Yale ISPS

Institution for Social and Policy Studies

ADVANCING RESEARCH • SHAPING POLICY • DEVELOPING LEADERS

HOW SHOULD HEALTH DATA BE USED?

PRIVACY, SECONDARY USE, AND BIG DATA SALES

ISPS-BIOETHICS WORKING PAPER

ISPS14-025

[7 OCTOBER 2014]

BONNIE KAPLAN, PHD, FACMI

CENTER FOR MEDICAL INFORMATICS

INTERDISCIPLINARY BIOETHICS CENTER

INFORMATION SOCIETY PROJECT

HOW SHOULD HEALTH DATA BE USED? Privacy, Secondary Use, and Big Data Sales[1]

Bonnie Kaplan, PhD, FACMI, Yale Center for Medical Informatics, Yale Interdisciplinary Bioethics Center, Yale Information Society Project, Yale University, New Haven, CT

Corresponding Author:
Bonnie Kaplan, PhD, FACMI
Yale University
238 Prospect Street
Box 208293
New Haven, CT 06511
203-436-9085
bonnie.kaplan@yale.edu

KEYWORDS:
Confidentiality
Health Data Privacy
Ethics
Health Records
Secondary Use
Big Data
Data Mining
Pharmaceutical Marketing
Health Data Sale
De-Identification
HIPAA
EU Data Protection Directive
Sorrell v. IMS Health, Inc.
R v. Department of Health, Ex Parte Source Informatics Ltd.

Running Title: How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales

[1] **Acknowledgements:**

I am grateful for the thoughtful contributions to the panel I organized on the *Sorrell* case for the 2011 American Medical Informatics Association Annual Symposium and comments on a very early draft of some portions of this paper by Paul DeMuro, JD, CPA, MBA, MBI, Oregon Health and Science University, Portland, OR; Kenneth W Goodman, PhD, FACMI, University of Miami, Miami, FL; and Carolyn Petersen, MS, MBI, Mayo Clinic, Rochester, MN. I also am grateful to Joel Winston for sharing drafts of his reporting with me, and to the editor for helpful suggestions.

Abstract

Electronic health records, data sharing, big data, data mining, and secondary use are enabling exciting opportunities for improving health and health care while also exacerbating privacy concerns. Two court cases about selling prescription data raise questions of what constitutes "privacy" and "public interest;" they present opportunity for ethical analysis of data privacy, commodifying data for sale and ownership, combining public and private data, data for research, and transparency and consent. These interwoven issues involve discussion of big data benefits and harms, and touch on common dualities of the individual v. the aggregate or the public interest, research (or, more broadly, innovation) v. privacy, individual v. institutional power, identification v. identity and authentication, and virtual v. real individuals and contextualized information. Transparency and accountability are needed for assessing appropriate, judicious, and ethical data use and users, as some are more compatible with societal norms and values than others.

Introduction

Electronic health records, data sharing, big data, and secondary use of health data enable exciting opportunities for improving health and health care. They also contribute to new concerns over privacy, confidentiality, and data protection. Two court cases, one in the United Kingdom and one in the United States, provide opportunities for thinking through ethical issues related to these developments. Each case involved selling data for marketing prescription drugs, and in each case, the court decided in favor of selling the data. However, the cases were decided on different grounds, raising more general issues

of secondary use of health data and the growth of health-related databases, data sharing, data aggregation, and biometric identification.

Significant health data protection, policy, and ethical considerations are inherent in these cases. The cases call into question just what constitutes "privacy" and "public interest," and considerations for balancing them. They provide an opportunity to weigh privacy and numerous beneficial uses for data: for individual patient care; for public health, research, biosurveillance, and marketing. The cases prompt ethical questions of commodifying medical information and of harmonizing policy across jurisdictional boundaries. They raise concerns of how health data can, and should, be used. Their consequences may affect biomedical informatics, patient and provider privacy, and regulation in ways this paper explores, both in the US and elsewhere.

How health data can, and should, be used is at the intersection public health, research, care, privacy, and ethics. This paper provides an ethical analysis of these interwoven ethical issues involving appropriate, judicious, and ethical secondary data use, reflecting more general discussion of big data benefits and harms, and touching on common dualities of the individual v. the aggregate or the public interest, research (or, more broadly, outside the health field, innovation) v. privacy, individual v. institutional power, identification v. identity, identification v. authentication, and virtual v. real individuals and contextualized information.[1]

I start by discussing what makes health data special, including international consensus on the importance of the clinician's duty of confidentiality and on health data privacy or protection. Next I summarize the court cases. Then I consider who benefits from data disclosure and aggregation, and secondary use for data mining, research, and

sale. Throughout, I highlight potential benefits and harms and argue that transparency and accountability is needed. Ethical and policy analysis should assess data uses and users, as some are more compatible with societal norms and values than others.

Considering how health data should be used in light of these issues suggests policy opportunities concerning patient data and privacy protection. As the use of electronic health records, electronic medical devices, mobile and e-health applications, and biometric, social and behavioral, and genomic data spreads, these considerations are becoming more relevant worldwide.

What's Special about Health Data? – International Principles

All countries recognize confidentiality as a patient's right.[2] Intimacies are revealed in the interest of good health care, so clinicians' professional and fiduciary duties include a duty of confidentiality. Yet, even if individual clinicians scrupulously meet this professional obligation, confidentiality is threatened by legal requirements to collect and document personal health information, especially when maintained in computer data bases that can be combined easily with other information about the person.[3] What patients reveal for the purpose of health care may then be used in ways they never intended. Even though privacy practices have not caught up to these trends, internationally, health information is given special protection, though specific ways of achieving it differ. Lifestyle choices, reproductive abilities, and stigmatizing conditions are considered highly sensitive. Yet, what is included in these categories differs with cultural background, from place to place, and time to time. Countries vary in what personal information is treated as needing restricted collection, use, and disclosure.[4] [5] They also balance privacy and other considerations differently, so that privacy protection

is more lax in some places than in others. In India, for example, the judiciary considers privacy on a case-by-case basis, as an exception to the rule that permits government interference in private life. Unlike in Europe and the United States, public interest, welfare, and safety take precedence over individual rights, liberty, and autonomy.[6]

