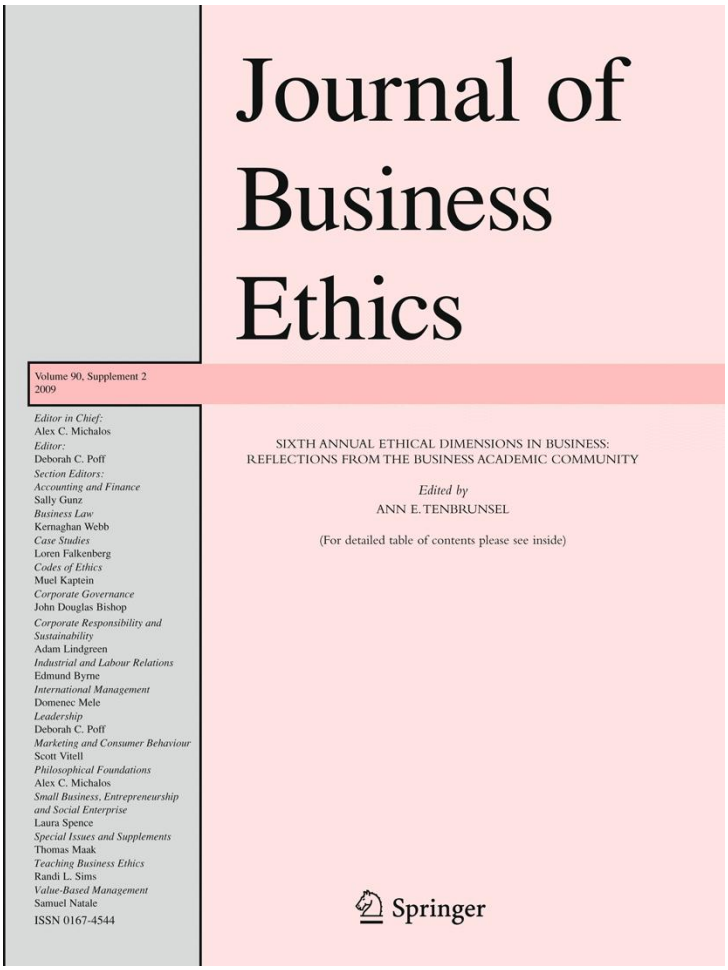
ISSN 0167-4544, Volume 90, Supplement 2



Journal of Business Ethics (2009) 90:169–178
DOI 10.1007/s10551-010-0385-5

Protect My Privacy or Support the Common-Good? Ethical Questions About Electronic Health Information Exchanges

Corey M. Angst

ABSTRACT. When information is transformed from what has traditionally been a paper-based format into digitized elements with meaning associated to them, new and intriguing discussions begin surrounding proper and improper uses of this codified and easily transmittable information. As these discussions continue, some health care providers, insurers, laboratories, pharmacies, and other healthcare stakeholders are creating and retroactively digitizing our medical information with the unambiguous endorsement of the federal government. Some argue that these enormous databases of medical information offer improved access to timely information, evidence-based treatments, and complete records from which to provide care. To the extent that these claims are true, it would seem that this is a valuable asset that offers immeasurable benefit to all. Others believe this digitization to be an egregious invasion of privacy. In this article, I investigate the broad research questions of whether the *public good* aspect of capturing private health information outweighs individual interests and whether it is ethical to mandate participation in health information exchanges by all individuals who use the U.S. health system.

KEY WORDS: health information exchange, privacy, electronic medical record, ethics, social dilemma, public good

Introduction

With the recent proliferation of clinician-managed electronic medical records (EMR) and personally controlled electronic health records (PHR), our society has embarked on a new frontier with respect to the use of digital health information. When information is transformed from what has traditionally been a paper-based format into digitized elements with meaning associated to them, new and intriguing discussions begin surrounding proper and improper uses of this codified and easily transmittable information. The popular press has elevated this issue to the forefront of the American conscience and it was a key campaign issue for our recent political candidates. For example, on February 17, 2009, President Obama signed into law, *HR 1, The American Recovery and Reinvestment Act*, which allocates $19.2 billion dollars in funding[1] to support the adoption and use of health information technology. Further, a number of large technology companies and consortia of firms (e.g. Google, Microsoft, Dossia) have entered the domain of medical information storage and search (Kush et al., 2008; Mandl and Kohane, 2008; Yasnoff et al., 2008), thus lending legitimacy and momentum to the movement. Yet, even without a set of common rules or guidelines established, and as the privacy of health information continues to be discussed and debated, new initiatives designed to share data are underway. One highly publicized program is seeking 100,000 volunteers to have their DNA genome mapped and made available online in conjunction with personal medical profiles including disease histories, allergies, medications, ethnic backgrounds, and other traits from food preferences to television viewing habits. The program, which was kicked off in early 2008 with 10 volunteers – the so called PGP10 – who are considered experts in the field of genomics and disclosure (see www.personalgenomes.org), is designed to demonstrate that the pace of medical research and discovery can be dramatically increased if individuals voluntarily forfeit certain elements of their private information (Harmon, 2008). Proponents suggest that these large databases could be used by researchers

