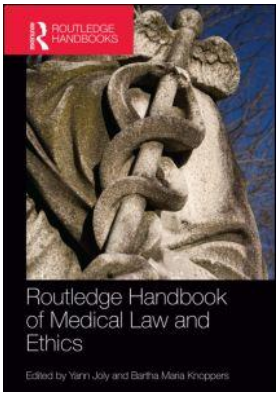
This article was downloaded by: *10.3.97.143*
On: 08 Dec 2023
Access details: *subscription number*
Publisher: *Routledge*
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: 5 Howick Place, London SW1P 1WG, UK



Routledge Handbook of Medical Law and Ethics

Yann Joly, Bartha Maria Knoppers

Privacy and confidentiality

Publication details
https://www.routledgehandbooks.com/doi/10.4324/9780203796184.ch4
Mark A. Rothstein
Published online on: 29 Aug 2014

How to cite :- Mark A. Rothstein. 29 Aug 2014, *Privacy and confidentiality from:* Routledge Handbook of Medical Law and Ethics Routledge
Accessed on: 08 Dec 2023
https://www.routledgehandbooks.com/doi/10.4324/9780203796184.ch4

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

4

Privacy and confidentiality

Mark A. Rothstein

4.1 Legal and ethical theory

4.1.1 Background

Privacy and confidentiality are foundational principles in medicine and all of healthcare, but both terms are often used inconsistently and are difficult to define. Privacy is generally recognized as the broader concept, sometimes including confidentiality. Privacy has several dimensions – informational, physical, decisional, proprietary, and relational (Beauchamp and Childress 2013: 312). This chapter concentrates on the informational dimension of privacy. Accordingly, *privacy* is defined here as a condition of limited access to an individual or information about an individual. *Confidentiality* is defined as the condition under which information obtained or disclosed within a confidential relationship is not redisclosed without the permission of the individual. *Security* is defined as the personal and electronic measures granting access to personal health information to persons or entities authorized to receive it and denying access to others (National Committee on Vital and Health Statistics (NCVHS) 2006).

Another ethical principle related to informational health privacy is *autonomy*. As defined by Beauchamp and Childress (2013: 101), '[a]t a minimum, personal autonomy encompasses self-rule that is free from both controlling interference by others and limitations that prevent meaningful choice, such as inadequate understanding.' Many individuals believe that they ought to be able to control the uses and disclosures of their health information and biospecimens, even if their records and specimens are deidentified (Rothstein 2010b; Hull *et al.* 2008). In addition, many individuals believe a physicians' obligation to respect patient autonomy arises from the physician–patient relationship.

The obligation of physicians to safeguard the confidentiality of patient-derived information dates back at least to the fourth century BCE and the Oath of Hippocrates. The pertinent provision of the Oath reads:

> What I may see or hear in the course of treatment in regard to the life of men, which on no account must be spread abroad, I will keep to myself, holding such things shameful to be spoken about.
>
> *(See Reich 1995: 2632)*

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

Although the Oath had a somewhat different meaning in ancient Greece than is often ascribed to it today (Miles 2004: 150), modern conceptions of the Oath are perhaps more important than the actual wording (Rothstein 2010a). Today, the Hippocratic Oath is generally considered the original source of a physician's duty to maintain as confidential virtually all patient health information.

In the nineteenth century, medicine emerged as a scientifically based health profession (Starr 1982). Codes of medical ethics, beginning with Thomas Percival's code of medical ethics in 1803, incorporated confidentiality requirements. The American Medical Association's (AMA) first Code of Ethics in 1847 also expressed the physician's duty to maintain confidentiality. The current version of the AMA's Code of Medical Ethics provides that:

> The information disclosed to a physician by a patient should be held in confidence. The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services. The patient should be able to make this disclosure with the knowledge that the physician will respect the confidential nature of the communication.
>
> *(AMA 2011: section 5.05)*

The AMA's Code of Medical Ethics, like other such codes, links maintaining confidentiality with the ability to provide appropriate health services. Without assurances of confidentiality, patients would be reluctant to share intimate information about their health and lifestyle. Likewise, without accurate and detailed histories and symptoms from patients, it would be difficult to provide appropriate medical care.

Codes of ethics from around the world similarly place a high priority on protecting the confidentiality of patient information. The World Medical Association's International Code of Medical Ethics and Declaration of Geneva explicitly mention the duty of a physician to protect confidentiality:

> A physician shall respect a patient's right to confidentiality. It is ethical to disclose confidential information when the patient consents to it or when there is a real and imminent threat of harm to the patient or to others and this threat can only be removed by a breach of confidentiality.
>
> *(World Medical Association (WMA) 2013: 2)*

Similar provisions appear in the codes of ethics or ethical guidelines of various national medical associations, including the Australian Medical Association (2006: subsection 1.1(12)), the British Medical Association (2013), and the Canadian Medical Association (2013: paras 31–7).

4.1.2 Right to privacy

The legal right to privacy has relatively recent origins. In 1890, two young law partners from Boston, Samuel D. Warren and Louis D. Brandeis, published a groundbreaking article in the *Harvard Law Review* titled simply 'The Right to Privacy' (Warren and Brandeis 1890). Presumably motivated by the intrusive Boston press, Warren and Brandeis argued more broadly in favor of a comprehensive common law right of individuals to be free from unwanted intrusions. They proposed a general legal principle of protecting the 'privacy of private life' and urged creating a legal cause of action to redress 'the more flagrant breaches of decency and propriety' (Warren and Brandeis 1890: 215–16).

