Privacy in practice: professional discourse about information control in health care

Denise L. Anthony
Department of Sociology, Dartmouth College, Hanover, New Hampshire, USA, and
Timothy Stablein
Department of Sociology, Union College, Schenectady, New York, USA

Received 31 December 2014
Revised 6 July 2015
29 August 2015
Accepted 9 September 2015

Abstract

Purpose – The purpose of this paper is to explore different health care professionals' discourse about privacy – its definition and importance in health care, and its role in their day-to-day work. Professionals' discourse about privacy reveals how new technologies and laws challenge existing practices of information control within and between professional groups in health care, with implications not only for patient privacy, but also for the role of information control in professions more generally.

Design/methodology/approach – The authors conducted in-depth, semi-structured interviews with $n = 83$ doctors, nurses, and health information professionals in two academic medical centers and one veteran's administration hospital/clinic in the Northeastern USA. Interview responses were qualitatively coded for themes and patterns across groups were identified.

Findings – The health care providers and the authors studied actively sought to uphold the protection (and control) of patient information through professional ethics and practices, as well as through the use of technologies and compliance with legal regulations. They used discourses of professionalism, as well as of law and technology, to sometimes accept and sometimes resist changes to practice required in the changing technological and legal context of health care. The authors found differences across professional groups; for some, protection of patient information is part of core professional ethics, while for others it is simply part of their occupational work, aligned with organizational interests.

Research limitations/implications – This qualitative study of physicians, nurses, and health information professionals revealed some differences in views and practices for protecting patient information in the changing technological and legal context of health care that suggest some professional groups (doctors) may be more likely to resist such changes and others (health information professionals) will actively adopt them.

Practical implications – New technologies and regulations are changing how information is used in health care delivery, challenging professional practices for the control of patient information that may change the value or meaning of medical records for different professional groups.

Originality/value – Qualitative findings suggest that professional groups in health care vary in the extent of information control they have, as well in how they view such control. Some groups may be more likely to (be able to) resist changes in the professional control of information that stem from new technologies or regulatory policies. Some professionals recognize that new IT systems

Journal of Health Organization and Management
Vol. 30 No. 2, 2016
pp. 207-226
Emerald Group Publishing Limited
1477-7266
DOI 10.1108/JHOM-12-2014-0220

and regulations challenge existing social control of information in health care, with the potential to undermine (or possibly bolster) professional self-control for some but not necessarily all occupational groups.

Keywords Information technology, Privacy, Professions, Professionalism, Health care professionals, Information control

Paper type Research paper

Introduction

Expectations of privacy and confidentiality in medical care are rooted in core professional ethical standards across a variety of health professions. For example, in each of its iterations throughout history, the Hippocratic Oath among physicians includes a commitment to protect patient confidentiality and privacy (Edelstein, 1943; Kao and Parsi, 2004). In one current version, takers of the oath state, "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know" (Miles, 2005). Nurses also have a code of ethics, the Nightingale Pledge. According to the American Nursing Association (2014), nurses pledge to "do all in my power to […] hold in confidence all personal matters committed to my keeping, and family affairs coming to my knowledge in the practice of my calling." Even newer "professional" occupations such as the American Academy of Professional Coders (2014), an organization that certifies health information specialists who work with medical records, have a code of ethics that includes protecting patient privacy and confidentiality.