to study any number of medical conditions, behaviors, traits, and other social phenomena (Lazer et al., 2009). Privacy advocates, on the other hand, argue that these projects are misguided and most "non-expert" participants would not have a full understanding of what opting-in means due to the still-evolving uses of the information that may arise.

With these innovations come issues that must be considered such as privacy and fair treatment of an individual's personal data. In particular, questions regarding how individual data can and should be used in different contexts is critically important. For example, are there situations in which health data should be considered a public good that can be accessed for research and treatment purposes? Are there instances in which identifiable data should be accessible by specific entities such as those involving law enforcement? In cases like these, it seems plausible that legislation would be enacted to mandate enrollment in health information exchanges (HIE). These are but a couple examples that demonstrate the complexities surrounding the capture of health data. Below, I provide a brief introduction that places the use of personal data within the context of the U.S. health system. I draw from relevant literatures to investigate the broad research questions of whether the public good aspect of capturing private health information outweighs individual interests and whether it is ethical to mandate participation in HIEs by all individuals who use the U.S. health system.

The health care context

Several factors have aligned to bring the topic of HIE to the forefront. The EMR (used by physicians for maintaining patient records) is considered by most to be the technology at the heart of the controversy (Lohr, 2006; Sidorov, 2006). Yet, the EMR, in and of itself is merely a database platform with a simple user interface designed for the entry and acquisition of patient information. The concerns around this technology are that detailed medical information is captured in specific fields that can easily be transmitted to another system. For example, a patient identifier such as Joe Smith, SSN 123-45-4321, could be tied directly to a variable named HbA1c (which is a standard measure used to assess blood sugar for patients with diabetes) and a value. Because the EMR technology platform resides within one hospital or physician practice, most people would not be concerned about the misuse of this data since there would appear to be some controls surrounding dissemination. The anxiety seemingly results when the reach of the EMR extends beyond the walls of the entity that captured the data. This is where HIE comes into play. Since the data were collected and coded in a standard way, specific elements can easily be transmitted to other systems that "speak the same language," thus making the systems interoperable, which many argue is where the benefits reside. For example, early studies of HIE estimate that approximately $120 billion in savings per year from health care costs can result by eliminating duplicate tests, shortening hospitals stays, and improving care for chronically ill patients (Hillestad et al., 2005; Pan et al., 2004). Skeptics and cynics argue that creating databases of health information only further the agenda of control by various stakeholders. A common complaint is that having access to large databases of medical information will allow insurance companies to "cherry-pick" only those people who are healthy and require fewer health services. Yet, there is another, possibly more controversial issue associated with HIE. HIE provides the mechanism through which disparate data can be joined by a common element (Mason, 1986) such as social security numbers (or even name, date of birth, and gender) in unanticipated ways, often without the knowledge or consent of the patient. This generation of new information, or what I will call "information conception," creates additional uses for the data and associated security and privacy risks. For example, while an individual may have allowed his medical record at a hospital to be tied to his social security number, he would not have been asked to consent to cross-referencing his social security number with a law enforcement database. Yet, the potential for some of this cross-matching to occur without the knowledge of consumers is high and increases as more stakeholders handle the data.

Taking this one step further, people knowingly and willingly provide information to an organization for a specific intent such as a transaction for a good or service. This is known in the literature as the "first exchange," (Culnan and Milberg, 1998). A subset of the first exchange customers will opt-in to loyalty or personalized programs from the same firms by

providing additional personal information with the understanding that greater service or personalized treatment would result. This non-monetary exchange is known as a "second exchange," (Culnan and Milberg, 1998). There is considerable value in this rich data not only for the acquiring firm but also for firms that offer related goods and services. With the proliferation of technology and standards that allow the transfer of data in understandable and analyzable formats, the opportunity to share/sell personal data across firms becomes much broader (Lester, 2001). The first exchange in healthcare may begin at the point-of-care encounter with a clinician. Thus, all medical information captured during a visit with a primary care physician, for example, would be noted in an electronic medical record and stored and managed by the legal governing entities or business associates[2] involved with the encounter. Depending upon the encounter itself, these entities may include the patient's treating physician and his/her practice, the insurer, the pharmacy, and/or a hospital. A second exchange, on the other hand, may occur without explicit knowledge or authorization from the patient, but in many cases can still benefit them or others (Glazer, 1991; Milne and Gordon, 1993).