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

Despite its well-deserved acclaim in the academic literature, the Warren and Brandeis article did not immediately translate into a well-accepted legal theory permitting the redress of invasions of privacy. Beginning in the 1930s, however, several courts recognized some aspects of a common law right to privacy, but the right was not clearly defined. In 1960, that would change. William L. Prosser, the leading figure in the development of American tort law, published an even more simply titled article 'Privacy,' in which he proposed the common law right of privacy was actionable in four discrete situations: (1) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity which places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness (Prosser 1960: 389).

All four categories of invasion of privacy could be violated in the context of health information and healthcare. The public disclosure of private facts represented one category most applicable to healthcare, and would be implicated whenever sensitive health information was wrongfully disclosed to the public. Although Prosser's classification scheme was criticized for being overly reductionist and restrictive (Bloustein 1964; Richards and Solove 2007), it was adopted by the *Restatement (Second) of Torts* (Prosser was the reporter) (Richards and Solove 2007). Since then, this categorical approach to invasion of privacy has been widely adopted by courts in the United States. Yet invasion of privacy cases have been difficult for plaintiffs to win due to the strict set of criteria imposed by the courts. Courts require that: (1) the publication of the information must be widespread; (2) the information disclosed must be of a private nature; (3) the disclosure must be highly offensive to a reasonable person; and (4) the matter must not be a legitimate concern of the public (Rothstein 2009).

4.1.3 Constitutional law (US)

The United States Constitution does not contain an express provision establishing or protecting the right to privacy. The Fourth Amendment to the Constitution prohibits unreasonable searches and seizures, and therefore, it has been the most widely invoked source of a constitutional right to privacy. Because the Constitution is designed to restrain the exercise of government powers, its provisions generally may not be invoked in purely private disputes. Thus a prerequisite to application of the Fourth Amendment is action by the federal, state, or local government. The fundamental legal question is whether the Supreme Court recognizes a constitutional right to informational health privacy in cases where the government is alleged to have violated an individual's privacy. In *Whalen* v. *Roe* (1977) 429 US 589, the plaintiffs challenged the constitutionality of a New York State law requiring the collection in a centralized database of the names and addresses of all persons who obtain, pursuant to a doctor's prescription, certain controlled drugs, including powerful analgesics. The Supreme Court stopped short of declaring an individual's constitutionally protected interest in informational health privacy, holding that even assuming there is such a right, the New York statute was a reasonable measure to prevent the unlawful diversion of controlled substances.

American courts have since followed the approach used in *Whalen*, assuming but not deciding there is a constitutional right to informational health privacy. Most recently, *National Aeronautics and Space Administration* v. *Nelson* (2011) 131 SCt 746 (*NASA*) involved a challenge to the intrusive background questionnaire mandated for employees working for a contractor at NASA's Jet Propulsion Laboratory. Among other things, the questionnaire asked employees if they had used, possessed, supplied, or manufactured illegal drugs in the last year. If so, they were required to explain and disclose any substance abuse treatment they received. Employees were also required to sign a release authorizing the government to obtain personal information from schools,

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

employers, and other sources during its investigation. The Supreme Court again assumed, without deciding, there was a constitutional right to informational privacy. Even assuming such a right, however, the Court upheld the questionnaire requirement as reasonable in light of the government's important interest in employee safety and probity, as well as the protections in place to prevent disclosure of the information to the public. Thus, as *NASA* and *Whalen* demonstrate, even if there is a constitutional right to informational health privacy, the courts have been so deferential to the government's interests that plaintiffs' claims are rarely sustained (Rothstein 2011).

4.1.4 Privacy Act *(US)*

In 1974, partly in response to the government abuses disclosed in the Watergate scandal, Congress enacted the *Privacy Act* 1974 (5 USC § 552a). The *Privacy Act* established a code of fair information practices that governs the collection, use, and dissemination of information about individuals maintained in 'systems of records' by federal executive branch agencies. The *Privacy Act* aims to: (1) restrict disclosure of personally identifiable records maintained by agencies; (2) grant individuals increased rights to access agency records maintained on themselves; (3) grant individuals the right to seek amendment of agency records upon a showing that the records are not accurate, relevant, timely, or complete; and (4) establish a code of fair information practices requiring the agencies to comply with statutory norms for collection, maintenance, and dissemination of records (US Department of Justice 2012).

The *Privacy Act* creates a default rule that individually identifiable information should not be disclosed unless one of the 12 statutory exceptions applies (5 USC § 552a(b)). Among these exceptions are disclosures for civil or criminal law enforcement activity, if (i) the activity is authorized by law; and (ii) the request is made in writing that specifies the portion of the records requested and the law enforcement activity for which the record is sought.

Each agency must keep an accurate accounting of the disclosures of records under its control (5 USC § 552a(c)), preserve an individual's right of access to his or her own records, and preserve an individual's right to request an amendment of his or her records (5 USC § 552a(d)). Furthermore, agencies must maintain only information that is relevant and necessary to accomplish their purpose, maintaining it in as complete, timely, and accurate a fashion as possible (5 USC § 552a(e)). Each agency must also provide public notice through publication in the Federal Register of the character and nature of the records it maintains, as well as the rules it follows in disclosing information.

The *Privacy Act* represents groundbreaking privacy legislation because it establishes a code of fair information practices – rules applicable across the federal government to limit disclosures and grant individuals rights with respect to their own information (Levin and Nicholson 2005) – rather than stating the specific information that will be protected from disclosure. However, its main limitation is that it applies only to information in the possession of the federal government (Schwartz and Solove 2013).

Another federal law, the *Freedom of Information Act* 1966 (5 USC § 552), prescribes rules for public access to documents in the possession of the federal government. An important exception to the disclosure requirement is for records protected by the *Privacy Act*, including individual health information.