Fair Information Practices and De-Identification

The same Fair Information Practices (FIPs) underpin privacy policies in both the European Union and the United States. The EU and the US each protect personal data, including data concerning health, albeit differently. The US approaches privacy by sector; separate laws address confidentiality in distinct domains, such as finance and health care. Health data privacy collected in the course of clinical care is governed by The US Health Insurance Portability and Accountability Act (HIPAA) of 1996, extended by a Privacy Rule in 2001 and again by changes mandated by the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act (part of the American Recovery and Reinvestment Act of 2009 (ARRA)) and the Genetic Information Non-Discrimination Act (GINA) of 2008.[7] [8] [9] The European Union takes a more comprehensive general approach to privacy, reflected in the 1995 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[10] [11] Nevertheless, both the US and the EU construe privacy as control and protection of data rather than other conceptions of privacy.[12]

Both the US and the EU make special note of health information, and both rely on stripping data of content presumed to identify the individual represented by the data. As Paul Ohm points out:

> In addition to HIPAA and the EU Data Protection Directive, almost every single privacy statute and regulation ever written in the U.S. [sic] and the EU embraces —implicitly or explicitly, pervasively or only incidentally—the assumption that anonymization protects privacy, most often by extending safe harbors from penalty to those who anonymize their data.[13]

As these safe harbors provide, neither HIPAA nor the EU Data Protection Directive apply after data is de-identified. However, relying on de-identification contributes to what has been considered an inadequate problematic legal framework for data protection.[14] Addressing concerns over de-identification "would require a significant shift in approach towards data-protection across Europe."[15] Similar deficiencies plague the US.[16] [17]

Privacy protection, then, depends not merely on de-identification but on expectations, transparency, and how data is used. De-identification, or anonymization, presumes that it is possible to identify and enumerate the kinds of data that might contribute to privacy risks and to specify how to prevent harms,[18] that such a list is static and sufficient in all contexts,[19] and that there are no privacy harms if the individual is not identified, even though individuals may object to uses of their personal data even if they themselves are anonymous.[20] Further HIPAA permits secondary uses of data for research, public health, law enforcement, judicial proceedings, and other "public interest and benefit activities," without individual authorization, thereby assuming that "public interest" is clearly understood.[21] [22] All are questionable assumptions.

Duty of Confidentialty

Health data privacy relates not only to expectations about privacy in general, but also to norms involving professional practice, privilege, autonomy, paternalism, and

protected communication and duty of confidentiality, as well as to requirements for data collection, dissemination, and retention.

Physicians and nurses have duties both to their individual patients and to the health of their communities.[23] At least since the time of the Hippocratic Oath, societal norms and common law have recognized that clinicians' duty to patients includes maintaining confidentiality, except where protecting the public interest or other individuals may override it. The World Medical Association's International Code of Ethics makes respecting the right to confidentiality a duty integral to a physicians' responsibility to patients.[24] The WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects (revised 2013) places a duty on physicians

> to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects…even though they have given consent.[25]

Recognizing that this personal information, whether collected for research or clinical practice, increasingly is held in databases, in 2002, the WMA adopted a Declaration on Ethical Considerations Regarding Health Databases:

> Confidentiality is at the heart of medical practice and is essential for maintaining trust and integrity in the patient-physician relationship. Knowing that their privacy will be respected gives patients the freedom to share sensitive personal information with their physician.[26]

The WMA reaffirms that violating this duty could "inhibit patients from confiding information for their own health care needs, exploit their vulnerability or inappropriately borrow on the trust that patients invest in their physicians" while at the same time recogniz-

ing the value of secondary health data use for quality assurance, risk management, retrospective study.[27]

Thus, a key reason for treating health data as requiring special protection is to maintain trust between clinician and patient in the interest of both social and public order as well as better care for each individual patient. In recognition of this ethical duty, confidentiality is seen worldwide as a health professional's legal duty that protects the professional from giving legal testimony, thereby serving the interests of patient and public by maintaining trust during medical encounters. Nowhere can this private data rightly be passed to a third party without the patient's permission. French criminal law makes this universal spirit apparent by criminalizing physician's breach of confidentiality even in court testimony, even if the patient would allow it.[28]

How people value and respond to concerns about health data privacy is affected by context and common expectations of privacy.[29] Many recognize that clinicians need highly personal information in order to care for them and, because of the long-standing history of trust in professional confidentiality, patients willingly share sensitive information with those who treat them. As Deryck Beyleveld and Elise Histed eloquently point out:

> Information that patients provide for their treatment is about very personal and sensitive areas of their lives. Indeed, it relates to their very existence, both physically and symbolically. As such, it is not information that they may be presumed to be prepared to disclose or have used freely. It is their vulnerability, constituted by pain and distress, or fears about their health and lives, that leads them to disclose this information to health professionals. At the same time, people are apt to attach great

> importance to intimate information about themselves and their bodies, and this can be associated with mystical and religious beliefs, which by their very nature can be idiosyncratic.[30]

Patient Benefits and Harms

For other reasons, individuals also may freely provide health information via health-related social networking and web postings and searches, or because it is required legally, as for prescriptions. Such information could be consolidated and linked with other data for beneficial or nefarious purposes, sometimes without individuals' knowledge. Patients benefit from having their record information available from previous clinical visits, whether or not with the same clinician or in the same facility. Clinicians can make better care decisions in light of fuller understanding of their patients' past clinical histories. Patients also benefit from public health surveillance and research that depends on combining health information from individual patients to improve public health and develop better treatments. Patients may benefit from making identifiable information concerning adverse drug events available to pharmaceutical companies so that those companies can follow up with patients and improve drug safety, as Source Infomatics argued in the UK court case discussed below, and the International Pharmaceutical Privacy Consortium argues more generally.[31] [32] Data aggregator IMS Health Canada (IMS Health, Inc. was a plantiff in one of the court cases) unsurprisingly takes the position that analyzing doctors' prescribing habits contributes to patients becoming informed consumers.[33]

Yet patients can be harmed when data about them is used to violate privacy: to deny employment, credit, housing, or insurance; and for identity theft and other unsavory

purposes. Some fear that patients who are insecure about prescription or other health record information confidentiality may withhold information, refuse diagnostic and genetic testing, or decline electronic prescriptions.[34] [35] [36] People change their behavior and withhold information in order to protect their health information privacy.[37] Even before the widespread use of electronic health records, a 2000 Gallup Poll indicated that the vast majority of people in the US opposed third-party access to medical data without a patient's permission, including 67% opposing release of data to medical researchers.[38] Similarly, the Pew Internet and American Life Project reported that, to protect privacy, nearly one in six patients withheld information, provided inaccurate information, doctor-hopped, paid out of pocket instead of using insurance, or even avoided care. Over 80% feared that seeking health information on the internet would result in changes in insurance coverage or otherwise reveal their information.[39]

Transparency and Consent

As information resources become more ubiquitous and information sharing becomes more profitable, more thought is needed concerning which data uses are acceptable and what control individuals should have over data about themselves. Privacy violations may compromise patient care, the information in patients' records, and patient-clinician relationships. The principles of data protection-- transparency, legitimacy, and proportionality--embodied in the EU Data Protection Directive, therefore, specify that the person from whom data is obtained should be informed of what will be done with it and to whom it will be disclosed. This allows the individual to consent or object and to withdraw or correct the data. Also, according to the Directive, the data should be kept

only as long as necessary for the specified purpose,[40] even though that could compromise later retrospective research.

