June 20, 2008

HIPAA and Its Privacy Regulations: Is There Too Much Privacy Regulation on Health Care Information?

Yuhong Wu
HIPAA and Its Privacy Regulations:

Is there too much privacy regulation on health care information?

I. Introduction

Over the last decade the development of information technologies, like personal computer, data warehousing, internet and search engine, etc., has brought significant changes to every sector of the U.S. economy, including health care industry. Today, it has almost become daily routine for every health care practitioner to use information technologies to collect, store and use health care information at every stage of treatment of patients. Health care providers and health insurance companies have become more and more relied on health care information to facilitate their decision-making. In the meantime, consumers are enjoying fruits that information technologies bear in health care industry. For example, consumers can use websites and search engines, like WebMD, drugstore.com, Google and Kosmix, to educate themselves on health and diseases, to consult preventive treatments, and to purchase drugs. According to a study in 2000, there were over sixty-five million American Internet users who have sought health and medical information online, and many of them used online information to make important decision about medical care.

The value of heath care information has been widely recognized. Scholars have pointed out that the effective function of health care system depends “in part on the accuracy, currency, completeness, and availability of health data.” For example, by migrating health care information from a paper-system to an electronic system, health data can be “easily located, collated and organized,” thus the flow of health care

1 The Online Health Care Revolution: How the Web helps American take better care of themselves, Pew Internet & American Life Project (November 2000)
2 Lawrence O. Gostin, Health Information Privacy, 80 Cornell, L. Rev. 451, 452(March, 1995)
information is so smoothed as to facilitate diagnosis and treatment and reduce medical errors.\(^3\) It has been advocated that access to health care information is critical to help consumer make informed decisions on her health care, to provide more effective, high quality and cost-efficient health care services, to fight fraud and abuse, to create better health policies, and to facilitate medical and pharmaceutical researches.\(^4\) A report by the Federal Trade Commission and Department of Justice has emphasized the importance of information to improve competition in health care market.\(^5\) Besides those inherent values of health care information, growing commercial usages of health care information have made health care information a critical strategic asset to many players in health care industry.\(^6\)

However, while access to health care information brings huge benefits to public, it raises real concerns on privacy too. Consumers worry that improper use and disclosure of their health information may “leave them vulnerable to unwanted exposure, stigma, discrimination and serious economic losses.”\(^7\) A study showed that approximately 80% of those surveyed in public opinion polls were concerned about their personal privacy in

---

\(^3\) Pew Internet & American Life Project, Institute For Healthcare Research and Policy, Georgetown University, Exposed Online: Why the New Federal Health Privacy Regulation Doesn’t Offer Much Protection to Internet Users 6-8 (Nov. 2001). http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf

\(^4\) Id. at 453.

\(^5\) David Hyman, Executive Summary of the Report, Improving Health Care: A Dose of Competition (July, 2004). In the report, it is recommended that “private payors, governments, and providers should furnish more information on prices and quality to consumers in ways that they find useful and relevant, and continue to experiment with financing structures that will give consumers greater incentives to use such information.”

\(^6\) Paul M. Schwartz, Privacy and the Economics of Personal Health Care Information, 76 Tex. L. Rev. 1, 12 (1997) (noting that “(t)he practice of medicine increasingly depends on the large-scale comparison and analysis of personal medical information. As a result, health care institutions view personal medical information as a critical strategic resource”).

In a 1993 Harris-Equifax poll specifically on health information privacy, eight percent of the respondents believed that consumers had lost all control over their health information privacy, and eighty-five percent of respondents believed that protecting health information privacy is a top priority. Anecdotes that information technologies lead to new kinds of intrusion to health information privacy further elevates public concerns on health information privacy.

In response to public concerns on health care information, in 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) that included an “Administrative Simplification” provision that addressed privacy and confidentiality of health information. On December 28, 2000, Department of Health and Human Services (HHS) published the final privacy regulations, the first federal health privacy regulation, modified them on August 14, 2003, and began enforcing the regulation on April 14, 2003 for most covered entities.

After three years of enforcement of HIPAA privacy regulation, although it is debated whether HIPAA and it privacy regulation achieve their goal to protect privacy of health care information, it appears that they have unreasonably restricted the use of health care information because HIPAA and its privacy regulation have created

---

8 Alan F. Westin et al., Health Care Information Privacy: A Survey of the Public and Leaders 23(1993)
9 Id. at 2.
10 Schwartz, at 43. One patient recently went to an internist for a routine treatment only to discover that this health care professional had electronic access to her psychiatrist's complete notes. These digital data were available not only to all other physicians, but to everyone, including nurses and clerical staff, working for the large HMO in Boston to which she belonged.
11 Pew Internet & American Life Project, Institute For Healthcare Research and Policy, Georgetown University, Exposed Online: Why the New Federal Health Privacy Regulation Doesn’t Offer Much Protection to Internet Users 6-8 (Nov. 2001). http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf. In the paper, it is suggested that given the wide range of activities on the Internet and the relatively narrow scope of the regulation, it is likely that a great deal of health information collected on health Web sites will not be covered by the new regulation.
anticommons property of health care information. Particularly, HIPAA and its regulation thwart parties, other than established health care providers, health care insurance plan, and health data clearing house, from actively getting involved in exploring legitimate potential use of health care information. Part II of this paper will do a brief review on history of privacy regulation of health care information. It will explore the debates over privacy of health care information and provide positions both for and against privacy regulation of health care information. Part III will provide a discussion of the essence of HIPAA and its privacy regulation. Part IV will explain how the privacy rights of health care information defined by HIPAA and its privacy regulation end up in an anticommons form and therefore lead to under-consumption of health care information. Finally, the author concludes that HIPAA and its privacy regulation result in over-regulating the use and disclosure of health care information and thus unreasonably prevent the optimal use of health care information.

II. Background

A. When Health Care Information becomes a privacy issue?

In old days, privacy of health care information has not stirred the nerve of this nation. In medical practice, health care information was documented on paper and kept locally in physicians’ offices. As “in ordinary day to day life . . . the physician answered to no one but himself,”12 individual health care information was rarely shared by parties than patients and their physicians. Outside the context of treating individual patient, health care information had little value, except for limited educational and research purpose. Therefore privacy of health care information was conveniently protected by

12 Timothy Stoltzfus Jost, Oversight of the Quality of Medical Care: Regulation, Management, or the Market?, 37 Ariz. L. Rev. 825, 831 (1995).
confined access to health information due to the local nature of medical practice and medical record management and lack of market value.

As organizational medical practice and health insurance entered the stage of health care, access to health care information was not only limited to patients and physician any more. Parties outside a patient-physician relationship, such as hospital administrators, employers and insurance companies gained access to individual health care information. Health care information started serving not only the primary purpose of diagnosis and treatment, but the secondary purpose of administration, reimbursement and insurance policy making. Although at this stage the possibility of exposure of health information to unwanted eyes increased, concerns on privacy of health care information were limited because of the prohibitive cost of aggregating and searching health information. Just imagining the manpower and expenses needed to manually search through paper records from file rooms located at different places and duplicate them, a person will not be surprised that there was lack of incentive for people to explore health information. The inconvenient access to health information maintained a natural shield against unwanted intrusion, thus protecting the privacy of health information.