While most patients understand that the treating physician is rarely the only party that is privy to the patient's health information, it may be surprising how far one's information can extend. This can be a result of several things such as relationships within the terms of a business associate agreement (BAA), relationships that extend beyond the BAA, or more simply that patients are informed of possible secondary uses of their data but choose not to question the use by other parties. While BAA's are legal contracts that guide the use of Protected Health Information (PHI), it is not beyond reason that the more expansive the second exchange, the more likely that PHI or even non-protected health information could be released to parties that do not maintain stringent data use policies. Eventually the data could be linked to other large collective databases as a means of generating new information, which seems to be the greatest cause for alarm among consumers of healthcare services. The benefits to the patient of these secondary exchanges are that their medical information can be made available to multiple stakeholders involved in care, thus potentially leading to improved treatment, less duplication, greater efficiency, and possibly improved quality of care. At an even more elementary level, it would be very valuable for patients to be able to traverse among all care providers and have their medical information transmitted with them – without making a concerted effort to have paper copies generated and mailed. This streamlining would benefit both the average patient who sees multiple providers for care and people who move to different geographic locations. Further, the electronic transmission of a computer-generated prescription to a pharmacy would reduce the chance that a pharmacist would misread a poorly written prescription and provide the wrong medication or the wrong dosage. At a more complex level, a massive database of health information would allow for improved public health reporting, bioterrorism surveillance, quality monitoring, and advances in clinical trials (Brailer, 2005). The Institute of Medicine, in its report, "To Err is Human," argued that up to 98,000 deaths result from avoidable healthcare provider errors (Kohn et al., 1999). Many believe this number can be dramatically decreased with HIE.

To summarize, whenever data elements are transmitted with a variable that is common between two databases, the opportunity arises for a matchup to take place that links disparate elements from one database to another. Presumably, if a national health information network were built (see http://www.hhs.gov/healthit/healthnetwork/background/ and http://www.nhinwatch.com/), the infrastructure would be in place to provide a means for nurturing this conception of new information. The initiative to move away from silos of private information into aggregated pools of data has created a groundswell of concern from the public regarding the protection of health information. At the same time, many of us wonder about the societal good that could conceivably result from sharing our private data. To investigate this question, I first consider whether electronic health information in aggregate is a public good.

Private information as a public good

The term, "public good" has its roots in the economic literature. It has been defined in several ways but the consensus suggests that it is a good that when any group member consumes it, the good cannot be

withheld from any other member of the group (Olson, 1971, pp. 14–15). For instance, people can enjoy the city parks regardless of whether they contributed to their upkeep through local taxes, thus public goods are non-excludable: once these goods are provided, nobody can be excluded from using them. As a result, there is a temptation to enjoy the good without making a contribution. Those who do so are called free-riders, and while it is rational to free-ride, if all do so the public good is not provided and all are worse off.

The question posed here is whether health data, in a de-identified, aggregated way should be considered a public good. Intriguing analogies can be drawn to the debate about whether "science" is a public good. Callon (1994) argues that with respect to *science*, one must think of a public good not from the perspective of an economist but instead from an anthropological and sociological sense and suggests that, "science is a public good, not because of its intrinsic properties but because it is a source of diversity and flexibility." In a sense, his argument is one step removed from the more direct question of whether data, which provide the means for discovery, i.e., "science," should be made available in a public way. I would argue that lawful and transparent uses of health data provide the same opportunities for diversity and flexibility. What is somewhat different is that no particular intellectual property, be it science or art, resides within the data itself. It is only through research that a sense-making process occurs, transforming data into new, actionable information. Thus, science adds meaning and context to data, but to what extent do we agree to make the data available such that this discovery process can take place, and are the impacts of discovery great enough to justify the risks? Prior literature suggests that there is a privacy calculus (Culnan and Armstrong, 1999; Dinev and Hart, 2006) associated with a decision such as this for which there are tradeoffs. Typically, one would evaluate how important the private information is and weigh that against the return associated with giving it up. Some preliminary work by Anderson and Agarwal (2008) suggests that people will relinquish some degree of privacy if the rewards or incentives are properly aligned. Other work suggests that disclosure of personal information will occur only if the individuals believe their data will be used in a just way that does not impact them negatively in the future (Derlega et al., 1993; Thibaut and Kelley, 1959). Anecdotally, the analogy to a breach of financial data is often made here but the difference is that one cannot as easily assess the financial remuneration necessary to compensate for a breach of medical information. Adding another layer of complexity to this equation is the fact that exposure of health information may or may not lead to a negative outcome. Thus, one must assess the perceived sensitivity of the information *and* the probability that exposure of the private information could lead to some harmful event. When one knows for certain that his or her information will be fully disclosed, the decision criteria are simply a function of the probability that something harmful will occur. Thus, it would appear that responses will vary greatly with respect to whether health information is a public good and under what conditions. One of these considerations is the extent to which the stakeholders are trusted entities. While most would expect the system to be used in an ethical way by trusted stakeholders, prior research suggests that as the number of stakeholders increases, overall trust in the system declines (Gulati, 1995; Zaheer and Venkatraman, 1995). Beyond trusted entities, we know that systems are not impervious to attack from unknown entities, thus there is some reason to believe that the system cannot be completely resistant to threats.