Patients' privacy concerns are exacerbated when patients, and even clinicians, have little idea of what becomes of their data, or just what is protected and what is not.[41] Withholding information from one's clinician is neither in the public interest nor beneficial to that patient's interest in proper health care. Yet, removing identifying information from patient records may not alleviate concerns, especially in light of increasing public awareness of privacy violations surrounding big data and the ease with which data sets that were meant to be kept apart now are combined and used for re-identification.[42] [43] [44] [45] [46] Further, without transparency, consent is meaningless.

Two Court Cases

Two court cases provide occasion for thinking about ethical implications of data sale and secondary use in light of international principles of health data privacy and protection. Each case involves selling prescription data for pharmaceutical marketing. In both the United States and the United Kingdom, data aggregators successfully challenged restrictions on such data use and sale.

The 2011 US Supreme Court case, *Sorrell v. IMS Health Inc.*, *et al.*,[47] was decided on free speech grounds. Although the legalities involve unique features of US constitutional law, a similar case in the UK in 2000, *R v. Department of Health, Ex Parte Source Informatics Ltd.*,[48] points to the international nature of the ethical issues. That case was decided on the grounds that selling anonymized (de-identified) data did not violate pharmacists' duty of confidentiality.

The decision in each case runs counter to public expectations of health data confidentiality. The public is hardly aware that aggregating and selling prescription and other health data is an international enterprise. Thus, the *Sorrell* and *Source* cases raise more general global concerns of privacy and data protection, on the one hand, and appropriate use and secondary use of data for data mining, marketing, research, public health, and health care, on the other. Elsewhere I address data de-identification, prescription and other health data aggregation and sale, as well as issues more specific to these two cases.[49] This paper explores other ethical issues related to the cases—benefits and harms of data sale; trade-offs between privacy, individual health and public health; and the need for transparency—so ethical dimensions of responsible and ethical health data collection and use can be assessed.

Who Benefits?

Clinical data includes data that patients are required to provide to receive care. In both the *Sorrell* and *Source* cases, prescription data was aggregated and sold. Patients, prescribers, and pharmacies are required by law to collect information related to prescribing. Data aggregators perform valuable service in collecting, cleaning, and combining this and other data into useful resources, though the value does not accrue directly to those who are the original source of the data. Data aggregators should be compensated for the value added, but the sources deserve some benefit as well. Currently, they primarily bear costs, both financially and in privacy.

The combination of required disclosure of personal data, together with how easily data can be collected and disseminated, is not unique to pharmacies. It is a cost of health care to collect and store patient records, a cost passed on to patients and payers, whether

private or governmental. The organizations providing this data obtain it from those legally required to provide it, from individuals who pay, directly or indirectly through their private or public insurers, for its collection and maintenance. These individuals gain little direct benefit from aggregating and selling data about them, and they may be harmed by it. It mostly occurs without their knowledge or permission. Even in light of arguments that patients should be required as a condition of treatment to allow data about them to be used for research—a requirement counter to professional norms to provide care—it seems improper to require either patients or clinicians to disclose data they would otherwise choose to keep private so that others may financially profit from it, whether or not it is de-identified.

Secondary use and big data analytics also are affected by costs of collecting, storing, and organizing data, as well as by the costs of meeting regulatory requirements. To reduce costs, sensitive health data processing is outsourced from countries with stronger privacy protections to countries with weaker ones, despite consequent privacy risks.[50] Also to reduce costs, US marketing organizations oppose opt-in consenting on the grounds that it would increase the cost of doing business.[51] Costs must be paid somehow. Both the *Source* and *Sorrell* cases were fought to protect the commercial value of health information. One way of recovering costs is by selling this data. Though some sources provide some data sets at little or no cost to researchers, cost could make it easier for pharmaceutical companies and other commercial enterprises than for researchers to access data.[52] [53] The trend towards treating data as private property could make it more difficult to develop comprehensive databases crucial for public health and research.[54]

Research, trade, innovation, as well as the globalized healthcare industry, provide considerable public benefit. There are ethical as well as economic costs to privileging privacy, yet economic value should not simply be assumed more important than privacy. Law and common ethical practice prevent releasing medical information without a patient's permission, but US law does not prevent selling or transferring rights to records.[55] What data can be sold, can be sold and replicated anywhere, and once sold, may be used for good or ill. Tracing the chain of data sales and use is difficult, making transparency and consent nearly impossible the further data is transferred from the original source.

Health Data Uses: Big Data, Data Mining, Research, and Biosurveillance

Electronic health records and health information networks provide a wealth of data for public health, outcome improvements, and research. Data could be used for a range of beneficial purposes, from outcomes and comparative effectiveness research to designing clinical trials and monitoring drug safety. The benefits of this data for public health, marketing, research, drug development, identifying adverse effects, and biosurveillance; for reducing costs and over-prescribing; and for regulating devices and software all are intertwined with privacy concerns. For some of these purposes, it is crucial to be able to identify individuals and link together an individual's records, so a requirement for de-identification may further impair research.