But after the big-bang in information technology, things have changed. Information technology makes creation, transmission, sharing and storage of personal health care information extremely efficient at very low cost. It is hard for health care industry to ignore the saving and productivity resulting from adoption of information technology. More important, besides primary use in individual medical treatment, patient management and financial reimbursement, other applications of health care information, such as for the purposes of education, regulatory purposes, commercial uses,

---

research, and public health, have become so practicable that health care information becomes a marketable asset.

While information technology brings great efficiency and productivity to healthcare industry and generates huge volume of valuable information, it also raises serious concerns on privacy of healthcare information. First, the volume and comprehensiveness of and easiness of access to healthcare information managed by information system may make accidental divulge disastrous. An unsecured information system will make personal healthcare information vulnerable to unwanted exposure. Second, as health care information becomes a marketable asset, the incentive of holders of healthcare information changes. People worry that health care providers, employers and insurance companies may profit from healthcare information under their control at the cost of consumers. However it may be argued that the concern on privacy of healthcare information is overstated. Although information technology may make the consequence of accidental disclosure of person healthcare information more serious, information technology offers solutions to address security problem too. A well designed information system with necessary security features provides no less protection than traditional paper record system does. Regarding to incentive changes, holders of healthcare information are not left unguarded. Generally it is in their self-interests that holders of healthcare information properly protect their information assets. Because inappropriate use or disclosure of personal healthcare information will cause lawsuits, damages to holders’ reputation and

15 See note 10.
16 See note 8.
aggressive regulation against holders, holders’ incentive to profit from healthcare information under their control is balanced.

B. Privacy Regulation of Health Information before HIPAA

Before HIPAA, the confidentiality and privacy of health information have largely been covered by state laws. Almost every state provides some form of protection for health information. Generally states recognize patients’ rights to access to their health information and exclude other from accessing to their health information. Also states mandate disclosure of personal health information, without patients’ authorization, under certain circumstances, such as for public health activities or law enforcement purpose. Protection of privacy of health information can be based on the implied promise of confidentiality in the physician-patient relationship, violation of the right of privacy, violation of professional licensing standards and tort, like defamation.

However, every state approaches privacy and confidentiality through different statutes, regulations and cases, and thus leaves many gaps and overlap in the laws. For example, a New York Court ruled that a spouse should not be given psychiatric information unless the patient authorizes disclosure, while some other states authorize disclosure of psychiatric information to spouse. The lack of uniform standard on privacy and confidentiality of health information creates particular problems and loopholes in modern health care activities. For example, today in a medical transaction parties from several states may participate. Some states do not consider situation like this


\[18\] Annotation, Physician’s tort liability for unauthorized disclosure of confidential information about patient, 48 A.L.R. 4th 668

\[19\] MacDonald v. Clinger, 84 A.D.2d 482, 446 N.Y.S.2d 801(4th Dep’t 982)

\[20\] E.g., Iowa Code Ann. § 229.25.
and some states handle the situation differently.\textsuperscript{21} Another example is private companies providing self-insurance under Employment Retirement Income Security Act (ERISA). In the context of previously existing weak federal privacy protection, ERISA has created a considerable loophole for self-insured companies. Under ERISA, a private company that opts for self-insurance will be subject neither to constitutional requirements for informational privacy (due to the lack of state action) nor to any existing state regulations (due to ERISA preemption).\textsuperscript{22} Therefore federal privacy regulations of health information are necessarily required.

However, before HIPAA, federal legal system did not provide a comprehensive protection for health information.\textsuperscript{23} Health information, treated as general issue of privacy and confidentiality, may be protected by other federal regulations when it falls under the coverage of a specific law.\textsuperscript{24} For example, if health information is possessed by government agencies, the health information will be subject to protection of Private Act of 1974.\textsuperscript{25} Also national professional organizations, like Joint Commission on Accreditation of Healthcare Organization, impose responsibility on hospital to protect health information “against loss, destruction, tampering and unauthorized access or use.”\textsuperscript{26} But existing protections of privacy of health information are weak and limited in scope.

In 1990s, as healthcare costs were increasing annually in double-digit percentage, public and private groups started discussing to reduce health care spending through

\textsuperscript{22}Schwartz, at 47.
\textsuperscript{23}Telemedicine: Diagnosing the Legal Issues, Health Law Handbook 1, 55(2001)
\textsuperscript{24}Daniel J. Solove, The Origin and Growth of Information Privacy Law, 828 PLI/PAT 23, 60
\textsuperscript{25}5 USC § 552a
\textsuperscript{26}1995 Joint Commission CAMH, at 383.
information technologies. As a by-product of the national legislative focus on reducing the administrative costs of health coverage, the issue of privacy and confidentiality of health information was brought on the table. In 1996, Congress passed HIPAA that included an “Administrative Simplification” provision that addressed privacy and confidentiality of health information and directed the Secretary of HHS to issue final regulations establishing privacy standards, if Congress failed to enact privacy standard within three years of the enactment of HIPAA. As Congress missed the HIPAA-mandated deadline of August 1999, HHS published the final privacy regulations on December 28, 2000, modified them on August 14, 2003, and began enforcing the regulation on April 14, 2003 for most covered entities. It is claimed that the privacy regulation will give consumer control over their health information, set boundaries on medical records use and release, and ensure the security of personal health information.

C. Debates on Privacy of Health Information

a. Health Information: an issue of rights or goods?

In 1890, Warren and Brandeis published “The Right to Privacy”, a milestone paper that had brought the concept of privacy into law. The authors advocated that “the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others.” The author noted that the right of privacy was not based upon property, because “the value of the production is found not in the right to take profits . . . but in the peace of mind or the

27 Marilou, M. King, HIPAA’s Privacy Standards: Driving a Wedge Between Patients and the Health Field, Health Law Handbook 1, 4(2001)
28 HIPAA §264.
29 Daniel J. Solove, The Origin and Growth of Information Privacy Law, 828 PLI/PAT 23, 34
30 Samuel D. Warren & Louis D. Brandies, The Right to Privacy, 4 HARV. L. REV. 193, 198(1890)
relief afforded by the ability to prevent any publication at all . . ." In a series of cases, courts had elaborated on the right of privacy. In 1977, the Supreme Court in Whalen v. Roe defined the “constitutional right to information privacy”, a right protecting the “individual interest in avoiding disclosure of personal matters.” Obviously, privacy to health information falls under the category of the “constitutional right to information privacy.”

However, legal scholars, like Richard Posner and Richard Epstein, disagree to the concept of the “constitutional right to information privacy.” In his 1978 paper “The Right of Privacy”, Posner argues that privacy should be viewed as, other than a preference, an "intermediate good" having an instrumental value and functioning as a form of "inputs into the production of income or some other broad measure of utility or welfare." Therefore privacy matters to the extent that it serves to increase wealth and social utility. Moreover privacy may be treated as a form of wealth and utility, because people try to “sell” themselves to the world by controlling information relating to them. Although Posner did not successfully reverse the public perception of a constitutional right to information privacy, he introduced a valuable approach to analyze information privacy in terms of economy, which will be discussed more below.

b. **Economic Analysis of Privacy of Health Information**

In economic analysis of privacy of health information, debates were focused on four aspects: (1) information asymmetries; (2) transaction cost; (3) rationality of market participant; and (4) distortion of market behaviors.