National health information exchange: voluntary versus mandated

Beyond the question of the public good, the other concerns being voiced about a national HIE revolve around whether the system should be voluntary or mandatory and whether consumers will be given an option. There is currently a spirited debate among those in the medical profession, civil liberty groups, informaticians, and the general public surrounding the topic of opt-in versus opt-out of electronic medical record systems (Cundy and Hassey, 2006; Watson and Halamka, 2006; Wilkinson, 2006). This debate considers whether the general public should have the right to decide if their health information can be digitized and made available for various purposes in a de-identified way, or if it should be available to *only* the health provider who *created* the record, thus making it unavailable to others who can potentially treat the patient (Wilkinson, 2006). Of

course, a system like this would need to be constructed in a way that allows privacy ''controls'' at various levels including but not limited to the illness, the treatment, the type of doctor, and other aspects. Essentially, one would be able to toggle on and off what information could be viewed and by whom. Naturally this leads to the question of whether the general consumer is capable (intellectually and technologically) of making such decisions and if their choices could negatively affect their care. In addition, it is reasonable to assume that a toggle system would alert the treating physician that the patient elected not to share all data in his record. One could argue that this opens the door for a liability risk for the clinician and also indirectly violates the privacy of the patient. So, while the solution to offer a choice seems reasonable, in practice, it is mired in complexities. Policy makers in the U.S. have sought case examples from other countries regarding whether a system should be opt-in or opt-out but there is no consensus (Watson and Halamka, 2006).

One clear challenge with any voluntary system – be it a default opt-in or opt-out – is whether a disparity in care will result between those who have a complete electronic record and those who do not. While no studies have directly addressed this question, some research has suggested that technologies such as EMRs and computerized physician order entry (CPOE) contribute to fewer errors in care (Bates and Gawande, 2003). Yet, some studies have found virtually no effect or a negative effect (Ash et al., 2004; Crosson et al., 2007; Koppel et al., 2005). To the extent that benefits do result, those people who have opted-out will be disadvantaged. For example, if a patient arrives at an Emergency Department at the local hospital and refuses to provide medical information because the hospital is entirely electronic, the patient may receive substandard care. The alternative is that the hospital will have to maintain two work processes – one for electronic entry and one for paper-based entry, which is likely to lead to increased complexity.

Thus far I have described a situation in which individuals are posed with a social dilemma – provide access to personal health information or not; and legislators are tasked with an ethical decision of mandating enrollment or offering voluntary participation. In the next section, I briefly depart from this line of reasoning and draw upon information systems' literature to offer insight into the deeper question of what information privacy is.

Information privacy

Information privacy has been defined as the ability of individuals to control the terms under which their personal information is acquired and used (Culnan and Bies, 2003; Westin, 1967). Prior work suggests that people have significantly different attitudes toward the digitization and use of private information (Malhotra et al., 2004). In particular, the digitization and use of electronic personal health information has been demonstrated to evoke highly variable emotions based on such factors as involvement, argument framing, and knowledge of the technology (Angst and Agarwal, 2009). Research has also noted that this digitization creates strong feelings of vulnerability in some people and that concern for privacy varies greatly and is not singular in its interpretation (Malhotra et al., 2004). For example, secondary use, errors, unauthorized access, and collection result in different perceptions of concern in most people (Smith et al., 1996; Stewart and Segars, 2002). What is intriguing is that extant research does not explicitly draw the connection to societal good but instead focuses on *concern* for privacy and the potential benefits and costs that may accrue *to the individual*. To quote Mason, ''information forms the intellectual capital from which human beings craft their lives and secure dignity'' (1986 p. 5). Because of the tremendous importance of information, one would expect strong policies and even stronger positions to be held by people regarding the ethical use of personal information. Further, we would expect a rich body of literature that informs our understanding of the phenomenon. Yet, the ethics of information accessibility and use are an understudied topic. Mason suggests that there are four ethical issues that must be considered in this ''information age'': Privacy, Accuracy, Property, and Accessibility (PAPA). While similarities exist between PAPA and Concern For Information Privacy (CFIP) (Smith et al., 1996), the two concepts differ in the perspective from which the ideology is being viewed. For example, the CFIP work takes the position of the individual and assesses the perceptions of concern related to the organizational use of