4.1.5 Health Insurance Portability and Accountability Act Privacy Rule *(US)*

Despite having seriously considered enacting comprehensive privacy legislation in the 1970s, Congress took no action on privacy legislation, including health privacy legislation, until the 1990s. Although several states enacted health privacy legislation in the absence of federal action,

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

these laws were of limited scope, such as granting patients a right of access to their health records and requiring informed consent before making certain disclosures (Pritts 2002). Federal action in the realm of health privacy came about indirectly and in an unlikely legislative vehicle.

During the 1990s (as well as today), many Americans obtained their healthcare coverage from employer-sponsored group health plans. If an employee had a preexisting health condition or had a dependent with such a condition, the employee found it difficult, if not impossible, to maintain comparable coverage under an employer-sponsored group health plan if the employee changed jobs. Both insured and self-insured health plans were free to deny coverage, exclude certain conditions, charge higher rates, or take other actions when a new employee or a newly covered dependent had a preexisting health condition. Concerned about the unfairness of this loss of health coverage and the drag on the nation's economy by limiting occupational mobility due to 'job lock,' Congress took up the bipartisan Kennedy-Kassebaum Bill, the *Health Insurance Portability and Accountability Act* (HIPAA) 1996. HIPAA was designed to increase the portability of health coverage by prohibiting employer-sponsored group health plans from imposing certain burdensome conditions on new enrollees.

By prohibiting exclusionary practices, HIPAA imposed costs on the health insurance industry. During the legislative process, the health insurance industry indicated that it would not oppose the bill if the legislation also contained a provision, long favored by the industry, requiring all health claims submitted for payment to be in standard electronic formats. The bill's sponsors agreed, thereby adding the provisions to Title II of HIPAA, 'Administrative Simplification.' Before its final enactment, however, Congress realized that the electronic filing of millions of health claims created issues of privacy and security. Therefore it added a provision that if Congress did not enact privacy legislation within two years, the Secretary of Health and Human Services (HHS) was required to do so (Pub. L. 104–191). After Congress failed to enact privacy legislation, the HHS issued the controversial *HIPAA Privacy Rule* (45 CFR Parts 160, 164).

This detour into the origins of the *HIPAA Privacy Rule* is important because it explains why it was never intended to be a comprehensive health privacy law and, indeed, it is not. Because of its narrow mandate, it only applies to three classes of covered entities in the healthcare payment chain: health providers (e.g. hospitals, physicians), health plans (e.g. health insurance companies, employer-sponsored group health plans), and health clearinghouses (entities that put billing information into standard electronic formats). In its current form, the *Privacy Rule* is more of a 'notice and disclosure' rule than a privacy rule. For example, informed consent from a patient is not required before a covered entity may use and disclose individually identifiable health information for treatment, payment, or healthcare operations (e.g. quality assurance). Instead, covered entities are merely required to provide a notice of privacy practices to patients and, for healthcare providers with a direct treatment relationship, to make a good faith effort to obtain the patient's written acknowledgment of receipt of the notice.

The *Privacy Rule* also includes 12 categories of 'permissive' disclosures for public purposes, including disclosures for public health, law enforcement, and to avert an imminent harm. Any legal obligations for a covered entity to make one of these disclosures (e.g. reporting cases of suspected child abuse) are based on other laws. The *Privacy Rule* merely provides that disclosures for these purposes are permitted. Significantly, the *Privacy Rule* does not contain a private right of action. An aggrieved individual's only remedy is to file a complaint with the Office for Civil Rights of HHS. Violators are subject to civil monetary penalties, and for egregious cases, criminal prosecutions may be brought by the Department of Justice.

4.1.6 International data protection law

European data protection law is similar to the US *Privacy Act* in that it uses general principles of fair information practices rather than detailed rules for each type of data and disclosure.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

The two foundational documents are the *European Convention on Human Rights* 1950 and the *Charter of Fundamental Rights of the European Union* 2000, which reiterates many of the same principles set forth a half-century earlier by the *European Convention on Human Rights* and those derived from shared constitutional traditions of EU member states. Both documents contain language guaranteeing privacy protection in one's private life (*European Convention on Human Rights* 1950: article 8; *Charter of Fundamental Rights of the European Union* 2000: article 7).

In response to the increased flow of information across borders, the European Parliament adopted Directive 95/46/EC. This Directive, along with Directive 2002/58/EC concerning personal data processing and privacy protections in the electronic communications sector, form the basis of modern data protection law in the European Union (Hiller *et al*. 2011). Directive 95/46/EC provides that:

> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> *(1995: article 1(1))*

To help achieve this goal, article 29 of the same Directive created the Data Protection Working Party, an independent advisory board on data protection and privacy (Directive 95/46/EC, 1995). The Working Party's responsibilities are described in article 30 of Directive 95/46/EC and article 15 of Directive 2002/58/EC and include examining the uniform application of EU data protection laws and advising the European Commission as to possible amendments or additional measures needed to safeguard privacy protections. In response to evolving technologies in healthcare that could implicate patient privacy protections, the Working Party issued a report in 2007 that provides guidance and recommended legal protection of individual health privacy in the use of electronic health records (see section 4.2.1 below) (Data Protection Working Party 2007). More recently, in 2012, the European Commission proposed the *General Data Protection Regulation*, which, if adopted, would substantially reform Directive 95/46/EC (see section 4.2.2 below).

As is the case in the US and Europe, other industrialized nations also try to preserve privacy by enacting data protection laws. For example, Australia enacted the *Privacy Act* 1988, essentially an analog to the US *Privacy Act*, to better protect how personal data is processed and collected (Atkinson *et al*. 2009). Likewise, although no general right to privacy exists in the *Canadian Charter of Rights and Freedoms*, Canadians are guaranteed a constitutional right comparable to the one provided by the American Fourth Amendment (Levin and Nicholson 2005). The Canadian government therefore enacted two major federal privacy laws, the *Privacy Act* 1983 and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000. In combination with the nation's aforementioned constitutional law, both strengthen personal data protection and quell privacy concerns in a manner that blends European and American privacy principles (Levin and Nicholson 2005; Office of the Privacy Commissioner of Canada 2009).