However, there also could be harms. Patients may withhold sensitive information if they fear it will be used against them, even though it may be useful for other purposes. Studies based on analyzing large data sets could be compromised if individual prescribers or patients withhold information or their consent for data use.[56]

Privacy advocates, researchers, and public health officials can be at odds over how to achieve benefits while protecting privacy in ways that stem from different values and historical legacies. For example, the UK's National Health Service (NHS) and a Wellcome Trust-lead coalition of leading medical research organizations oppose the EU's move towards greater health data protection. Though the proposals are acceptable to most other EU nations, they would make illegal the NHS mass database of citizens' health information that could provide a valuable resource for improving care.[57] [58] [59] The database also provokes privacy concerns while providing financial benefit as the NHS sells the data.[60] Individuals can opt-out of the new care.gov database, which was to contain, for the first time, records from primary care (GP) practices. Privacy concerns delayed including those GP records.[61] Although other rules allow greater third-party access to other NHS databases,[62] insurers, pharmaceutical companies, and other private commercial enterprises will receive "pseudoanonymized" records that the NHS claims "will not contain information that identifies you," but that instead include NHS numbers, date of birth, postcode, ethnicity and gender.[63] The database was created, according to NHS England to improve NHS services,[64] and to "drive economic growth by making England the default location for world-class health services research."[65] In the US, too, researchers and bioethicicts recognize that privacy protections can impede research and health care quality improvement, with calls from such influential agencies as the Institute of Medicine for changing the HIPAA Privacy Rule to allow for information-based research, i.e. research using medical records or stored biological samples.[66]

Some innovative approaches to meeting privacy, research, and commercial needs for data sharing include the new international Open Humans Network, which "attempts to

break down health data silos through an online portal that will connect participants willing to share data about themselves publicly with researchers who are interested in using that public data and contributing their analyses and insight to it"[67] and businesses based on similar ideas, such as PatientsLikeMe. Using the data people post, PatientsLikeMe produces publishable material on patient outcomes and comparative effectiveness, valuable for effectiveness research. Epidemiologic trends also can identified through social media postings.[68] [69] [70] Those engaging in this social networking presumably feel it is beneficial to them. Even so, it would be better if they were aware of what is done with their data, instead of being surprised if they have not read subscription agreements carefully enough to know that PatientsLikeMe sells data to pharmaceutical and other companies and that sites such as Facebook are not private places.[71] [72]

Who Sells and Uses Data?

As is evident from the multiplicity of uses, health data is valuable. Internationally, the need for "liberating" data for secondary use is recognized as beneficial for individual and public benefit, research, entrepreneurship, and policy. Though transborder data flow is regulated by international agreements, such as the EU Data Protection Directive, presumably health data could be sold worldwide, to anyone, for any purpose. Balancing this with privacy concerns is fraught.[73] Strong privacy protection, such as the European Court of Human Rights's rights-centric approach, could adversely affect the globalized healthcare industry, and innovation and trade.[74] [75] [76] [77]

Entire patient records are among the many possible sources of data for which there is a lucrative market, for laudable as well as for unsavory purposes. In the active black market in identifiable medical record information, health information is more

valuable than US Social Security numbers for identity theft.[78] [79] It sells for about ten times more than credit card data because it can be monetized for getting treatment paid for via identity theft.[80]

Electronic records also make it possible for computer or software vendors, intermediaries, or newly created organizations to bundle and sell rights and data,[81] useful for research, policy, marketing, and business. In the US, an exhaustive list of organizations can use and legally sell health information,[82] some for purposes patients and clinicians would not anticipate. Data sold by both US state and federal agencies can be linked to individuals using public information even if some of the data is de-identified.[83] [84]

One Man's Bread is Another Man's Poison

Some may consider what is done with this data as harmful to some individuals providing the data while benefiting other individuals, depending on what the data reveal. This combination of benefits and harms is evident in a variety of examples in which one's records affect one's services and costs. In the US, where private medical insurance is the norm, private insurers use prescription and other claims data to deny insurance, charge differential premiums, or exclude some conditions.[85] Businesses often check the MIB (Medical Information Bureau) for job applicants' underwriting data.[86] Aggregators purchase and combine data from the states as well as from pharmacies.[87] Credit agencies are the most frequent buyers of multi-state health profiles, though IMS Health also purchases data from the states.[88] Government fusion centers, designed to promote data sharing among federal agencies, state, and local governments, combine data from

multiple sources, including health record information, for law enforcement, immigration control, and homeland security.[89] [90]

Organizations, too, may benefit financially while providing social benefit through data sales. The American Medical Association, state health information exchanges (HIEs), and the US Centers for Medicare and Medicaid sell provider data.[91] [92] [93] The UK's National Health Service, too, sells data.[94] Insurance companies or health information technology vendors might aggregate and sell provider-identified data on performance and quality measures, number of procedures performed, US meaningful use criteria, data security breaches, and other useful purposes. Cash-strapped community health organizations, state Regional Extension Centers, county hospitals, the Veterans Administration, Indian Health Service, the Joint Commission, or hospital associations also could sell data for similarly beneficent purposes.

Genetic data is similarly double-edged. It is needed for research, personalized medicine, and biobanking, but also can make individuals and communities vulnerable. For example, in 2000, Iceland's Parliament's sold exclusive rights to all the genetic and geneological data from each of its 275,000 citizens to the US company deCODE Genetics. Soon thereafter, deCODE signed a $200 million contract with Hoffman LaRoche to search for several common human genetic diseases. Iceland had an opt-out policy and the data was encrypted to de-identify individuals. Nevertheless, the Icelandic Supreme Court later ruled that creating the database was unconstitutional because it did not adequately protect personal privacy.[95]

Clearly, provider or patient information is valuable. Hospitals could purchase data about competitors, providers could identify populations for treatment, researchers

could conduct studies involving health care and public health practices, and government agencies could identify and influence health trends. If such sales were restricted, some fear, the data would not be collected or maintained at all, which could compromise research and new drug development.[96] [97] The Iceland genetic database sale, for example, led to successfully identifying genes linked to disease,[98] [99] though possibilities for these kinds of discoveries were limited to the company with exclusive rights to this gene discovery. DeCode's 2009 bankruptcy and consequent database ownership change from a scientific research company to Saga Investments LLC, and subsequent sale in 2012 to biotech pioneer Amgen again raised questions about data privacy.[100] [101]

Countries as different as Canada, Estonia, Sweden, Singapore, and the Kingdom of Tonga developed various models for protecting privacy and differing policies regarding commercial involvement and rights to samples for genebanks, all with the goal of improving public health of the studied population, and, in some cases, to generate revenue for national health care budgets. Though all these polices are intended to maintain confidentiality, all need personal identifiers so as to link individuals' records from genetic, medical, geneological, and lifestyle databases. International controversy over such databases, therefore, centers around confidentiality, consent, to what extent commercial interests should influence policy, and whether commercial ownership facilitates or impedes research,[102] [103] [104] all concerns related to collecting and selling health care data in general.

As a way of raising additional considerations, I pose possibilities that might occur were there unrestricted selling of health data. Abortion opponents presumably could buy aggregated prescription information for medications that cause abortions, or animal rights

activists could buy information about researchers' animal purchases. Depending upon who purchases it and their purpose, such information could threaten or protect researchers', clinicians', and patients' safety and might have adverse effects on research and clinical practice, or open new avenues. Physicians, patients, hospitals, etc. in one country may be targeted for marketing by commercial ventures or medical tourism facilities in another. Some may welcome learning of such opportunities while others may feel harassed or violated. Individuals in one country may experience salutary or salacious effects from having (identified or possibly re-identified) data available elsewhere. But without transparency, there is little chance of gaining individual consent or, on both individual and societal levels, assessing harm or benefit.