the focal individual's personal information. It concludes that there are differing levels of concern depending upon the characteristics of the information and the way it is being used. PAPA, on the other hand, comes more from the system design perspective and suggests that developers (and their corporate representatives) should build ethical systems that address each of the four concepts of privacy, accuracy, property, and accessibility. Mason challenges society to develop social contracts between people and information systems that do not "unduly invade a person's privacy" (1986, p. 11); build systems that contain accurate information about people (or allow it to be edited if it is incorrect); assess some level of ownership not only to the data but also to the intellectual property; and finally, the systems should be designed so that they can be accessed by all people, irrespective of technological skill or literacy in general. As Mason notes, IT has enabled a greater capacity for computation, storage, and retrieval but it has also provided the means for surveillance and exploration (e.g., data mining). It stands to reason that as information becomes more private and personal, the desire for others to acquire it, for both noble and inappropriate reasons, increases.

Other researchers have introduced a multi-stakeholder perspective relative to consumer privacy such that the corporation, the activist, and the centrist hold differing and oftentimes conflicting views of privacy protection (Culnan and Bies, 2003). In the context of healthcare, the perspectives of the corporation and the activist are the most intriguing. The corporate perspective suggests that restricting the use of lawfully acquired data by corporations and their partners unnecessarily handicaps them with respect to competing in the marketplace, which ultimately results in poor performance and an inability to provide for society (Lester, 2001). Activists, on the other hand, argue that stringent controls be put in place such that technology does not engender unfettered access to data, which would violate the rights of all and result in negative social consequences (Culnan and Bies, 2003; Garfinkel et al., 2000).

While the positions of corporations and activists are interesting, the belief structures inherent within these groups may not be malleable. It is more likely that the centrists could be persuaded to embrace the perspective that health information is a public good. Centrists believe that consumers should have a voice about the uses of their personal information as governed by laws and self-regulation, but at the same time that corporations can responsibly use personal information (O'Harrow, 2001). Therefore, from a policy standpoint, it is important to craft messages that are directed toward the centrists.

Discussion

If I were to be involved in a car accident while travelling in Boston, it certainly would be to my benefit to have my medical history available to the treating physicians and absolutely critical if I had severe allergies to penicillin for example. In our current system, my medical information resides in more than five different geographic regions due to the relocations I have made over the years. Thus, I would have no confidence – nor should I – that a concise longitudinal medical report would be available to these physicians and therefore, my allergies, current prescriptions, and family history would go unnoticed. Few would argue that allowing data transmission in this context would be unlawful or unethical. On the other hand, if Joe Smith, SSN 123-45-4321 who checked into the hospital with a low HbA1C value was somehow cross-referenced with an FBI Most Wanted database and found to be a felon with a warrant for his arrest, some would argue that the information exchange would invade one's civil liberties. The irony of this situation is that the better and more complete the information in an HIE, the more useful it becomes for various stakeholders, which ultimately may lead to its demise: a classic case of the so called *Icarus Paradox* (Miller, 1990).

However, what makes the HIE more *complete*? It is only through participation of the masses that value builds, thus cooperation is critical. Prior research suggests that people will cooperate only if they expect others to act in a similar way and if they believe they will be treated fairly with respect to the give-and-take relationship to the public good (Wade-Benzoni et al., 1996). People find themselves in these types of social dilemmas when they are presented with an option that provides them with greater benefit when acting selfishly, irrespective of what other decision-makers do, than when acting in

a cooperative manner with the others (Dawes, 1980; Weber et al., 2004). In addition, if everyone acts selfishly, the affected population as a whole will receive less benefit than if a cooperative choice was made (Biel and Thøgersen, 2007; Dawes, 1980; Messick and Brewer, 1983). In the particular case of people seeing the value in HIE and voluntarily opting-in, questions remain unanswered regarding which way public perceptions will tip. If momentum is not building and power-yielding entities decide that participation in HIE should be mandated, it is conceivable that legislation will be written to enforce such a policy.