---

31 Id, at 200.
34 Schwartz, at 8.
35 Id.
Posner argues that privacy creates harmful information asymmetries that prevent exchanges necessary to an efficient marketplace. Under privacy protection, health information relating to an individual is unevenly distributed between market participants because an individual has the right to exclude other from access to her health information. Naturally, it is in individual’s interest to hide bad health information from other parities in health care market, such as employers and insurance companies. Studies have indicated that individual’s tendency of hiding bad information is real.\textsuperscript{36} Posner argues that individual:

profess high standards of behavior in order to induce others to engage in social or business dealings with them from which they derive an advantage but at the same time they conceal some of the facts that these acquaintances would find useful in forming an accurate picture of their character. Privacy facilitates attempts by individuals "to manipulate the world around them by selective disclosure of facts about themselves." Dishonesty will prove the best policy for many if the law acts to protect personal information.\textsuperscript{37}

Similarly, Richard Epstein argues against privacy protection of genetic information because of information asymmetries that will result in that “truth is discouraged and lies are protected, promoted and necessary.”\textsuperscript{38}

To some legal scholars, Posner’s information asymmetry argument is not convincing. Paul Schwartz argues that Posner has overstated the effect of perfect information on the functioning of market dynamics.\textsuperscript{39} He pointed out a number of studies

\begin{itemize}
    \item \textsuperscript{36} Most studies and surveys conducted so far have been focused on the people’s concerns that their health care information will be used improperly by health care providers, employers and insurance companies. However these studies reflect people’s general tendency of preferring hiding bad information from others if given chances.
    \item \textsuperscript{37} Posner, at 400.
    \item \textsuperscript{39} Paul M. Schwartz, Privacy and the economics of personal health care information, 76 Tex. L. Rev. 1, 24. (1997)
\end{itemize}
suggesting that “a wide variety of markets are able to function despite imperfect
information” and “almost all decisions are based on less than complete information and
complete understanding of all relevant areas.”40

In Schwartz’s view, the issue of information asymmetry is not simply “whether
one party has more information than another”, but, more important, whether the
information disparities between parties will “have negative effect on their negotiations
and on the functioning of the marketplace.”41 In other words, Schwartz seems to believe
that, because information asymmetries are unavoidable, information asymmetries should
be structured by law in favor of individual consumer. Schwartz demonstrates the
“negative effect on negotiation” with the example of “gag rules”42. The example shows
that, without privacy protection of health information, health care providers and
insurance companies would acquire informational monopoly because of their superior
market positions, organizational advantages and general ignorance of consumers. Health
care providers and insurance companies will use their information monopoly to advance
their interests, which often conflict with interest of consumers (for example, insurance
companies’ interest in reducing health care costs and individual’s interest in access and
quality of health care are often in confliction). Therefore information asymmetries in
favor of health care providers and insurance companies will not “generate optimal
information to guide individual decision-making about the use of personal medical
data.”43

40 Id.
41 Id.
42 Id. at 47. Gag rules are clauses that prevent physician from telling patients about treatment options for
which the HMO does not reimburse. Because agreements, like “gag rule” between insurers and physicians
are generally confidential, unless physician freely share their superior knowledge, health care consumers
will not be able to formulate the preferences for which they wish to negotiate.
43 Id, at 49.
Furthermore, Schwartz argues that Posner and Epstein overstate the benefits from open access to personal data. For example, Schwartz is skeptical about the promised economic benefits of unrestricted disclosure of genetic data because genetics as a predictive tool bears high uncertainty due to “(1) the heterogeneous origins of most diseases, (2) the phenomenon of genetic polymorphism, and (3) the fluid state of current genetic knowledge.”

The second reason against privacy of health information is transaction cost. Posner argues that privacy imposes transaction cost so as to obstruct efficient marketplace transactions. Individual privacy right increases cost of negotiating among the affected parties. And “generally the costs of a transaction rise with the number of parties to the transaction – perhaps exponentially.” In some circumstances, transaction cost could outweigh potential benefits of transactions so that parties forgo the beneficial usage of health information. Posner gives the examples of the Bureau of the Census and magazine subscription-list in which complicated negotiations with affected parties drive up transaction cost and result in less benefit to society. Consequently, Posner believes that access to personal information should not be limited because free access will increase social utility.

Some legal scholars disagree with Posner’s argument of transaction cost. It is pointed out that new information technology is “low-friction” regarding information costs.

---

44 Id, at 20.
45 Posner, at 397.
46 Id, at 51.
47 Id. at 404. As a general rule, Posner concludes privacy in personal information should be protected only to the extent to which it increases social utility and assigned away from individuals when it does not. Posner provides a test beginning with the inquiry whether (1) personal information is a byproduct of socially productive activity and (2) its compelled disclosure would impair the incentives to engage in that activity. This two-pronged analysis leads Posner to a judgment that most facts about people should not be protected.
regardless of the number of parties involved.48 It is argued that with help of technologies, “the transaction costs for all the parties are minor whether viewed at the moment of negotiating the agreement (the ex ante cost) or complying with it (the ex post cost).”49 Schwartz uses the example of supermarket to illustrate this point.50 When consumers apply memberships, supermarkets inform consumers in written information regarding proposed data use and give them chance to decline outside use of these data. Equipped with the extraordinary data-processing capacity of information technologies, supermarkets minimize the transaction cost of using consumer information.

The third debate ground is the rationality of market participants. Epstein argues that “individual employers driven by concerns of profit and loss are much more likely to rationally” use genetic information.51 As rational market participants aiming to maximize their market values, employers should have incentive to discriminate against workers when workers’ genetic conditions impose risk and cost against them. Similarly, insurance companies will use genetic information against applicants only when applicants’ genetic conditions pose future risk. When both of these groups act adversely to individuals who do pose greater risks, they are using genetic information in a rational way so as to advance their own interests. Driven by their profit-seeking nature, employers and insurance companies have no incentive to irrationally use genetic information to discriminate workers and applications.

Other legal scholars challenge the assumption that entrepreneurs and businesses are rational to make economically efficient use of personal information. Studies have

48 Schwartz, at 45 footnote 145.
49 Schwartz, at 24.
50 Id, at 23.
51 Epstein, at 18.
shown that employers and insurance companies have often discriminated between employees with different health conditions based on social stigma, ignorance and misunderstandings.\textsuperscript{52} For example, a survey found that supervisors commonly overestimate the actual experience of cancer patients regarding fatigue, infections and nausea during treatment.\textsuperscript{53} The complexity of modern health information, like genetic information, is more likely to cause misunderstanding and thus lead to irrational decisions. Moreover, scholars have pointed out the some individuals allow their “acquired taste for discrimination” to override their economic self-interest.\textsuperscript{54} So Schwartz asserts that employers do not “invariably make economically efficient use of personal data” and are “more complicated creature than the fully rational employer of Posner’s and Epstein’s imagination.”\textsuperscript{55}.