4.2 Current and emerging issues

4.2.1 Electronic health records and networks

New electronic technology is revolutionizing the way health information is collected, aggregated, analyzed, stored, used, and disclosed. As such, health information technology (HIT) also presents important challenges for health information privacy and security. In the 'old days' of paper records, healthcare was too often compromised by illegible, nonstandard, fragmented,

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

uncoordinated, and error-filled records. The disarray caused by paper-based health records, however, served to protect health privacy by making it virtually impossible to compile inclusive individual health information from numerous sources over long periods of time (Silversides 2010). Moreover, paper records allowed individuals to control access to their health information by simply changing healthcare providers and choosing what elements of their health histories to disclose to their new providers.

HIT holds the promise of interoperable, comprehensive, and longitudinal health records and networks, while offering greater safety, accuracy, efficiency, and effectiveness (Rynning 2007). At the same time, the consolidated and integrated health information never goes away (see section 4.2.2 below), raising questions about who should have access to sensitive information, especially when it has little or no current clinical utility (Rynning 2007). The following section is divided into two parts that discuss access to health information (1) within healthcare settings and (2) beyond healthcare settings.

4.2.1.1 Healthcare settings

Many hospitals and larger medical institutions have electronic health record (EHR) systems with role-based access controls. For example, food service or custodial employees are denied access to sensitive clinical information, while there are generally no limits on the scope of information available to physicians, nurses, pharmacists, various technicians, and other health professionals with direct patient care responsibilities. Security measures, such as password protected access, encryption, and audit trails are a necessary but insufficient means of limiting access to unauthorized personnel.

Although instances of lost laptops and hackers unlawfully breaking into EHRs garner great publicity, they are not the greatest threats to health privacy. The greatest privacy threat involves an authorized user accessing more information than is necessary to treat an immediate problem (Chalmers and Muir 2003). For example, a physician in an emergency department treating a woman for a sprained ankle is unlikely to need access to the woman's reproductive health history, but there is currently no operational way to limit the scope of this access. Even though, as a practical matter, busy physicians do not have the time to troll through exhaustive health records, as long as they *could* access this information many patients will be concerned that their sensitive information is not really confidential.

The lack of privacy controls on health information can lead to a variety of individual and societal harms. First, individuals may suffer embarrassment, stigma, discrimination, and other harms to their dignity if sensitive information is inappropriately disclosed. Second, quality healthcare may be undermined if individuals who fear widespread disclosure of their sensitive information forego timely treatment for stigmatizing conditions or engage in defensive practices, such as withholding or 'editing' the sensitive information they share with their healthcare providers. Third, public health harms may occur if individuals with infectious disease, mental illness, substance abuse, or other sensitive conditions delay or decline treatment because they fear a loss of privacy (Rothstein 2012; California Health Care Foundation 2005).

One of the most promising technologies for limiting unnecessarily broad access to health information is segmentation, permitting patients to designate entire fields of sensitive information as inaccessible unless they provide additional consent. Candidate classes of health information for segmentation include genetic information, domestic violence information, mental health information, sexuality and reproductive health information, substance abuse information, sexually transmitted disease information, and child and adolescent health information.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

Many technical and policy issues need to be resolved before segmentation is operational. These issues prevent widespread implementation of EHR segmenting in the clinic by raising questions regarding whether there should be a 'break-the-glass' feature for emergency access to comprehensive health records; whether clinical decision support should operate on all health information, including segmented information; and whether the records should carry a notation that some information is being withheld at the request of the patient (Rothstein 2010a; NCVHS 2008).

4.2.1.2 Beyond healthcare

Many individuals and entities beyond healthcare (e.g. employers, insurers) have a legitimate need to access an individual's past or current health information, but there is little agreement on what information should be available or how to prevent overly broad access. Among the issues are the following: (1) Is it permissible for third parties to require individuals to sign authorizations giving access to their health information? (2) Is it possible to limit the amount of health information disclosed pursuant to an authorization? (3) How may the third-party recipients use the health information they obtain.

A variety of individuals and entities have economic leverage over other individuals, which can be used to compel them to sign an authorization to disclose their health information. For example, if an individual applies for a life insurance policy, the life insurer can require authorization for health information disclosure as a condition of applying for the policy. This is lawful and appropriate for an insurance product whose availability and pricing traditionally have been based on medical underwriting. The life insurance applicant need not sign the authorization, but if the applicant declines to do so, the insurer may not consider the individual's application (Rothstein and Talbott 2006). It is not known precisely how many of these 'compelled authorizations' are signed each year, but a conservative estimate is that there are at least 25 million compelled authorizations in the United States annually (Rothstein and Talbott 2007). The largest numbers of authorizations are for employment (10.2 million) and life insurance (6.8 million), but other forms of insurance and government benefits also generate numerous compelled authorizations.

Some statutes limit the permissible scope of disclosure. For example, workers' compensation laws in some states limit the health information disclosed to matters relevant to the workers' compensation claim (e.g. *Colorado Workers' Compensation Act,* Colo. Rev. Stat. § 8-47-203(1); *Louisiana Workers' Compensation Law*, La. Rev. Stat. Ann. § 23:1127(B)(1); *Minnesota Workers' Compensation Act*, Minn. Stat. § 176.138(b)). Similarly, federal law prohibits the disclosure of genetic information in the process of conducting preplacement medical examinations (see section 4.2.3 below). The main problem is, as noted above, there is no easy way to limit the scope of the disclosures. Consequently, it is common for the custodians of the health records simply to send the entire file, regardless of how broadly or narrowly the authorization is worded.