Ownership, Commodification, and De-Contextualization

The right to sell data is muddied by lack of clarity over the legalities of data ownership. Law in and outside the US does not address health data ownership clearly; it is not clear who the owner should be, or whether ownership is better than the current approach.[105] [106] It also is not clear where those who also sell data analytics services obtain the data, or how they might use it.[107] Whether the data itself or the means of access to it is owned by electronic health records vendors, some academic medical centers pay for getting data from their own patients' records. Well-known electronic health record vendors have sold de-identified copies of their patient databases to pharmaceutical companies, medical devicemakers, and health services researchers.[108] Vendor contracts are unusual in that some vendors lay claim to patient record data whereas businesses and financial institutions typically do not give up their data to their software vendors.[109] Vendors often consider their contracts intellectual property and do not reveal these and

other contract provisions, a practice The American Medical Informatics Association considers unethical.[110]

If health data is property, presumably, whoever owns the data can sell it. Some advocate clearly-defined property rights in medical information, giving patients the right to monetize their access and control rights, as a way for individuals to control and benefit from what happens to data about them.[111] Others argue against property rights in patient data and advocate instead public ownership akin to a data commons so that data from multiple sources can be de-identified and combined population-wide for public benefit.[112] Commodifying medical information strikes others as anathema to professional values and the special relationship between doctor and patient. The idea of selling personal health data also disturbs those who think it commodifies the self and sullies ideas of personhood.[113] [114] Compromising of personhood is compounded because data in databases necessarily is de-contextualized. De-identification is an attempt to remove any connection with the person, but even identifiable health record data typically does not include all information a person may consider central to the self.

Conclusions

Widespread use of electronic patient record systems enables opportunities to improve health care through data sharing, secondary use, and big data analytics. Multiple health care professionals, payers, researchers, and commercial enterprises can access data and reduce costs by eliminating duplication of services and conducting research on effective care. Widespread use of electronic patient records systems also creates more opportunities for privacy violations, data breaches, and inappropriate uses.

Ethical and policy analysis related to health data and informatics should consider benefits and harms, taking into account both the uses and users of the information.[115] [116] Embarrassing an estranged spouse by publishing his or her mental health records is more distasteful than using those records combined with others' to study and improve mental health. As this example suggests, some users (the researcher) are more appealing than others (the spouse). Moreover, an uncontroversial use may be morally offensive if the user is unsavory or controversial.[117] How should distinctions be made so that some data uses and users are permissible and some not? On what grounds? And who is best placed to make such decisions: the courts or legislators, clinicians and researchers who are most familiar with their data needs, companies that develop and market new medications, or patients and prescribers who are most affected by privacy violations and can best weigh the relative importance of various values to themselves.[118]

Those most familiar with, closest to, and affected by the potential use should have a strong say. They need to know about those uses, though, to do to so in an informed, thoughtful way. Many patients do not know what is, or can be, done with their data, but keeping them ignorant is not the way to address concerns. Lack of accountability and transparency about health data uses feed the public's privacy concerns,[119] undermine the possibility of informed consent, and impair research, care, and public health.

Ethical considerations over data use will, and should, evolve as the public becomes more aware of the value and pitfalls of data sharing, data aggregation, and data mining. Because something can be done does not mean that it should be, and what is legal is not the same as what is ethical. Cases like *Source* and *Sorrell* encourage debate over propriety and values related to different kinds of data use. They also lead to

examining when it is in the public interest for personal health data to be made available, just what that "public interest" is,[120] [121]and, for that matter, just what "privacy" comprises and entails as norms evolve.[122] The issues include considering, in a healthcare context, dualities playing out with respect to big data in domains other than healthcare: the individual v. the aggregate, research v. privacy, individual v. institutional power, identification v. identity, identification v. authentication, and virtual people v. real people and contextualized information. They involve big data harms and benefits related to innovation and economic advancement, power shifts, access to knowledge, and freedom of communication.

Societies and governments need to grapple with these ethical issues, tensions between privacy and other considerations, and shifting norms. The numerous cross-cutting issues suggest that other areas of law, ethics, and social policy also can inform the related ethical and legal considerations**.** For some time, the legal, the bioethics, and the informatics communities have been considering issues such as appropriate secondary use of data; patient and clinician relationships in light of the growth of electronic health records and health information technologies;[123] [124] [125] reliance on increasingly untenable de-identification; burgeoning electronic data collection, sharing, transmission, and aggregation; data use for public health, research, and innovation; and privacy and security of health data.

As health information exchanges and health tourism develops, as lifetime electronic health records which follow patients across governmental and institutional boundaries are used more widely; as databases grow and biobanks become digital; as biometric identification becomes more common; as radio frequency identification devices

(RFIDs) are embedded in medical devices, smartpills, and patients; as home sensors and monitors increasingly are used; e- and mobile health applications expand, and health information exchanges develop,[126] [127] [128] [129] informaticians can add to the conversation among governments, courts, regulatory agencies, professional societies, and other organizations consider responses to issues raised in *Sorrell* and *Source* and to other uses of health-related data. Combining legal and ethics scholarship with informaticians' expertise concerning judicious and ethical data collection and use, together with their technical knowledge of data aggregation and identification, can contribute to more informed policies.

The *Source* and *Sorrell* court cases can provoke an initial reaction of outrage over privacy violations and data use without consent. Consequently, they call into question just what constitutes "privacy" and "public interest," and considerations for balancing them. They provide an opportunity to weigh privacy and numerous beneficial uses for data. Transparency and accountability are needed so that harms and benefits can be judged through public discussion and so that individual as well as societal decisions can be made on more informed and thoughtful grounds. Using data collected for one purpose (such as prescriptions) for another purpose (such as pharmaceutical marketing) can undermine public confidence, especially if the public is unaware of the reuse. Doing so without individuals' permission violates international principles of data privacy.[130] [131] [132] [133] [134] The court cases prompt ethical questions of commodifying medical information and of harmonizing policy across jurisdictional boundaries. Their consequences may affect biomedical informatics, patient and clinician privacy, and regulation in ways this paper explores, in the US, UK, and elsewhere.