Furthermore, both sides on privacy of health information raise the concern of market distortion. People against privacy of health information argue that privacy causes adverse selection and reverse discrimination: being able to hide bad health information from insurance companies, people who are sick or more likely to be sick shift their burden to insurance companies and healthy people. The other side argues that open access to health care or genetic information will distort individual behavior: “health care consumer will limit or modify the information they share with those who provide treatment;” patient will decrease seeking preventive care; and employees will be locked

\textsuperscript{52} Domestic and International Data Protection Issues: Hearings Before the Government Information, Justice, & Agriculture Subcomm. of the House Comm. on Government Operations, 102d Cong. 229 (1991) [hereinafter Data Protection Hearings] at 229 (“[E]ven the U.S. military misunderstood the consequences of being only a carrier.”);
\textsuperscript{53} Ellen Neuborne, Illness on Job Adds Insult to Injury, USA Today, Jan. 14, 1997, at 12A.
\textsuperscript{54} Schwartz, at 31.
\textsuperscript{55} Schwartz, at 30.
in their current job and thus “labor market efficiency suffers.” Moreover, the other side argues that “open disclosure permits certain workers to be cast off into an increasingly strained public insurance market,” and “will cause harmful risk segmentation” in insurance markets.

D. Proposed Solutions to Privacy of Health Information

Based on economical analysis, different solutions to privacy of health information were proposed. Posner suggests “not protection for facts about people – my ill health . . . would not be facts over which I had property rights.” Epstein supports open access to genetic information. Generally, their position is that there is no need of privacy regulation on health care information but let market searches out the optimal use of health information.

While agreeing with Posner that sharing of personal information is essential to political, commercial and communal life, Paul Schwartz believes that “because much information may be both harmful and useful in different contexts for different reasons, a socially optimal distribution of information is unlikely to exist at either extreme on the privacy/disclosure continuum.” Schwartz further believes that, despite a strong public demand for privacy of health care information, market fails to generate efficient rules for access to personal medical data. Therefore, Schwartz concludes that privacy standard of health care information should be set through law.

Schwartz discusses the multifunctional character of health care information and their implication in setting the standard of a health care information privacy law.

---

56 Id, at 72-73.
57 Id.
58 Posner, at 404.
59 Schwartz, at 53.
60 Id, at 47.
Schwartz argues that “personal health care information has become multifunctional” as “computer changes information into a fluid form that makes it applicable at many stages of administration.” 61 This change raises “a more complex issue than a choice between privacy or disclosure.” 62 “Rather than establishing a single rule regarding disclosure or privacy, the law must now engage in more complex kinds of standard setting. It must create fair information practices that are capable of responding to the different contexts in which personal medical data are used.” 63 Here, “the idea of standard setting through default and mandatory rules” 64 comes handy.

Default rules are those that parties can negotiate around; in contrast, mandatory rules set immutable norms on parties. By setting a default rule, “fewer parties are forced to negotiate around the law, and transaction costs can be lowered.” 65 Moreover, such standard setting is beneficial because it is unlikely to result in situation unanticipated by parties. In contrast to default rules, mandatory rules are utilized to set fundamental background conditions around which parties are not permitted to negotiate.

Schwartz suggests a privacy default rule, rather than a disclosure default rule recommended by Posner and Epstein. Referring to Richard S. Murphy’s paper, Schwartz argues that “a default for disclosure of personal data will be difficult to bargain around because merchants may find it difficult to tell which of their customers value data privacy more highly, and consumers will lack knowledge regarding the use of their information and its value.” 66 But a privacy default rule will encourage more relevant data about a

---

61 Id., at 51.
62 Id., at 53.
63 Id., at 54.
64 Id., at 54.
65 Id.
66 Id., at 55.
transaction to be revealed because merchants will be forced to share this information as
an initial step before affected parties decide whether to negotiate around the
nondisclosure norm. Moreover, due to the “multifunctional” nature and the need of
third-party access in certain situations, an approach of privacy default rule plus
mandatory exceptions is more appropriate.

Schwartz introduces four requirements for health care information privacy law:
“(1) defined obligations that limit the use of personal health care data; (2) transparent
processing systems; (3) limited procedural and substantive rights; and (4) government
oversight.”

The first requirement aims to create a statutory scheme of defined obligations
under which controls for medical data are tied to and follow data through their different
applications. In the statutory scheme, limitation on freedom of contract, expressed in
mandatory categories, should only be imposed to the extent that a significant social need
exists for access to health care records. The default privacy rule would force health care
providers and insurers, the parties with superior knowledge, to disgorge their knowledge
to the uninformed parties.

The requirement of transparent processing systems addresses the sharing of
information regarding the use of personal medical data. It requires notice of information

---

67 Richard S. Murphy, Property Rights in Personal Information: An Economic Defense of Privacy, 84 Geo
L.J. 2381, 2413-16 (1996)
68 Schwartz, at 56
69 Schwartz, supra note 30, at 58. The most critical mandatory categories should be for (1) payment; (2)
quality control (including physician monitoring); (3) sharing certain information with spouses, life partners,
or next of kin (when such disclosure is consistent with accepted medical practice); (4) public health
reporting; (5) health research; and (6) law enforcement. To the greatest extent possible, these categories
should reflect the same general principles as in the default rule, which, as we shall see, limits the
utilization of health care data to: (1) the minimum amount necessary; (2) based on a need to know; and (3)
for purposes that are compatible with the original collection.
practice being given to all health care consumers. The notice will describes individual’s right to access, copy, correct, monitor her record, and explain the purpose for collection of personal medical data, the procedures under which individual’s rights can be exercised and the extent of legal authorization for disclosure of the collected data.

The requirement of limited procedural and substantive rights reflects the balance between individual and societal interests. Schwartz suggests that procedural interests include: (1) “being informed whether one is required to supply medical information; (2) being granted a mechanism by which one can inspect and correct data and find out which parties have gained access to one's records; and (3) being able to grant or refuse informed consent to proposed uses of medical data that are not mandatory.” As for substantive rights, Schwartz suggests formal documentation of informed consent be required only under when “a use or disclosure is sought that is not mandatory and falls outside the default standard.” He justifies that this approach will “lead individuals to scrutinize closely all consent documents concerning health care information and improve the quality of negotiations in the privacy marketplace.” Also Schwartz suggests three kinds of remedies: civil action with availability of monetary penalties, alternative dispute resolution and criminal penalties.

Although there is lack of hard evidences to show which solution has a better balance between privacy and access to health information, the approach advocated by Schwartz won the favor of legislature and was implemented in HIPAA.