The most difficult and contentious issue regarding authorization is how health information may be used. Upon disclosure to a third party, use of the information is not a matter of privacy so much as it is a matter of how the information may inform health assessment or risk allocation. For example, when a long-term care insurer obtains the health records of an applicant for long-term care insurance, what information should the insurance company be able to use in underwriting? Certain genetic factors (along with prior head trauma, alcoholism, and other factors) are known to predispose individuals to Alzheimer's disease. Naturally, higher costs are associated with the care of affected individuals. Results of genetic tests and whole-genome sequencing information increasingly will be contained in EHRs. If insurers are permitted to use the results of a genetic test or to require their own genetic testing, an at-risk individual is likely to be denied

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

coverage or be charged higher premiums, a situation that some would call 'genetic discrimination.' On the other hand, if long-term care insurers were prohibited from using genetic information, there is likely to be an adverse selection of applicants (at-risk individuals are more likely to apply for insurance) who will be charged higher premiums for long-term care insurance. As more individuals are unable to afford private insurance policies, and will be forced to receive long-term care services (e.g. nursing home care) under the government's Medicaid program, higher tax revenues will need to be generated as a result (Rothstein 2001). Thus policies for health information uses and disclosures involve more complicated and contentious issues than merely informational health privacy.

4.2.2 Social media

Despite their very recent conception, social media have become ubiquitous in society and play an important role in the lives of many. The archetypal social media giant, Facebook, was launched from a college dormitory room in 2004. By 2012, it had over one billion active users. Twitter, created in 2006, boasted over 200 million users by 2013 who sent more than one billion tweets every three days. Similarly, YouTube, founded in 2005, features millions of videos uploaded for free by users across the world. The privacy issues surrounding these forms of social media, such as the broad disclosure of highly sensitive matters, are well known and often debated in contexts besides the health privacy issues of this chapter (Leary 2011; Swire 2012).

Like social media sites, health-based sites are becoming extremely important as health education portals and information dissemination centers. Some sites combine both social and health information media. PatientsLikeMe is a social network designed to provide a forum for patients and their families to share their experiences and stories for the benefit of other patients. In addition to being a valuable, online support network, PatientsLikeMe provides information about treatment options, research, and local support groups. Many patients freely upload their personal health information in the hope it will benefit others or aid research efforts. The Internet has enabled population-based health activities as well, including the Personal Genome Project, which aims to recruit 100,000 individuals interested in sequencing their genome for research (Personal Genome Project 2013).

Social networks can be very effective in sharing health information quickly and effectively (Terry 2010), and can also be used for less formal communications. Some physicians and other healthcare providers now use social network technology to establish patient groups based on diagnosis or affiliation with a specific provider. On this point, a number of issues surface. First, there is a concern about the propriety of physician interaction with patients in an informal domain to discuss health issues. Opinion 9.124 of the AMA, 'Professionalism in the Use of Social Media,' provides that '[i]f [physicians] interact with patients on the Internet, [they] must maintain appropriate boundaries of the patient–physician relationship in accordance with professional ethical guidelines just as they would in any other context' (AMA 2013: 1). Second, patient populations differ in their computer savviness and access to technology. Thus the 'digital divide' can be seen as exacerbating health disparities (Brodie *et al.* 2000; Chang *et al.* 2004). Third, there is concern about the security of sensitive health information contained on certain websites, which can be vulnerable to hacking, and the lack of protection against third-party disclosure. It is important to note that neither the *HIPAA Privacy Rule* nor any other federal health privacy rule applies to social media.

Both social media (located on public access websites) and EHRs (private repositories) present a major problem for individual privacy. The information, once posted, 'never goes away'

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

(Rosen 2010). Because privacy for social media sites is not regulated in the same ways as for EHRs, for example, they have not systematically addressed the issue of removing information. In comparison, many state laws prohibit deleting or removing information from a health record, electronic or not (Center on Medical Record Rights and Privacy 2013). Such laws were enacted to prevent the alteration of health information in contemplation of medical malpractice litigation. Restricting access at the request of the patient, however, would seem not to violate these statutes (see section 4.2.1 above).

In 2012, the European Commission proposed the *General Data Protection Regulation*, a comprehensive package aimed at amending the Data Protection Directive of 1995 (see section 4.1.6 above). Of particular relevance to this issue, article 17 of the proposal creates the 'right to be forgotten and erasure' on the Internet. At the request of the subject of the information, the controller of the data which has made it public (e.g. website) has an obligation to remove personal information and also to inform third parties to erase any links to or copies of the personal data (European Commission 2012). Other proposals are also being developed to promote the idea of online 'obscurity' (Hartzog and Stutzman 2013).

4.2.3 Genetic privacy

Genetic privacy, a subset of health privacy, has received a great deal of attention since the launch of the Human Genome Project in 1990 (Alpert 2003; Rothstein 1997). Genetic privacy raises the question of whether privacy law, ethics, and policy ought to focus on specific types of health concerns (e.g. genetic information, mental health information) or should be more general. Thomas Murray, borrowing terminology from the 'HIV exceptionalism' debates of the 1980s, coined the term 'genetic exceptionalism' to refer to the argument that genetics raises such unique ethical and legal issues that it ought to be addressed separately from other health conditions or information (Murray 1997). Among the reasons why genetics was said to be different is that it has implications for reproduction, family members, and members of the same ethnic group; the immutable nature of genetic inheritance; the predictive capacity of genetic information for future health; historical misuse of genetics; and the distinction afforded to genetic information by many members of the public.