Interestingly, one aspect of HIE that has seemingly been ignored by the privacy-advocacy groups is the "paper-trail" that is left in electronic systems. If one were to unlawfully access a paper-based record of a patient, there is little the covered entity could do to find the culprit. With electronic systems, viewing, accessing, modifying, and deleting are all date- and time-stamped and tracked by some sort of identifier, be it a username and password or more generically by the computer's IP address. This inherently results in a process that allows stakeholders to monitor and control a record.

My contentions in this article rely on the assumption that digital medical information can and will be managed in a secure manner by stakeholders who are cognizant of the accepted uses of the data at the level of the consumer. While this may or may not be true or achievable in reality, this position was recently echoed by Dr. Don E. Detmer, the President of the American Medical Informatics Association. He states:

> In general, [AMIA's] positions could be characterized as "privacy moderate" as we advocated rigorous protection of PHI [Protected Health Information] and responsible data stewardship, while arguing strongly for an HIT infrastructure and policy framework that will improve health care quality, reduce costs, improve public health and facilitate research, among other purposes. (Detmer, 2009)

Conclusion

Insurance companies argue that if patients wish to retain full privacy of their medical information, they should refuse certain tests and refrain from purchasing health insurance (Borna and Avila, 1999). They contend that controlling the information after it is digitized is far more difficult than not revealing it in the first place. Further, they suggest that the insurance policy is by definition a waiver of physician–patient privilege and thus a release of privacy. While this may be somewhat of an over simplification, especially considering the complexities of Health Insurance Portability and Accountability Act (HIPAA) and covered entities,[3] the message appears to be clear that stakeholders vary in their beliefs about what information should be public and what should be private.

In and of itself, the HIE can be neither ethical or unethical, beneficial to society or detrimental; yet there are ways to design and build systems that balance the needs and desires of multiple stakeholders without infringing upon others' rights. Information system ethicists suggest that participative design is one way to improve the probability that the system will meet both goals (Mumford and Henshall, 1979). Of course, the challenge remains that peoples' beliefs about their needs and rights are heterogeneously distributed and thus difficult to determine with any certainty. Therefore, what would be most appealing to the "privacy fundamentalist" would unnecessarily restrict the choices of the "privacy unconcerned," (Harris-Interactive and Westin, 2002).

Intriguing research questions abound in this domain, not the least of which is the ethical question of whether privacy-advocacy groups are truly acting in the interest of the general public or a select group of "privacy fundamentalist" (Harris-Interactive and Westin, 2002). There appears to be a delicate balance between acting in self-interest (some might argue that self-preservation is a more accurate depiction) or acting in the interest of society as a whole. In examining the extreme case of opting-in to a genome project where entire medical histories and other personal information are made available, it would be impossible to argue that this is without risk. No one can say for certain if or how this information could be used in the future because some of its applications may not yet be conceived. Yet, all indicators seem to suggest that we are at the precipice of transformational change in the healthcare industry. It is difficult to debate the increased

control and portability of information that EMR adoption brings. While results in the health domain are somewhat mixed at this stage, IS literature suggests that having more and better information available to users will ultimately lead to better care, improved outcomes, and reduced costs. To the extent that these benefits materialize, we can expect even greater focus on issues of privacy and societal good.

In closing, several key questions come to mind which could potentially lead to future research. First, it seems logical that considerable bio-medical research could be conducted using a subset of the national population, therefore is it possible to determine when a critical mass of information is reached? To the extent that this is possible, it may not be necessary to legislate any mandatory systems if enough people volunteer information. Second, are there ways to provide controls within the system so that people can choose what information to share and what not to share? Presumably there are no technical limitations associated with providing this function, but the question then becomes whether an *incomplete* record is of value – or worse, if it provides confounding or harmful information to those who access it.

Finally, it can be assumed that a large portion of the general public is under-informed or completely unaware of this digitization movement in healthcare. Irrespective of how one feels about this activity, the population of healthcare consumers in the US has a right to be educated on the pros and cons of such a system so an informed decision can be made. Drawing one final time upon the privacy calculus described above, I leave the reader with a thought-provoking question: ''How much privacy would one be willing to give up to save one life…ten lives…one thousand lives…one million lives? What about your own life or that of your children?'' Yes, this is intentionally a very oblique perspective which loses sight of the fact that one's personal data provides only incremental (and likely miniscule) value, but it forces one to consider the broader context.

Notes

[1] See Title XIII entitled the ''Health Information Technology for Economic and Clinical Health Act'' or the ''HITECH Act''.

[2] An extensive discussion of HIPAA and business associate agreements is beyond the scope of this study. Please see http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html for more information.