Contributor:

Bonnie Kaplan, PhD, FACMI, is a Lecturer in Medical Informatics at the Yale School of Medicine, a Yale Interdisciplinary Center for Bioethics Center Scholar, a Faculty Fellow of the Information Society Project at the Yale Law School, and affiliate faculty of the Program for Bioethics at the Yale School of Medicine. Currently a Hastings Center Visiting Scholar, her research involves ethical, legal, and social issues in health information technology, health information technology implementation issues, and sociotechnical evaluation of health information technology systems. She is past chair of the Ethical, Legal, and Social Issues Working Group and of the People and Organizational Issues Working Group of the American Medical Informatics Association (AMIA), a recipient of the American Medical Informatics Association President's Award, and a Fellow of the American College of Medical Informatics.

Notes

[1] Laura Wexler's respondent's comments at The Critical Life of Information Conference, Yale University, April 11, 2014 outlined dualities related to big data. See http://wgss.yale.edu/sites/default/files/files/Critical%20Life%20of%20Information%20Program%20spreads.pdf, accessed August 19, 2014.

[2] Jost TS. *Readings in Comparative Health Law and Bioethics*. 2 ed. Durham, NC: Carolina Academic Press; 2007.

[3] B. Selling Health Data: De-Identification, Privacy, and Speech. *Cambridge Quarterly of Healthcare Ethics* in press.

[4] Jones P. Permission-Based Marketing under Canada's New Privacy Laws. *Franchise Law Journal* 2004;24(2):267-303.

[5] Walden I. Anonymising Personal Data. *International Journal of Law and Information Technology* 2002;10(2):224-37.

[6] Srinivas N, Biswas A. Protecting Patient Information in India: Data Privacy Law and Its Challenges. *NUJS Law Review* 2012;5(3):411-24.

[7] United States Government, Department of Health and Human Services, Office for Civil Rights. Summary of the HIPAA Privacy Rule. Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/, accessed June 30, 2013.

[8] United States Government, Department of Health and Human Services, Office for Civil Rights. Standards for Privacy of Individually Identifiable Health Information. Available at http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm, accessed January 19, 2014.

[9] United States Government, Department of Health and Human Services, Office of the Secretary. 45 CFR Parts 160 and 164: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule. In. Federal Register; January 25, 2013:5565-702. Available at http://www.gpo.gov/fdsys/pkg/FR-

2013-01-25/pdf/2013-01073.pdf, accessed July 2, 2014.

[10] European Union. EU Directive 95/46/EC - The Data Protection Directive Available at http://www.dataprotection.ie/docs/EU-Directive-95-46-EC--Chapter-2/93.htm, accessed March 23, 2014.

[11] European Union. The European Data Protection Supervisor. Available at http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm, accessed March 23, 2014. Maintained or enhanced in http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT, accessed March 23, 2014.

[12] Solove DJ. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 2006;154(3):477-560.

[13] Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 2010;57:1701-77, p. 270.

[14] Taylor MJ. Health Research, Data Protection, and the Public Interest in Notification. *Medical Law Review* 2011;19(2):267-303.

[15] See n. 14, Taylor 2011, p. 303.

[16] Kaplan B. Health Data Privacy. In: Yanisky-Ravid S, ed. *Beyond Intellectual Property: The Future of Privacy*. New York: Fordham University Press; forthcoming.

[17] See n. 3, Kaplan in press.

[18] See n. 13, Ohm 2010.

[19] See n. 16, Kaplan forthcoming.

[20] Beyleveld D, Histed E. Betrayal of Confidence in the Court of Appeal. *Medical Law International* 2000;4:277-311.

[21] Koontz L. What Is Privacy? In: Koontz L, ed. *Information Privacy in the Evolving Healthcare Environment* Chicago: Healthcare Information and Management Society (HIMSS); 2013:1-20.

[22] See n. 16, Kaplan forthcoming.

[23] See n. 3, Kaplan in press.

[24] World Medical Association. International Code of Medical Ethics. Available at http://www.wma.net/en/30publications/10policies/c8/index.html, accessed May 2, 2014.

[25] World Medical Association. Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects. Available at http://www.wma.net/en/30publications/10policies/b3/, accessed May 2, 2014.

[26] World Medical Association. Declaration on Ethical Considerations Regarding Health Databases. Available at http://www.wma.net/en/30publications/10policies/d1/, accessed May 2, 2014.

[27] See n. 26, WMA.

[28] See n. 2, Jost 2007.

[29] Malin BA, El Emam K, O'Keefe CM. Biomedical Data Privacy: Problems, Perspectives, and Recent Advances. *JAMIA (Journal of the American Medical Informatics Association)* 2013;20(1):2-6.

[30] See n. 20, Beyleveld, Histed 2004, p. 296.

[31] Dunkel YF. Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United State in Light of the Source Informatics Cases. *Loyola of Los Angeles International and Comparative Law Review* 2001;23(1):41-80.

[32] See n. 6, Srinivas 2012.

[33] See n. 4, Jones 2004.

[34] Powell J, Fitton R, Fitton C. Sharing Electronic Health Records: The Patient View. *Informatics in Primary Care* 2006;14(1):55-7.

[35] Schers H, van den Hoogen H, Grol R, van den Bosch W. Continuity of Information in General Practice. Patient Views on Confidentiality. *Scandinavian Journal of Primary Health Care* 2003;21(1):21-6.

[36] See n. 20 Beyeleveld, Histed, 2000.

[37] See n. 20, Malin, El Eman, O'Keefe, 2013.

[38] See n. 31, Dunkel, 2001.

[39] Deskmuch P, Coasdell D. HIPAA: Privacy and Security in Health Care Networks. In: Freeman L, Peace AG, eds. *Information Ethics: Privacy and Intellectual Property*. Hershey, PA: Idea Group; 2005:219-37.

[40] See n. 10, EU

[41] McGraw D. Building Public Trust in Uses of Health Insurance Portability and Accountability Act De-identified Data. *JAMIA (Journal of the American Medical Informatics Association)* 2013;20(1):29-34.

[42] Curfman GD, Morrissey S, Drazen JM. Prescriptions, Privacy, and the First Amendment. *New England Journal of Medicine* 2011;364(21):2053–5.

[43] Tien L. Online Behavioral Tracking and the Identification of Internet Users. In: The Information Society Project at the Yale Law School, ed. *From Mad Men to Mad Bots: Advertising in the Digital Age*. Yale University, New Haven, CT; 2011.

[44] Benitez K, Malin B. Evaluating Re-identification Risks with respect to the HIPAA Privacy Rule. *JAMIA (Journal of the American Medical Informatics Association)* 2010;17(2):169-77.

[45] See n. 13, Ohm 2010.