Even though most scholars, including Murray, have concluded that genetic exceptionalism is unwarranted (Hellman 2003; Lemmens 2000; Suter 2001), virtually all genetic privacy and antidiscrimination laws in America, both at the federal and state levels, have been genetic-specific or 'exceptional' laws. The simple explanation is that genetic laws are narrower and therefore more politically feasible than legislation addressing broader social problems (Rothstein 2005; Suter 2001).

Numerous state laws address genetic privacy and the use of genetic information in health insurance and employment (National Conference of State Legislatures 2013). At the federal level, the most important law is the *Genetic Information Nondiscrimination Act* 2008 (GINA). GINA was not a response to a wave of genetic discrimination, but rather an attempt to 'allay [the public's] concerns about the potential for discrimination, thereby allowing individuals to take advantage of genetic testing, technologies, research, and new therapies' (GINA 2008, § 2(5)). GINA has several shortcomings, including the following: (1) GINA only applies to health insurance and employment and does not prohibit genetic discrimination in life insurance, disability insurance, long-term care insurance, or other potential uses of genetic information; (2) GINA prohibits discrimination based on genotype, but not phenotype, thereby extending protection only to individuals who are asymptomatic; and (3) GINA prohibits employers from requiring or requesting an individual to undergo genetic testing or to disclose the results of a genetic test as a condition

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

of employment. However, there is currently no feasible way to segment genetic from nongenetic information in health records, such that only nongenetic information is disclosed in determining whether an individual has the ability to perform essential job functions. Taking into account these limitations, it can be said that GINA has a limited though salutary aim, and it is unclear whether it has achieved even its modest goal.

Looking beyond genetic testing in the legislative context, a somewhat unusual feature of genetic testing is that, at least in the United States, it is widely promoted by direct-to-consumer (DTC) companies. There are different types of tests performed (e.g. ancestry, health risk assessment) and there are different motivations for obtaining them (e.g. family health history, curiosity). All DTC testing uses a home collection kit, modern genetic testing technology, proprietary analytics, and customer review of results via password-protected Internet access. In the United States, the legality of DTC genetic testing depends on the law of the state in which the consumer lives: it is lawful in about half the states (American Society of Human Genetics 2007). Typically, DTC testing companies have privacy policies indicating that individually identifiable results will not be given or sold to any other party. DTC companies, however, are not covered entities under the *HIPAA Privacy Rule* and there is little federal oversight of their practices with regard to quality as well as privacy (American Society of Human Genetics 2007). A ruling by the Food and Drug Administration in 2013 cast great doubt on the future of DTC genetic testing.

Another unregulated type of genetic testing is nonconsensual testing. Because of the rapid advances in genetic technologies, it is possible to perform a genetic analysis using small amounts of DNA. Consequently, genetic testing can be performed using residues of DNA (e.g. in blood, saliva) on commonly used items (e.g. sheets, drinking glasses) or abandoned property (e.g. used chewing gum, cigarette butts). Under American law, individuals generally have no legal rights in 'abandoned' property and no reasonable expectation of privacy in the DNA specimens left behind as a result of normal daily activities. Several commercial enterprises have seized on this opportunity to offer genetic testing services on a wide range of materials without any informed consent or verified chain of custody (Rothstein 2009; Joh 2011). One common use of this type of testing is surreptitious paternity testing. Although the results are not admissible in court because of the lack of a chain of custody, the testing is often the first step in challenging paternity.

In contrast to the United States, the United Kingdom enacted the *Human Tissue Act* 2004, section 45 of which makes it unlawful for any individual, without proper consent, to possess any 'bodily material' with the intent to have DNA testing performed. There are exceptions for medical treatment, law enforcement, research, and other uses. Persons found guilty of violating the Act are subject to a fine, imprisonment for up to three years, or both (*Human Tissue Act* 2004, § 45(3)).

Genetic privacy serves to illustrate the types of specialized concerns likely to be associated with informational discoveries related to many other new technologies. For example, the successful sequencing of the human genome spawned a series of large-scale research undertakings in proteomics, transcriptomics, matabanomics, toxicogenomics, pharmacogenomics, epigenomics, and microbiomics. Each new application raises the issue of whether information generated by novel research methods should be regulated separately or under more general laws applicable to health information.

4.3 Conclusion

Privacy and confidentiality are essential components of modern, patient-centered healthcare. Patients expect their physicians and other healthcare providers to safeguard the confidentiality

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

of their sensitive health information, and to obtain the patient's permission for any nonroutine uses and disclosures. Without a reasonable expectation of confidentiality, many patients would be reluctant to disclose personal, often-sensitive, health information vital to appropriate care.

Despite widespread public support for privacy and confidentiality principles, legal protection, especially in the United States, is fragmented and inadequate. The primary national law on informational health privacy, the *HIPAA Privacy Rule*, is not comprehensive in application, contains numerous exceptions, and does not provide adequate remedies for individuals whose privacy has been violated.

Internationally, data protection laws typically have wider applicability than privacy laws in the United States because they are broader and reach both the public and private sectors. General provisions for transparency, data collection, heightened standards for sensitive information, enforcement, and oversight are also part of the data protection framework. The European Commission's proposed *General Data Protection Regulation* is a comprehensive legislative package that, if adopted, will apply to all European Union member states and establish more uniform and stringent protections.

Even as legal and ethical standards are still attempting to keep pace with modern healthcare, new developments in science and technology race ahead. This chapter has addressed three contemporary challenges. First, the shift from paper-based to electronic health records and systems will result in individual health records that are interoperable, comprehensive, and longitudinal. Healthcare providers, privacy experts, computer scientists, and policymakers are struggling to balance privacy with safety and efficiency in regulating access to and use of sensitive, electronic health information. Second, social media platforms, virtually all developed in the last decade, have allowed users to post vast quantities of personal information, including health information, voluntarily online. Social media therefore raise issues concerning the transparency of the website's privacy rules, information security, secondary uses of the information, and procedures to remove personal information from sites. Third, new clinical and research topics and methods, exemplified in genomics, involve analyzing large data sets of sensitive information. Thoughtful, nuanced regulation has proven to be elusive in many countries.