[3] A covered entity is defined as a health care provider who transmits any health information in electronic form in connection with a transaction covered by the privacy rule, a health care plan, or a health care clearinghouse (see http://www.dpw.state.pa.us/About/HIPAAPrivacy/003670787.htm).

References

Anderson, C. and R. Agarwal: 2008, Boundary Risks, Affect, and Consumer Willingness to Disclose Personal Health Information. INFORMS 2008, Washington, DC.

Angst, C. M. and R. Agarwal: 2009, 'Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion', *MIS Quarterly* **33**(2), 339–370.

Ash, J. S., M. Berg and E. Coiera: 2004, 'Some Unintended Consequences of Information Technology in Health Care: The Nature of Patient Care Information System Related Errors', *Journal of the American Medical Informatics Association* **11**, 104–112.

Bates, D. W. and A. Gawande: 2003, 'Improving Safety with Information Technology', *New England Journal of Medicine* **348**, 2526–2534.

Biel, A. and J. Thøgersen: 2007, 'Activation of Social Norms in Social Dilemmas: A Review of the Evidence and Reflections on the Implications for Environmental Behaviour', *Journal of Economic Psychology* **28**(1), 93–112.

Borna, S. and S. Avila: 1999, 'Genetic Information: Consumers' Right to Privacy Versus Insurance Companies' Right to Know – a Public Opinion Survey', *Journal of Business Ethics* **19**, 355–362.

Brailer, D. J.: 2005, 'Interoperability: The Key to the Future Health Care System', *Health Affairs* (Web Exclusive), **24**(1), W5-19–W5-21.

Callon, M.: 1994, 'Is Science a Public Good?', *Science, Technology and Human Values* **19**(4), 395–424.

Crosson, J. C., P. A. Ohman-Strickland, K. A. Hahn, B. DiCicco-Bloom, E. Shaw, A. J. Orzano and B. F. Crabtree: 2007, 'Electronic Medical Records and Diabetes Quality of Care: Results from a Sample of Family Medicine Practices', *Annals of Family Medicine* **5**(3), 209–215.

Culnan, M. J. and P. K. Armstrong: 1999, 'Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation', *Organization Science* **10**(1), 104–115.

Culnan, M. J. and R. J. Bies: 2003, 'Consumer Privacy: Balancing Economic and Justice Considerations', *Journal of Social Issues* **59**(2), 323.

Culnan, M. J. and S. J. Milberg: 1998, *The Second Exchange: Managing Customer Information in Marketing Relationships* (Georgetown University, Washington, DC).

Cundy, P. R. and A. Hassey: 2006, 'To Opt in or Opt Out of Electronic Patient Records?: Isle of Wight and Scottish Projects are not Opt Out Schemes', *BMJ* **333**(7559), 146.

Dawes, R. M.: 1980, 'Social Dilemmas', *Annual Review of Psychology* **31**, 169–193.

Derlega, V. J., S. Metts, S. Petronio and S. T. Margulis: 1993, *Self-Disclosure* (Sage, Newbury Park, CA).

Detmer, D. E.: 2009, *AMIA President and CEO Summarizes AMIA's Involvement in Stimulus Package* (American Medical Informatics Association, Bethesda, MD).

Dinev, T. and P. Hart: 2006, 'An Extended Privacy Calculus Model for E-Commerce Transactions', *Information System Research* **17**(1), 61–80.

Garfinkel, S. and D. Russell: 2000, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly & Associates, Sebastopol, CA).

Glazer, R.: 1991, 'Marketing in an Information-Intensive Environment: Strategic Implications of Knowledge as an Asset', *Journal of Marketing* **55**, 1–19.

Gulati, R.: 1995, 'Does Familiarity Breed Trust? The Implications of Repeated Ties for Contractual Choices in Alliances', *Academy of Management Journal* **38**(1), 85–112.

Harmon, A.: 2008, 'The DNA Age: Taking a Peek at the Experts' Genetic Secrets', *The New York Times*, New York.

Harris-Interactive, and A. F. Westin: 2002, *The Harris Poll: #46* (Harris Interactive, New York).

Hillestad, R., J. Bigelow, A. G. Bower, F. Girosi, R. Meili, R. Scoville and R. Taylor: 2005, 'Can Electronic Medical Record Systems Transform Healthcare? An Assessment of Potential Health Benefits, Savings, and Costs', *Health Affairs* **24**(5), 1103–1117.

Kohn, L. T., J. M. Corrigan and M. Donaldson: 1999, *To Err is Human: Building a Safer Health System* (Institute of Medicine, National Academy Press, Washington, DC).