[46] See n. 3 Kaplan in press.

[47] Sorrell v. IMS Health, Inc. et al, 131 S. Ct. 2653, (2011).

[48] R v. Department of Health, Ex Parte Source Informatics Ltd., [C.A. 2000] 1 All ER 786. See also R v. Department of Health, Ex Parte Source Informatics Ltd. *European Law Report* 2000;4:397-414.

[49] See n. 3, Kaplan in press.

[50] See n. 6, Srinivas 2012.

[51] See n. 4, Jones 2004.

[52] Baxter AD. IMS Health v Ayotte: A New Direction on Commercial Speech Cases. *Berkeley Technol Law J* 2010;25:649-70.

[53] Pasquale F. Restoring Transparency to Automated Authority. *Journal on Telecommications and High Technology Law* 2011; 9:235–54.

[54] Rodwin MA. Patient Data: Property, Privacy, & the Public Interest. *American Journal of Law and Medicine* 2010;36:586-618, p. 589.

[55] Hall MA, Schulman KA. Ownership of Medical Information. *JAMA* 2009;301(12):1282-4.

[56] Gooch GR, Rohack JJ, Finley M. The Moral From Sorrell: Educate, Don't Legislate. *Health Matrix* 2013;23(1):237-77.

[57] O'Donoghue C. EU Research Group Condemns EU Regulation for Restricting Growth in Life Sciences Sector. 2014. Available at http://www.globalregulatoryenforcementlawblog.com/2014/02/articles/data-security/eu-research-group-condemns-eu-regulation-for-restricting-growth-in-life-sciences-sector/, accessed March 23, 2014.

[58] Farrar J. Sharing NHS Data Saves Lives; EU Obstruction Will Not. *The Telegraph* 2014 January 14, 2014. Available at http://www.telegraph.co.uk/health/nhs/10569467/Sharing-NHS-data-saves-lives-EU-obstruction-will-not.html, accessed March 23, 2014.

[59] European Public Health Alliance. [Update] General Data Protection Regulation. Available at http://www.epha.org/5926, accessed March 23, 2014.

[60] Doctorow C. UK Set to Sell Sensitive NHS Records to Commercial Companies with No Meaningful Privacy Protections - UPDATED. February 4, 2014. Available at http://boingboing.net/2014/02/04/uk-set-to-sell-sensitive-nhs-r.html, accessed February 5, 2014.

[61] Donnelly L. Hospital Records of All NHS Patients Sold to Insurers. *The Telegraph* February 23, 2014. Available at http://www.telegraph.co.uk/health/healthnews/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html, accessed July 24, 2014.

[62] See n. 61, Donnelly 2014.

[63] Your Records: Better Information Means Better Care. Available at http://www.nhs.uk/nhsengland/thenhs/records/healthrecords/pages/care-data.aspx, accessed July 24, 2014.

[64] See n. 63, NHS England.

[65] Ramesh R. NHS Patient Data to Be Made Available for Sale to Drug and Insurance Firms. *The Guardian* January 19, 2014. Available at http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy, accessed July 24, 2014.

[66] Institute of Medicine. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: National Academies; 2009. Available at http://www.iom.edu/~/media/Files/Report%20Files/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research/HIPAA%20report%20brief%20FINAL.pdf accessed January 22, 2014.

[67] Open Humans Network. Open Humans Network Wins Knight News Challenge: Health Award. Available at http://openhumans.org/, accessed July 1, 2014.

[68] Christakis NA, Fowler JH. Social Network Vsualization in Epidemiology. *Norwegian Journal of Epidemiology* 2009;19(1):5-16.

[69] Christakis NA, Fowler JH. Social Network Sensors for Early Detection of Contagious Outbreaks. *PLoS ONE* 2010;5(9): e12948.

[70] Velasco E, Agheneza T, Denecke K, Kirchner G, Eckmanns T. Social Media and Internet-Based Data in Global Systems for Public Health Surveillance: A Systematic Review. *The Milbank Quarterly* 2014;93(1):7-33.

[71] Andrews L. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Data Privacy*. New York: Free Press; 2011.

[72] Angwin J. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books, Henry Holt and Company; 2014.

[73] Geissbuhler A, Safran C, Buchan I, Bellazzi R, Labkoff S, Eilenberg K, . . . De Moor G. Trustworthy Reuse of Health Data: A Transnational Perspective. *International Journal of Medical Informatics* 2013;83(1):1-9.

[74] See n. 6, Srinivas 2012.

[75] See n. 14, Taylor 2011.

[76] Bambauer JR. Is Data Speech? *Stanford Law Review* 2014;66:57-120.

[77] Zarsky TZ. The Privacy/Innovation Connundrum. Working paper, on file with author. Presented at The Information Society Project at the Yale Law School *Privacy and Innovation* conference, Yale University, New Haven, CT; 2014.

[78] Avila J, Marshall S. Your Medical Records May Not Be Private: ABC News Investigation. September 13, 2012. Available at http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986&page=2, accessed March 22, 2014.

[79] Nguyen V, Nious K, Carroll J. Your Medical Records Could Be Sold on Black Market: NBC Investigative Unit surprises strangers with private medical details. June 18, 2013. Available at http://www.nbcbayarea.com/news/local/Medical-Records-Could-Be-Sold-on-Black-Market-212040241.html, accessed March 22, 2014.

[80] Lawrence D. End of Windows XP Support Means Added Opportunity for Hackers. *Businessweek* April 04, 2014. Available at http://www.businessweek.com/articles/2014-04-04/end-of-windows-xp-support-means-added-opportunity-for-hackers, accessed July 1, 2014.

[81] See n. 55, Hall, Schulman 2009.

[82] See n. 31, Dunkel 2001.

[83] See n. 44, Benitez, Malin 2010.

[84] Roberston J. States' Hospital Data for Sale Puts Privacy in Jeopardy. 2013. Available at http://www.healthleadersmedia.com/content/QUA-292963/States-hospital-data-for-sale-puts-privacy-in-jeopardy, accessed June 14, 2013.

[85] Brief for the New England Journal of Medicine, the Massachusetts Medical Society, the National Physicians Alliance, and the American Medical Students Association as Amici Curiae Supporting Petitioners, William H. Sorrell v. IMS Health, Inc. et al., 2010 U.S. Briefs 779 (No. 10-779), 2011 U.S. S. Ct. Briefs LEXIS 299.

[86] Holtzman DH. *Privacy Lost: How Technology is Endangering Your Privacy*. San Francisco: Jossey-Bass; 2006.