References

Alpert, S. (2003) 'Protecting medical privacy: challenges in the age of genetic information,' *Journal of Social Issues*, 59 (2): 301–22.

American Medical Association (AMA) (2011) *Code of Medical Ethics of the American Medical Association*. Chicago: American Medical Association.

American Medical Association (AMA) (2013) 'Opinion 9.124: Professionalism in the use of social media,' viewed 10 September 2013 at: http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9124.page.

American Society of Human Genetics (ASHG) (2007) 'ASHG statement on direct-to-consumer genetic testing in the United States,' *American Journal of Human Genetics*, 81 (3): 635–7.

Atkinson, P., Glasner, P., and Lock, M. (eds) (2009) *Handbook of Genetics and Society: Mapping the New Genomic Era*. London: Routledge.

Australian Medical Association (2006) 'Code of Ethics,' viewed 10 September 2013 at: https://ama.com.au/codeofethics.

Beauchamp, T. L. and Childress, J. F. (2013) *Principles of Biomedical Ethics*, 7th edn. New York: Oxford University Press.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

Bloustein, E. J. (1964) 'Privacy as an aspect of human dignity: an answer to Dean Prosser,' *New York University Law Review*, 39 (6): 962–1067.

British Medical Association (2013) 'Confidentiality and Disclosure of Health Information Tool Kit,' viewed 10 September 2013 at: http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit.

Brodie, M., Flournoy, R. E., Altman, D. E., Blendon, R. J., Benson, J. M., and Rosenbaum, M. D. (2000) 'Health information, the internet, and the digital divide,' *Health Affairs*, 19 (6): 255–65.

California Health Care Foundation (2005) 'National Consumer Health Privacy Survey 2005,' viewed 10 September 2013 at: http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/C/PDF%20ConsumerPrivacy2005ExecSum.pdf.

Canadian Medical Association (CMA) (2004) 'CMA Code of Ethics,' viewed 10 September 2013 at: http://policybase.cma.ca/dbtw-wpd/PolicyPDF/PD04-06.pdf.

Chalmers, J. and Muir, R. (2003) 'Patient privacy and confidentiality,' *British Medical Journal*, 326 (7392): 725–6.

Chang, B. L., Bakken, S., Scott Brown, S., Houston, T. K., Kreps, G. L., Kukafka, R., Safran, C., and Stavri, Z. (2004) 'Bridging the digital divide: reaching vulnerable populations,' *Journal of the American Medical Informatics Association*, 11 (6): 448–57.

Data Protection Working Party (2007) 'Working Document on the processing of personal data relating to health in electronic health records (EHR),' viewed 10 September 2013 at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf.

Georgetown University Health Policy Institute (n.d.) 'Center on Medical Record Rights and Privacy,' viewed 10 September 2013 at: http://www.hpi.georgetown.edu/privacy/records.html.

Hartzog, W. and Stutzman, F. D. (2013) 'The case for online obscurity,' *California Law Review*, 101 (1): 1–50.

Hellman, D. (2003) 'What makes genetic discrimination exceptional?' *American Journal of Law and Medicine*, 29 (1): 77–116.

Hiller, J., McMullen, M. S., Chumney, W. M., and Baumer, D. L. (2011) 'Privacy and security in the implementation of health information technology (electronic health records): U.S. and EU compared,' *Boston University Journal of Science and Technology Law*, 17 (1): 1–40.

Hull, S. C., Sharp, R. R., Botkin, J. R., Brown, M., Hughes, M., Sugarman, J., *et al.* (2008) 'Patients' views on identifiability of samples and informed consent for genetic research,' *American Journal of Bioethics*, 8 (10): 62–70.

Joh, E. E. (2011) 'DNA theft: recognizing the crime of nonconsensual genetic collection and testing,' *Boston University Law Review*, 91 (2): 665–700.

Leary, M. G. (2011) 'Reasonable expectations of privacy for youth in a digital age,' *Mississippi Law Journal*, 80 (3): 1033–94.

Lemmens, T. (2000) 'Selective justice, genetic discrimination, and insurance: should we single out genes in our laws?' *McGill Law Journal*, 45 (2): 347–412.

Levin, A. and Nicholson, M. J. (2005) 'Privacy law in the United States, the EU, and Canada: the allure of the middle ground,' *University of Ottawa Law and Technology Journal*, 2 (2): 357–95.

Miles, S. H. (2004) *The Hippocratic Oath and the Ethics of Medicine*. New York: Oxford University Press.

Murray, T. H. (1997) 'Genetic exceptionalism and "future diaries": Is genetic information different from other medical information?' in M. A. Rothstein (ed.), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven, CT: Yale University Press.

National Committee on Vital and Health Statistics (NCVHS) (2006) 'Privacy and Confidentiality in the Nationwide Health Information Network,' viewed 10 September 2013 at: http://www.ncvhs.hhs.gov/060622lt.htm.

National Committee on Vital and Health Statistics (NCVHS) (2008) 'Letter to Michael O. Leavitt, Secretary of Health and Human Services dated February 20, 2008,' viewed 10 September 2013 at: http://www.ncvhs.hhs.gov/080220lt.pdf.

National Conference of State Legislatures (NCSL) (2013) 'Genetic Nondiscrimination Laws,' viewed 20 November 2013 at: http://www.ncsl.org/research/health/genetic-privacy-laws.aspx.

Office of the Privacy Commissioner of Canada (2009) *Privacy Legislation in Canada*, fact sheet, viewed 10 September 2013 at: http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp.