III. HIPAA and Its Privacy Regulation

70 Id, at 63.
71 Id, at 65.
72 Id.
HIPAA and its privacy regulation regulate privacy of health information by addressing three aspects: (1) covered entities that have to comply with HIPAA; (2) protected health information; (3) Individual rights of health information. In essence, HIPAA and its privacy regulation mandate that a “covered entity” may not “use or disclose” an individual’s protected health information, unless otherwise specifically allowed by either HIPAA or by more stringent state law.73

A. Covered Entities: Who Must Comply?

HIPAA and its privacy regulations target three group of entities: health plans, health care clearinghouse and health care provider who transmits any information in electronic form in connection with a HIPAA transaction.74

Health care providers are “a provider of services (as defined in section 1861(u)), a provider of medical or other health services (as defined in section 1861(s)) and any other person furnishing health care services or supplies.”75 Basically, “provider of services” covers organizational providers of health care, such as hospitals, critical access hospitals, skilled nursing facilities, etc.; “providers of medical or other health services” include physicians, nurses, physician assistants, qualified psychologists, clinical social workers, technicians, therapists, etc.; “other health providers”, acting as a catch-all phase, includes dentists and dental labs, pharmacies and pharmacists, employee assistance programs, etc. However health care provider, who does not transmit any health information electronically in connection with a HIPAA transaction by itself or its chose business

73 42 USCA §1320d, 45 CFR §160-164.
74 45 CFR §160.102
75 110 Stat 1936, 2022. Section 1861(u) refers to Medicare Part A; section 1861(2) refers to Medicare Part B.
associate, is not covered. So practitioners who submit claims in “old ways”, like paper or telephone, will not be a “covered health care provider”.

“Health plans” includes group plans of 50 or more participants, health insurance issuers licensed in a state, health maintenance organizations, Medicare, Medicaid and all federal health programs, long-term care and Medicare supplemental policies, any employee welfare benefit plan, and “any other individual or group plans that provides or pays for the cost of medical care.”

“Covered health care clearinghouses” are public or private entity that processes health information to standard data elements.

Besides directly regulating above three groups of entities, HIPAA privacy regulations requires covered entities to require their “business associates” to provide privacy and security protections whenever protected healthcare information is disclosed to them. A “business associate” is one who performs a service for a covered entity, and receives or creates PHI in order to perform that service. HIPAA privacy regulation requires covered entities to include in their contract mandatory clauses that are intended

76 For more information about the transaction standards, visit the HHS Administrative Simplification Web site at http://aspe.hhs.gov/admnsimp/bannertx.htm.
77 45 CFR §160.103
78 “Health care clearinghouse means a public or private entity, including billing services, repricing companies, community health management information systems or community health information systems, and "value-added" networks and switches, that does either of the following functions: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity. 45 C.F.R. §160.103(2002), definition of “health care clearinghouse.”
79 45 CFR §§ 160.103, 164.502(e), 164.504, 164.514(e)
80 Id.
to enhance, by contract, the privacy and security of protected healthcare information under the control the business associate.\textsuperscript{81}

Although some people criticized that covered entities by HIPAA and its privacy regulation are not broad enough\textsuperscript{82}, the coverage of HIPAA and its privacy regulation is almost ubiquitous in health industry. A close look of HIPAA definition of covered entities shows that every existing participant in health care industry that may use information technology to create, maintain and transmit valid and reliable health information is included. Even though there still might be practitioners who do not transmit health information electronically (thus not covered by HIPAA), the number should be small and it is the trend that the number will be zero in the near future as one of HIPAA goals is to replace “paper” with information technology.\textsuperscript{83} Moreover, a new comer to healthcare market will be most likely to fall under the category of “other health providers”, the catch-all category. Therefore HIPAA and its privacy regulation indeed regulate all valid and reliable, thus valuable, primary sources of health information.

\textbf{B. Protected Health Information}

HIPAA defines “protected health information” (PHI) as individually identifiable health information transmitted or maintained in any form.\textsuperscript{84} Individually identifiable health information is:

any information, including demographic information collected from an individual, that-- "(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and "(B) relates to the past, present, or future physical or mental health or condition of an

\textsuperscript{81} 65 Fed. Reg. 82,462, 2504 (Dec. 28, 2000)
\textsuperscript{82} Pew Internet & American Life Project, Institute For Healthcare Research and Policy, Georgetown University, Exposed Online: Why the New Federal Health Privacy Regulation Doesn’t Offer Much Protection to Internet Users 6-8 (Nov. 2001).
http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf
\textsuperscript{83} 42 USCA §1173
\textsuperscript{84} 45 C.F.R. §160.103
individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-- "(i) identifies the individual; or "(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.\(^{85}\)

Typically, health information, as natural result of healthcare activities, is: (1) personal information, including name, date of birth, gender, marital status, and occupation, etc.; (2) financial information, including employer, health insurance identification, and other information to assist billing, etc.; and (3) medical information, including physical examinations, medical history, treatment administered, progress report, physician orders, etc..\(^{86}\) Additionally, information emerging with new biotechnologies, like genetic information, is considered as health information.

Because HIPAA and its privacy regulation regulate only individually identifiable health information, HIPAA does not prohibit use and disclosure of “de-identified” health information. The HIPAA privacy regulation specifies three method of de-identification. First, where the “identifiers” listed in the Privacy Standards are removed from the information, the information is de-identified as long as the covered entity does not have knowledge that the information without identifiers could be used alone or in combination with other information to identify the individual that is subject of the information.\(^{87}\)

---

\(^{85}\) 42 USCA §1171
\(^{86}\) Robert D, Miller, Problems in Health Care Law (7th ed. 1997)

\(^{87}\) “\(i.\) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

A. Names;
B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

   1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
second way to de-identify PHI is to have a person with “appropriate statistical knowledge” determine the risk is “very small” that the information could be used to identify an individual, even though the information contains the identifiers listed in the regulations. Some statistical experts have raised doubt on this method by contending that 87% of the United States population can be identified from birth data, zip code, and gender only. The third way is to code, encrypt or otherwise conceal the identifiers.

C. **Individual Rights of Health Information**

Besides right to access, copy, and correct one’s health care information, HIPAA privacy regulation grants consumer the right of privacy. In HIPAA, consumer’s right to privacy is enforced through a bundle of rights to exclude other from using consumer’s

2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

C. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

D. Telephone numbers;

E. Fax numbers;

F. Electronic mail addresses;

G. Social security numbers;

H. Medical record numbers;

I. Health plan beneficiary numbers;

J. Account numbers;

K. Certificate/license numbers;

L. Vehicle identifiers and serial numbers, including license plate numbers;

M. Device identifiers and serial numbers;

N. Web Universal Resource Locators (URLs);

O. Internet Protocol (IP) address numbers;

P. Biometric identifiers, including finger and voice prints;

Q. Full face photographic images and any comparable images; and

R. Any other unique identifying number, characteristic, or code; and

ii. The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.” 45 C.F.R. §165.514(b).