[87] See, for example, RPC Health Data Store. CMS MedPAR Hospital Data File. Available at http://www.healthdatastore.com/cms-medpar-hospital-data-file.aspx, accessed September 13, 2013.

[88] [Winston JS]. States' Hospital Data for Sale Puts Patient Privacy in Jeopardy. June 7, 2013. Available at https://www.annualmedicalreport.com/states-hospital-data-for-sale-puts-patient-privacy-in-jeopardy/, accessed January 19, 2014.

[89] Bady A. World Without Walls-Privacy Laws Should Be Recrafted for the Data Fusion Age. *Technology Review* 2011:66 –71.

[90] United States Government, Department of Justice. Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era. 2006. Available at http://www.it.ojp.gov/documents/fusion_center_guidelines.pdf, accessed March, 2012.

[91] See n. 42, Curfman, Morrissey, Drazen 2011.

[92] Hebda T, Czar P. *Handbook of Informatics for Nurses and Healthcare Professionals*. 4th ed. Upper Saddle River, NJ: Pearson/Prentice Hall; 2009.

[93] United States Government, Department of Health and Human Services, Centers for Medicare & Medicaid Services. Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Unique Identifiers, Form CMS-R-0235, OMB No. 0938-0734. Available at

http://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads//cms-r-0235.pdf, , accessed September 13, 2013.

[94] See n. 61, Donnelly 2014.

[95] McGraw Hill General and Human Biology Case Studies. Gene Banks Versus Privacy Invasion. Available at http://www.mhhe.com/biosci/genbio/casestudies/sellinggenes.mhtml, accessed May 2, 2014.

[96] Brief for the Association of Clinical Research Organizations as Amici Curiae Supporting Respondents, William H. Sorrell v. IMS Health, Inc. et al, 2011 WL 2647130 (2011) (No. 10-779), (2011).

[97] See n. 56, Gooch, Rohack, Finley 2013.

[98] See n. 95, McGraw Hill 2014.

[99] Austin MA, Harding S, McElroy C. Genebanks: A Comparision of Eight Proposed International Genetic Databases. *Community Genetics* 2003;6(1):37-45.

[100] Gillham WW. *Genes, Chromosomes, and Disease: From Simple Traits, to Complex Traits, to Personalized Medicine*. Upper Saddle River, NJ: Pearson Education, published as FT Press Science; 2011.

[101] Amgen to Acquire deCODE Genetics, a Global Leader in Human Genetics. Available at www.amgen.com/media/media_pr_detail.jsp?releaseID=1765710, accessed May 2, 2014.

[102] See n. 99, Austin, Harding, McElroy 2003.

[103] Annas GJ. Rules for Research on Human Genetic Variation--Lessons from Iceland. *New England Journal of Medicine* 2000;342(24):1830-3.

[104] Gulcher JR, Steffánsson K. The Icelanding Healthcare Database and Informed Consent. *New England Journal of Medicine* 2000;342(24):1827-9.

[105] See n. 16, Kaplan forthcoming.

[106] Evans BJ. Much Ado About Data Ownership. *Harvard Journal of Law & Technology* 2011;25(11).

[107] For example, GE Data Visualization uses information "based on 7.2 million patient records from GE's proprietary database". Available at http://visualization.geblogs.com/visualization/network/, accessed September 27, 2013. GE Healthcare's Healthcare IT Solutions, http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT?gclid=CIKQ4Z6P7LkCFcE7OgodTDIAPQ, and http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT/Knowledge_Cente, accessed September 27, 2013, includes patient records and patient portals.

[108] Sittig DF, Singh H. Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use. *Pediatrics* April 2011;127(4):e1042-7.

[109] Moore J, Tholemeier R. Whose Data Is It Anyway? November 20, 2013. Available at http://thehealthcareblog.com/blog/2013/11/20/whose-data-is-it-anyway-2/, accessed February 3, 2014

[110] Goodman KW, Berner E, Dente MA, Kaplan B, Koppel R, Rucker D, . . . Winkelstein P. Challenges in Ethics, Safety, Best Practices, and Oversight Regarding HIT Vendors, Their Customers, and Patients: A Report of an AMIA Special Task Force. *JAMIA (Journal of the American Medical Informatics Association)* 2011;18(1):77-81.

[111] Hall MA. Property, Privacy, and the Pursuit of Interconnected Electronic Health Records. *Iowa Law Review* 2010;95:631-63.

[112] See n. 54, Rodwin 2010.

[113] See n. 55, Hall, Schulman 2009.

[114] Atherley G. The Public-Private Partnership Between IMS Health and the Canada Pension Plan. *Fraser Forum* 2011:5-7.

[115] Miller RA, Schaffner KF, Meisel A. Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine. *Annals of Internal Medicine* 1985;102:529-36.

[116] Goodman KW. Health Information Technology: Challenges in Ethics, Science and Uncertainty. In: Himma K, Tavani H, eds. *The Handbook of Information and Computer Ethics*. Hoboken: Wiley;

2008:293-309.

[117] See n. 116, Goodman 2008.

[118] Data Mining Case Tests Boundaries of Medical Privacy. *CMAJ* 2011;183(9):E509-10.

[119] See n. 50, McGraw 2013.

[120] See n. 14, Taylor 2011.

[121] See n. 54, Rodwin 2010, pp. 617-618.

[122] See n. 12, Solove 2006.

[123] Goodman KW. Ethics, Information Technology, and Public Health: New Challenges for the Clinician-Patient Relationship. *Journal of Law, Medicine and Ethics* 2010(Spring):58-63.

[124] Kaplan B, Litewka S. Ethical Challenges of Telemedicine and Telehealth. *Cambridge Quarterly of Healthcare Ethics* 2008;17(4):401-16.

[125] See n. 16, Kaplan forthcoming.

[126] See n. 123,Goodman 2010.

[127] See n. 124,Kaplan, Litewka 2008.

[128] See n. 16, Kaplan forthcoming.

[129] Roland D. UK to Get 200 High-Tech Factory Jobs Making 'Swallowable Sensors'. *The Telegraph* 2014 March 10, 2014. Available at http://www.telegraph.co.uk/finance/10687395/UK-to-get-200-high-tech-factory-jobs-making-swallowable-sensors.html, accessed July 17. 2014.

[130] See n. 21, Koontz, 2013.

[131] See n. 41, McGraw 2013.

[132] See n. 20, Beyleveld, Histed, 2000.

[133] See n. 10, EU.

[134] Rodrigues RJ, Wilson P, Schanz SJ. *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases*. Washington DC World Health

Organisation (WHO); 2001.