Personal Genome Project (2013) Viewed 10 September 2013 at: http://www.personalgenomes.org.

Pritts, J. L. (2002) 'Altered states: state health privacy laws and the impact of the federal health privacy rule,' *Yale Journal of Health Policy, Law, and Ethics*, 2 (2): 325–50.

Prosser, W. L. (1960) 'Privacy,' *California Law Review*, 48 (3): 383–423.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

Reich, W. T. (ed.) (1995) 'Oath of Hippocrates,' *Encyclopedia of Bioethics*, rev. edn. New York: Simon & Schuster Macmillan, Vol. 5.
Richards, N. M. and Solove, D. J. (2007) 'Privacy's other path: recovering the law of confidentiality,' *Georgetown Law Journal*, 96 (1): 123–82.
Rosen, J. (2010) 'The web means the end of forgetting,' *New York Times Magazine*, viewed 10 September 2013 at: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=alland.
Rothstein, M. A. (ed.) (1997) *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*. New Haven, CT: Yale University Press.
Rothstein, M. A. (2001) 'Predictive genetic testing for Alzheimer's disease in long-term care insurance,' *Georgia Law Review*, 35 (2): 707–33.
Rothstein, M. A. (2005) 'Genetic exceptionalism and legislative pragmatism,' *Hastings Center Report*, 35 (4): 27–33.
Rothstein, M. A. (2009) 'Genetic stalking and voyeurism: a new challenge to privacy,' *University of Kansas Law Review*, 57 (3): 539–78.
Rothstein, M. A. (2010a) 'The Hippocratic bargain and health information technology,' *Journal of Law, Medicine and Ethics*, 38 (1): 7–13.
Rothstein, M. A. (2010b) 'Is deidentification sufficient to protect health privacy in research?' *American Journal of Bioethics*, 10 (9): 3–11.
Rothstein, M. A. (2011) 'Constitutional right to informational health privacy in critical condition,' *Journal of Law, Medicine and Ethics*, 39 (2): 280–4.
Rothstein, M. A. (2012) 'Access to sensitive information in segmented electronic health records,' *Journal of Law, Medicine and Ethics*, 40 (2): 394–400.
Rothstein, M. A. and Talbott, M. K. (2006) 'Compelled disclosure of health information: protecting against the greatest potential threat to privacy,' *Journal of the American Medical Association*, 295 (24): 2882–5.
Rothstein, M. A. and Talbott, M. K. (2007) 'Compelled authorizations for disclosure of health records: magnitude and implications,' *American Journal of Bioethics*, 7 (3): 38–45.
Rynning, E. (2007) 'Public trust and privacy in shared electronic health records,' *European Journal of Health Law*, 14 (2): 105–12.
Schwartz, P. M. and Solove, D. J. (2013) *Privacy Law Fundamentals*, 2nd edn. Portsmouth, NH: International Association of Privacy Professionals.
Silversides, A. (2010) '"Chaos" protects health privacy,' *Canadian Medical Association Journal*, 182 (1): E37–E38.
Starr, P. (1982) *The Social Transformation of American Medicine*. New York: Basic Books.
Suter, S. M. (2001) 'The allure and peril of genetic exceptionalism: Do we need special genetics legislation?' *Washington University Law Quarterly*, 79 (3): 669–748.
Swire, P. (2012) 'Social networks, privacy, and freedom of association: data protection vs. data empowerment,' *North Carolina Law Review*, 90 (5): 1371–415.
Terry, N. P. (2010) 'Physicians and patients who "friend" or "tweet": constructing a legal framework for social networking in a highly regulated domain,' *Indiana Law Review*, 43 (2): 285–341.
US Department of Justice (2012) 'Privacy Act Overview, 2012 Edition: Policy Objectives,' viewed 17 November 2013 at: http://www.justice.gov/opcl/privacyactoverview2012/1974polobj.htm.
Warren, S. D. and Brandeis, L. D. (1890) 'The right to privacy,' *Harvard Law Review*, 4 (5): 193–220.
World Medical Association (WMA) (2006) 'WMA International Code of Medical Ethics,' viewed 20 September 2013 at: http://www.wma.net/en/30publications/10policies/c8/index.html.

Legislation

Australia

Privacy Act of 1988.

Canada

Canadian Charter of Rights and Freedoms.
Personal Information Protection and Electronic Documents Act, RSC 2000, c. 5.
Privacy Act of 1983, RSC 1985, c. P-21.

Downloaded By: 10.3.97.143 At: 18:22 08 Dec 2023; For: 9780203796184, chapter4, 10.4324/9780203796184.ch4

European Union

Charter of Fundamental Rights of the European Union 2000 (EU).
Council of Europe (1950) *European Convention on Human Rights* (EU).
European Commission (2012) *Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (EU).
European Union (2002) Directive 2002/58/EC – Directive on Privacy and Electronic Communications.
European Union (1995) Directive 95/46/EC – Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

United Kingdom

Human Tissue Act of 2004, § 45(3).

United States

Colorado Workers' Compensation Act, Colo. Rev. Stat. § 8-47-203(1).
Freedom of Information Act of 1966, 5 USC § 552.
Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233.
Health Insurance Portability and Accountability Act of 1996, Privacy Rule of 2001, 45 CFR Parts 160 and 164.
Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
Louisiana Workers' Compensation Law, La. Rev. Stat. Ann. § 23:1127(B)(1).
Minnesota Workers' Compensation Act, Minn. Stat. § 176.138(b).
Privacy Act of 1974, 5 USC § 552a.
United States Constitution.

Cases

National Aeronautics and Space Administration v. *Nelson* (2011) 131 SCt 746.
Whalen v. *Roe* (1977) 429 US 589.