88 Id.
90 45 C.F.R. §164.502(d)(2).
91 45 C.F.R. §160.101-104
health information. The bundle of rights includes the right to have protected health information secured by covered entities, the right to agree or object uses and disclosure of protected health information, the right to request confidential communications and additional protections for health care information, and right to receive an accounting of disclosures of health care information.\textsuperscript{92}

HIPAA imposes obligations on covered entities to secure protected health information. It requires covered entities to “make reasonable efforts to prevent use and disclosure not permitted by the rule.”\textsuperscript{93} In determining whether a covered entity has provided reasonable safeguards, such as appropriate policies, procedures and training, “the [HHS] will take into account all the circumstances, including the potential effect on patient care and the financial and administrative burden of any safeguards.”\textsuperscript{94}

HIPAA provides two mechanisms for individual to directly control the use and disclosure of protected health information. The first mechanism is “consent.” HIPAA privacy regulations require that a covered health care provider must obtain the individual’s consent prior to being able to use or disclose protected health information for treatment, payment or health care operation purpose, with exceptions for (1) “indirect treatment providers”; (2) inmates as patients, who are not entitled to provide consent while they are inmates; (3) in situations that involve an emergency, a legal mandate to treat, or communication barriers with the individual.\textsuperscript{95} Under the last situation the provider must attempt to obtain the consent and must document the attempt and the reasons that it fails. Once receiving consent, a health care provider has almost no limit on

\textsuperscript{92} 45 CFR §164
\textsuperscript{93} Id.
\textsuperscript{94} Guidance on Standard for Privacy of Individually Identifiable Health Information, available at http://www.aspe.hhs.gov/admnsimp/final /pvcguide1.htm
\textsuperscript{95} 45 CFR § 164.506
use of PHI for its own treatment-related use and disclosure. A health care provider may condition its rendering treatment on an individual’s consent on use and disclosure of PHI. Consents are effective forever, unless revoked in writing. Health plan and health care clearing houses are not required to obtain consent.

The second mechanism is “authorization.” Authorization is required for the use or disclosure of protected healthcare information for any purpose other than treatment, payment or health care operations (as opposed to individual’s consent). Like the HIPAA consent, an authorization may be revoked, but unlike the consent, a covered health care provider may not condition treatment upon an individual’s signing of an authorization, except for research related treatment. To obtain authorization, a covered entity must warn individual that information used or disclosed pursuant to the authorization may be no longer protected by the HIPAA rules and may be redisclosed by the recipient. It must describe each purpose of the requested use or disclosures. HIPAA provides particular protection for “psychotherapy notes”, for which authorization must be obtained with only a few exceptions. Absence of any required element, or the improper combination of an authorization with another document, will invalidate the authorization.

HIPAA also considers circumstances where uses and disclosures may be made without consent, authorization or opportunity to agree or object. These uses and disclosures include: (1) for public health activities (include child abuse/neglect reporting and FDA monitoring); (2) about victims of abuse, neglect or domestic violence; (3) for health oversight activities; for judicial and administrative proceedings; (4) from law

96 Id.
97 Id.
98 Id.
99 Id.
100 Id.
enforcement purpose; (5) about decedents; (6) for cadaveric organ, eye or tissue
donations; (7) for research (unrelated to treatment); (8) to avert serious threats to health
or safety; (9) for specialized government functions; and (10) for compliance with
workers’ compensation and other similar laws. Most of these provisions impose
significant procedural requirements that must be followed before the use or disclosure
may be made.

To further protect privacy of health care information, HIPAA privacy regulation
imposes a “minimum necessary” requirement that sets limit on scope and amount of
protected healthcare information being used or disclosed. For use internal to a covered
entity, the entity must decide who need access to protected healthcare information to
perform their duties, how much protected healthcare information is needed for their
duties and what conditions are appropriate for them to use protected healthcare
information. The covered entity must then make reasonable efforts to limit access
accordingly. As to disclosures of protected healthcare information to parties outside legal
boundaries of a covered entity, the covered entity must only disclose the amount of
protected healthcare information “reasonably necessary” for the purpose for which the
disclosure is sought. However the “minimum necessary” disclosure rules do not apply to
treatment-related disclosures. A covered entity may rely on the reasonable
representations of public officials, other covered entities, professional workforce
members or business associates and researchers to determine how much protected
healthcare information is the minimally necessary for disclosures to them.

101 45 CFR §164.512
102 45 CFR §164.502(b), 164.514(d)
In sum, HIPAA privacy regulations create privacy right of personal healthcare information by giving individuals absolute control over their health information, setting boundaries on the use and disclosure of health information, and mandating covered entities to establish reasonable safeguards for healthcare information. In fact, HIPAA defines the privacy right in its finest granular form: the privacy right is enforced not only at individual level, but also for every chunk of personal healthcare information that is needed in any possible usage. As discussed below, HIPAA creates anticommons of healthcare information.

IV AntiCommons of Healthcare Information

A. Tragedy of the Anticommons

The term “tragedy of the anticommons” was first coined by Frank Michelman and popularized in 1998 by Michael Heller. Heller defines an “anticommons property as a property regime in which multiple owners are each endowed with the right to exclude others from a scarce resource, and no one has an effective privilege of use.”\footnote{Michael A. Heller, The Tragedy of the anticommons: property in the transition from Marx to Markets, 111 Harv. L. Rev. 621, 622 (1998).} It is contrasted with a commons property to which “multiple owners are each endowed with the privilege to use . . . and no one has the right to exclude another.”\footnote{Id.} In a tragedy of the commons, “rational individuals, acting separately, may collectively overconsume scarce resources.”\footnote{Id. at 677.} In contrast, in a tragedy of the anticommons, “rational individuals, acting separately, may collectively waste the resource by underconsuming it compared with a social optimum.”\footnote{Id.}
In his paper, Heller points out that “anticommons property may occur at the level of a particular use of a scarce resource, rather than at the level of an entire property regime.”  He demonstrates this with the example of Moscow komunalkas. Komunalkas were large prerevolutionary apartments, which, at some points in Soviet history, might have shared by several dozen people with each family assigned one room. During privatization, tenants received some ownership rights in their room and, indirectly, the right to block others from using the whole apartment as a single-family or office space. In other words, each owner could keep any other owner from renting out the entire apartment in its most valuable market use. To illustrate in number, in the case of some old, centrally located komunalkas in Moscow, the market value of the entire apartment might approach $500,000. Assume such a komunalka had four tenants, each occupying one room. Because of the discomforts and irritations of communal living, each of four communal rooms might have had a market value of only $25,000 if the rooms were kept in anticommons use, so that the whole apartment would have an anticommons value of $100,000. Converting the komunalka from anticommons to private property creates a $400,000 gain.

Heller asserts that “once anticommons property appears, neither markets nor subsequent regulation will reliably convert it into useful private property, even if the property rights are ‘clearly defined’ and contracts are subject to the ‘rule of law.’ Transaction costs, holdouts, and rent-seeking may prevent economically justified conversion from taking place.” Although anticommons tragedy may be overcome through development of informal social norm, its application is limited, if not impossible.

107 Id., at 669.
108 Id., at 650.
109 Id., at 687.
in most of situations.\textsuperscript{110} Heller suggests that “governments must take care to avoid creating anticommons property accidentally when they define new property rights. One path to well-functioning private property is to convey a core bundle of rights to a single owner, rather than rights of exclusion to multiple owners.”\textsuperscript{111}

Anticommons shows it face not only in real estate business in former communist countries, but in high-tech industries in this country. During the genetic gold rush, researchers and organizations seek many patents on biological discoveries. Consequently, to develop new treatments or processes, people will have to use many patented procedures in order to create a marketable product. However, because negotiating a licensing agreement with the patent holders is prohibitively expensive, those patents form an anticommons property that leads to underuse of existing technologies.

