reach $18.4 billion in the U.S. by 2014.\textsuperscript{178} Given all the advantages, many of those products are likely to have built-in adherence technology.

The privacy issues related to adherence technology must be addressed through legislative action on the state and national level. Patient privacy laws such as HIPAA can be strengthened and updated in order to specifically address these new technologies. Judicial action to further define the medical privacy right is also needed. In the meantime, these technological advances will ensure that medical privacy law continues to be an important issue that all branches of the government—and all Americans—should consider.

\textsuperscript{174} Pierre, supra note 89, at 571.

\textsuperscript{175} Public Policy & Adherence: Statistics, supra note 12.

\textsuperscript{176} Gilman & Cooper, supra note 26, at 281.