Koppel, R., J. Metlay, A. Cohen, B. Abaluck, A. R. Localio, S. E. Kimmel and B. L. Strom: 2005, 'Role of Computerized Physician Order Entry Systems in Facilitating Medication Errors', *Journal of the American Medical Association* **293**, 197–1203.

Kush, R. D., E. Helton, F. W. Rockhold and C. D. Hardison: 2008, 'Electronic Health Records, Medical Research, and the Tower of Babel', *New England Journal of Medicine* **358**(16), 1738–1740.

Lazer, D., A. Pentland, L. Adamic, S. Aral, A. Barabasi, D. Brewer, N. Christakis, N. Contractor, J. Fowler and M. Gutmann: 2009, 'Computational Social Science', *Science* **323**(5915), 721–723.

Lester, T.: 2001, 'The Reinvention of Privacy', *Atlantic Monthly* March, 27–39.

Lohr, S.: 2006, 'Smart Care via a Mouse, but What Will It Cost?', *The New York Times Online*, New York.

Malhotra, N. K., S. S. Kim and J. Agarwal: 2004, 'Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model', *Information Systems Research* **15**(4), 336–355.

Mandl, K. D. and I. S. Kohane: 2008, 'Tectonic Shifts in the Health Information Economy', *New England Journal of Medicine* **358**(16), 1732–1737.

Mason, R. O.: 1986, 'Four Ethical Issues of the Information Age', *MIS Quarterly* **10**(1), 5–12.

Messick, D. M. and M. B. Brewer: 1983, 'Solving Social Dilemmas', in L. Wheeler and P. Shaver (eds.), *Review of Personality and Social Psychology* (Sage, Beverly Hills, CA), pp. 11–44.

Miller, D.: 1990, *The Icarus Paradox: How Exceptional Companies Bring About Their Own Downfall* (Harper-Business, New York).

Milne, G. R. and M. E. Gordon: 1993, 'Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework', *Journal of Public Policy & Marketing* **12**, 206–215.

Mumford, E. and D. Henshall: 1979, *A Participative Approach to the Design of Computer Systems* (Associated Business Press, London).

O'Harrow, R.: 2001, 'Night and Day, Computers Collect Information', *The Washington Post*, Washington, DC, G10.

Olson, M.: 1971, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Harvard University Press, Boston, MA).

Pan, E., D. Johnston, J. Adler-Milstein, J. Walker and B. Middleton: 2004, *The Value of Healthcare Information Exchange and Interoperability* (Center for Information Technology Leadership, Boston, MA).

Sidorov, J.: 2006, 'It Ain't Necessarily so: The Electronic Health Record and the Unlikely Prospect of Reducing Health Care Costs', *Health Affairs* **25**(4), 1079–1085.

Smith, H. J., S. J. Milberg and S. J. Burke: 1996, 'Information Privacy: Measuring Individuals' Concerns About Organizational Practices', *MIS Quarterly* **20**(2), 167–196.

Stewart, K. A. and A. H. Segars: 2002, 'An Empirical Examination of the Concern for Information Privacy Instrument', *Information Systems Research* **13**(1), 36–49.

Thibaut, J. and H. H. Kelley: 1959, *The Social Psychology of Groups* (Wiley, New York).

Wade-Benzoni, K. A., A. E. Tenbrunsel and M. H. Bazerman: 1996, 'Egocentric Interpretations of Fairness in Environmental Asymmetric Social Dilemmas: Explaining Harvesting Behavior and the Role of Communication', *Organizational Behavior and Human Decision Processes* **67**, 111–126.

Watson, N. and J. D. Halamka: 2006, 'Patients Should have to Opt Out of National Electronic Care Records: For and Against', *BMJ* **333**(7557), 39–42.

Weber, J., S. Kopelman and D. Messick: 2004, 'A Conceptual Review of Decision Making in Social Dilemmas: Applying a Logic of Appropriateness', *Personality and Social Psychology Review* **8**(3), 281–307.

Westin, A. F.: 1967, *Privacy and Freedom* (Atheneum, New York).

Wilkinson, J.: 2006, 'What's all the Fuss About?', *BMJ* **333**(7557), 42–43.

Yasnoff, W., D. Peel, J. Pyles, D. Simborg, K. Mandl and I. Kohane: 2008, 'Shifts in Health Information', *New England Journal of Medicine* **359**(2), 209.

Zaheer, A. and N. Venkatraman: 1995, 'Relational Governance as an Interorganizational Strategy: An Empirical Test of the Role of Trust in Economic Exchange', *Strategic Management Journal* **16**(5), 373–392.

Mendoza College of Business,
University of Notre Dame,
Notre Dame, IN 46556, U.S.A.
E-mail: cangst@nd.edu