B. \textit{Anticommons of Healthcare Information under HIPAA}

\textit{“Our economy is not simply supplied by information, it is fueled by information.”}\textsuperscript{112}

It is a well-known fact that healthcare information is “multi-functional”.\textsuperscript{113} Besides its original function for the purpose of treating individual patients, healthcare information plays a critical role in medical research, pharmaceutical development, insurance premium setting, and public policy-making. For example, the Medical Information Bureau (MIB) has long collected personal healthcare information and provided them to insurance industry for the purpose of risk assessment and fraud detection. But unlike its primary clinical function, other functions of healthcare information have little value when used in isolation. The functions of healthcare

\textsuperscript{110} Id, at 678.
\textsuperscript{111} Id, at 688.
\textsuperscript{113} Schwartz, at 15.
information, other than the clinical one, can be meaningful only when personal healthcare information is collected into a large-scale pool through which comparison and analysis can be conducted. In other words, the value of healthcare information can only be materialized at the level of “collective use.”

However, under HIPAA privacy regulations, the “collective use of healthcare information” becomes very difficult as HIPAA creates an anticommons form of healthcare information at “collective level”.

Under HIPAA privacy regulation, individual is granted a strict right to exclude other from using her healthcare information. The right to exclude is primarily enforced thought the requirement that no use or disclosure of healthcare information is allowed without individual’s consent or authorization. Additionally, the right to exclude is further strengthened by the right to revoke authorization, the right to request confidential communications and additional protections for health care information, the right to monitor use and disclosure of healthcare information, the “minimum necessary” requirement and covered entities’ obligation to secure protected health information.

As a result, HIPAA privacy regulation creates an anticommons form of healthcare information at “collective level”. To illustrate, let’s assume healthcare information of all patients with disease X is legitimately desired. To compile the specific information, authorization of every patient with disease X must be obtained under HIPAA. If some patients decide not to give authorization, information collected will be incomplete and therefore useless. Thus patients not giving authorization effectively exclude other from a valuable scarce resource, the complete healthcare information of all patients with disease X. As shown in above example, HIPAA privacy regulation causes an anticommons
property regime in which “multiple owners are each endowed with the right to exclude others from a scarce resource, and no one has an effective privilege of use.”\(^{114}\)

As Heller warns, with anticommons property, “rational individuals, acting separately, may collectively waste the resource by underconsuming it compared with a social optimum.”\(^{115}\) The tragedy of anticommons of healthcare information is more than possible.

First, under current market conditions, consumers are likely to underconsume and thus collectively waste their healthcare information. Because of lack of professional knowledge and the complexity of healthcare market,\(^{116}\) consumers may neither fully understand the value of their health information nor know how to make an effective use of their health information. Moreover, current market does not provide to them effective ways to use their health information. Although it is expected that, as consumers learn more about their health care information and their values, they will start making effective use of their health care information, at least now the chance is slim because consumer education is not the top priority of major market participants, like health providers and insurance companies. So consumer most likely will just sit on their healthcare information and do nothing with them.

Second, the right of exclusion as defined in HIPAA privacy regulation raises prohibitive barrier for interested parties to explore an optimal use of health care information. Under current HIPAA privacy regulation, transaction costs of negotiating agreement with individual are very high. The high costs are partly due to the huge

\(^{114}\) Heller, at 622.
\(^{115}\) Id.
\(^{116}\) Schwartz, at 44 footnote 275.
number of parties involved and partly because of the scope of allowed usages and the amount of health care information permitted in a usage. HIPAA privacy regulation not only requires authorization for every disclosure where information goes outside the boundaries of covered entities, but also allows only “reasonably necessary” amount of protected healthcare information. These requirements put extraordinary burden on the party who want make efficient use of health care information.

Assume a hypothetical organization is established to seek efficient use of health care information on behalf of individuals. The organization can obtain required information either directly from individual or from those covered entities. In both ways the organization will face huge transaction costs and uncertainty. To collect information directly from individuals, the organization has to bear the cost of search and negotiation, which, due to the large number of parties involved, may be high enough to dissuade the organization. To collect information from intermediate covered entities, the organization will rely on not only successful negotiations with targeted entities (which again means large transaction cost), but also success of targeted entities to obtain authorization from individual from required information (which means uncertainty). The uncertainty of gaining access to required information is magnified as the “minimum necessary” requirement and individual’s right to revoke authorization. The “minimum requirement” imposes a burden on the organization to persuade many parties to agree on how much information is “minimum necessary.” The right to revoke authorization at any time subjects utility of health care information to the threat of individual holdout.

To make it worse, the hypothetical organization itself may be subject to HIPAA privacy regulation because it may be deemed as a health care provider “furnishing health
care services or supplies”. In operation, when the organization comes up with an application that asks for disclosure of some protected healthcare information, as required by HIPAA privacy rule, the organization has to contact each affected individual for authorization. Next time when it works on another application that needs disclosure of protected healthcare information that are different from those for previous application, the organization has to reach out again for individual’s authorization. The inefficiency is obvious.

Although, as argued by Schwartz, it is anticipated that transaction cost will reduced with help of information technology, it is arguable that the transaction cost may remain high because HIPAA privacy regulation discourages businesses from investing in development of necessary technologies. A rational business can hardly ignore the business uncertainty rising out of the anticommons form of healthcare information under HIPAA privacy regulation, and therefore is likely to take a wait-and-see strategy before putting effort to develop necessary technology. This concern is somehow corroborated by the fact that after three years of HIPAA privacy regulation information technology has contributed much poorly to reduce transaction cost in healthcare industry than it has done in other sectors of economy.

In the end, HIPAA privacy regulation creates a deadlock situation in which on one hand owners of healthcare information cannot use their healthcare information effectively and on the other hand parties who can make an optimal use of healthcare information are not allowed to do so. A tragedy of anticommons in healthcare information is becoming real as rational owners of healthcare information, acting
separately, are collectively wasting a scarce resource by under-using it compared with a social optimum.

C. The Use and Disclosure of Health Information for Research under HIPAA

“Americans support both protecting the privacy of medical records and encouraging medical research.”\(^{117}\)

The anticommons property of healthcare information raises an obstacle to research use of healthcare information. Although, in designing HIPAA privacy regulation, HHS intended to “achieve the appropriate balance between protecting individuals' privacy interests, while permitting researchers to access protected health information for important, and potentially life-saving, studies,”\(^{118}\) some legal scholars argues that HIPAA privacy regulation “will discourage entities from making medical records available for research and will diminish the pace and volume of research.”\(^{119}\)

Besides patients’ authorization, HIPAA privacy regulation provides two additional solutions to research use and disclosure of protected health information: (1) “de-identifying” healthcare information; (2) four exceptions where the use and disclosure of protected healthcare information are allowed without patients’ authorization.

It is lawful to use and disclose “de-identified” healthcare information under HIPAA privacy regulation. Because HIPAA privacy regulation protects only individually identifiable health information\(^{120}\), healthcare information that has been sufficiently de-


\(^{118}\) 67 Fed. Reg. at 53,131


\(^{120}\) 45 C.F.R. §164.501. Individually identifiable health information is information that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
identified is not subject to restriction of HIPAA. However the practice of “deidentifying” protected healthcare information can be very expensive. For example, some medical records are scanned and stored in database as images. To hide identifiers in an image is a very complicated and expensive process. More important, even though “deidentified” healthcare information can be used in some research, it is useless for many other types of research, such as “epidemiologic research, health service research and other population-based research that require identification of each subject’s geographic information, as well as certain dates and ages.”

To provide convenient research use of protected healthcare information, HIPAA privacy regulation carves out four exceptions: (1) using and disclosing a limited data set pursuant to a data use agreement; (2) reviews preparatory to research; (3) research on

---

121 See footnotes 87, 88 and 90.
122 Jennifer Kulynych & David Korn, The Effect of the New Federal Medical-Privacy Rule on Research, 346 New Eng. J. Med. 201 (Jan. 17, 2002). The authors points out the use of de-identifies healthcare information in research known as retrospective archival, or non-interventional research.
124 45 C.F.R. §164.514(e). Allowing a covered entity to use or disclose a limited data set, if the covered entity enters into a data use agreement with the limited data set recipient only for the purposes of research, public health, or health care operations.

A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

A data use agreement between the covered entity and the limited data set recipient must: (A) Establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with paragraph (e)(3) of this section. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity; (B) Establish who is permitted to use or receive the limited data set; and (C) Provide that the limited data set recipient will: (1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law; (2) Use appropriate safeguards to
decendent’s information; and (4) IRB or privacy board approval of a waiver of or alteration to patient authorization.\textsuperscript{125} However these exceptions are under criticizing too. Although the limited data set approach appears to be a compromise between the de-identification and the authorization requirement, it still bears high transaction costs and may unreasonably limit the scope of healthcare information for research. The reviews preparatory to research only provide a narrow solution for a researcher “who is an employee or a member of the covered entity’s workforce to use protected health information to contact prospective research subjects while on the physical premises of the covered entity.”\textsuperscript{126} The “research on decedent’s information” exception raises the concern on unwanted exposure of living relative’s health information, particularly genetic and

\textsuperscript{125} 45 C.F.R. §164.512(i). Allowing a covered entity to use or disclose protected health information for research, regardless of the source of funding of the research, provided that:

(i) Board approval of a waiver of authorization. The covered entity obtains documentation that an alteration to or waiver, in whole or in part, of the individual authorization required by § 164.508 for use or disclosure of protected health information has been approved by either: (A) An Institutional Review Board (IRB), established in accordance with 7 CFR lc.107, 10 CFR 745.107, 14 CFR 1230.107, 15 CFR 27.107, 16 CFR 1028.107, 21 CFR 56.107, 22 CFR 225.107, 24 CFR 60.107, 28 CFR 46.107, 32 CFR 219.107, 34 CFR 97.107, 38 CFR 16.107, 40 CFR 26.107, 45 CFR 46.107, 45 CFR 690.107, or 49 CFR 11.107; or (B) A privacy board that: (1) Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests; (2) Includes at least one member who is not affiliated with the covered entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities; and (3) Does not have any member participating in a review of any project in which the member has a conflict of interest.

(ii) Reviews preparatory to research. The covered entity obtains from the researcher representations that: (A) Use or disclosure is sought solely to review protected health information as necessary to prepare a research protocol or for similar purposes preparatory to research; (B) No protected health information is to be removed from the covered entity by the researcher in the course of the review; and (C) The protected health information for which use or access is sought is necessary for the research purposes.

(iii) Research on decedent's information. The covered entity obtains from the researcher: (A) Representation that the use or disclosure sought is solely for research on the protected health information of decedents; (B) Documentation, at the request of the covered entity, of the death of such individuals; and (C) Representation that the protected health information for which use or disclosure is sought is necessary for the research purposes.

\textsuperscript{126} Tovino, at 498.
other hereditary information. Finally, IRB or privacy board may not be a good solution because “IRBs are asked to review too much, too quickly, with too little expertise and not enough training, and that IRBs face conflicts that threaten their independence.”

As a result, as one commentator observes, HIPAA’s Privacy Rule’s research provisions “establish onerous administrative requirements the burden of which may outweigh any autonomy that could be realized by the research subjects.”

V. Conclusion

As information technology brings great efficiency and productivity to healthcare industry and generates huge volume of valuable information, it also raises serious concerns on privacy of healthcare information. Since Warren and Brandeis published “the Right to Privacy”, information privacy has been perceived by public and treated by the courts as a constitutional right. But some legal scholars argue that privacy, as intermediate goods, matters to the extent that it serves to increase wealth and social utility. So they argue that privacy of healthcare information should not be protected because doing so creates information asymmetries, raises transaction cost and distorts market behavior. Other legal scholars disagree. They argue that market has failed to make proper use of healthcare information and economic analysis of healthcare information by the other side was flawed. Instead of allowing open access to healthcare information, they propose a legal frame that grants and enforces individual’s privacy right of healthcare information.

In 1996, Congress passed HIPAA, and later on August 14, 2003 Department of Health and Human Services finalized HIPAA privacy regulations. HIPAA privacy

\[127\] Id, at 496.
\[128\] Id, at 490-5.
\[129\] Id, at 502.
regulation creates privacy right of personal healthcare information by giving individuals absolute control over their health information, setting boundaries on the use and disclosure of health information, and mandating covered entities to establish reasonable safeguards for healthcare information. In fact, HIPAA defines the privacy right in its finest granular form: the privacy right is enforced not only at individual level, but also for every chunk of personal healthcare information that is needed in any possible usage.

Unfortunately, HIPAA privacy regulation creates anticommons property of healthcare information. As a result, HIPAA privacy regulation causes a deadlock situation in which on one hand owners of healthcare information cannot use their healthcare information effectively and on the other hand parties who can make an optimal use of healthcare information are not allowed to do so. A tragedy of anticommons in healthcare information is becoming real as rational owners of healthcare information, acting separately, are collectively wasting a scarce resource by under-using it compared with a social optimum.

HIPAA privacy regulation makes research use of healthcare information difficult. Although theoretically HIPAA privacy regulation provides particular means for research use of healthcare information, in reality HIPAA privacy regulation results in onerous burdens to researchers and effectively discourages them from making use of available healthcare information.

Although HIPAA privacy regulation is purposefully designed to benefit public, one might reasonably doubt whether HIPAA privacy regulation is the best way to achieve that end. A comment of a legal scholar might accurately reflect this concern:

I believe the new regulations are excessively and unnecessarily complex and often more attuned to making sure that business and government
agencies get access to medical records than to the protection of patients' privacy. . . . The implementation of the new HIPAA privacy regulations is likely to be costly, inconsistent, and frustrating to both physicians and patients.\textsuperscript{130}