While ethical codes are often defined as one of the core features of professions (Scott, 2008; Suchman and Dimick, 2010; Wilensky, 1964), ethics alone are not a sufficient indicator of professional status (Abbott, 1988). Another core feature of professions is the ability to control information (among other things) (Abbott, 1988; Freidson, 1970a, b; Larson, 1977; Parsons, 1954), so anything that might alter or challenge that control has important implications for professions: for professional relationships with clients, for intra- and inter-professional relationships, as well as for professional identity itself. For example, studies of new technologies in medical practice find they often spur inter-professional conflict, as well as challenge existing intra-professional practices and organizational routines (Barley, 1986; Koppel *et al.*, 2008; Koppel, 2013). The widespread diffusion of new information and communication technologies (ICTs) into health care creates a change in at least the way that information is managed and disseminated (e.g. Blumenthal, 2010; Canada Health Infoway, 2014; Hendy *et al.*, 2007; Institute of Medicine, 2001), which has implications for the professional control of information. Moreover, because access to information in health care depends on interactions across multiple professional groups within and across socio-technical organizations (Harrison *et al.*, 2007; Holønd, 2012), ICTs may challenge the information control of multiple professional groups, causing additional disruptions and possibilities for change. According to Suchman and Dimick (2010), "medical professionalism in the new Information age will depend not only on the medical professions' own assessment of what contributes sound and ethical IT use, but also on the inter-professional balance of power in particular sites of practice" (p. 172). Studies of professions in health care, however, typically focus on one professional group, usually doctors (Kellogg, 2011; Timmermans and Berg, 2003), and on serious medical situations (e.g. Anspach, 1993; Chiarello, 2013; Heimer and Staffen, 1998). Chiarello (2011, 2013) however shows that it is important to consider the professional and ethical aspects of mundane as well as serious medical issues to more fully understand the role of professionalism and how it is changing over time.

In this paper we explore how different types of health care professionals, including doctors, nurses, and new health information professionals, think about one specific aspect of information control in health care, protecting the privacy of patient information. We use the growing use of ICTs, such as electronic health records (EHR) systems, as well as new legal protections (in the USA) for patient information, to examine how different types of health care professionals think about patient privacy and the control of patient information in health care. We explore different professional groups' discourse about privacy – its definition and importance in health care, and its role in their day-to-day work. Here discourse is defined as the language used by different types of professionals to define and describe privacy as related to their professional work in health care delivery. Evetts (2006, p. 139) defines professional discourse as "the ways in which occupational and professional workers themselves are accepting, incorporating and accommodating the idea of 'profession' and particularly 'professionalism' in their work." We identify how the control and protection of patient information is considered part of the core ethic of some professions, while for others it is more simply part of their occupational work. Professionals' discourse about privacy also reveals how new technologies and laws challenge existing practices of information control within and between professional groups in health care, with implications not only for patient privacy but also for the role of information control in professions more generally.

Background

Professions and information control

Much of the vast literature on professions centers on the ability to interpret, define, and manipulate information within their jurisdictions (Abbott, 1988; Larson, 1977; Parsons, 1954). Such "information control" is not only a source of professional expertise, but also of professions' authority and status in client relationships, and of the ability to delineate, negotiate and protect professional and occupational boundaries (Freidson, 1970a, b; Starr, 1982; Turner, 1995). Ethical codes about how professionals use and protect client information serve to legitimize the monopoly power and social status of professions (Roberts and Dietrich, 1999). However, an alternative view argues that professional control of information is not only about power, autonomy and status, but is also integral to the trust embedded in professional-client relationships (Dingwall and King, 1995; Evetts, 2006; Parsons, 1951). According to Evetts, the rewards of power, autonomy, and status exist for professions because professionalism "*requires* professionals to be *worthy* of that trust, to put clients first, to maintain confidentiality and not use their knowledge for fraudulent purposes" (Evetts, 2006, p. 134, italics added). That is, the professional control of information, particularly client information, is as much part of the ethical values and identity of professional occupations as it is of their expertise, power, and status (Adler *et al.*, 2008). How do professional groups talk about information control as part of their profession? Does the discourse of information control differ across professional groups?

Professional control of information is also an important part of the process of becoming a professional, through the learning of codes and schema for meaningfully interpreting the "persons, events, and objects commonly encountered in the occupational world" (Van Maanen and Barley, 1984, p. 300). Such learning inculcates a strong professional identity which is itself a powerful force on behavior that can promote client trust and collaboration within the profession, but also impede communication and cause professional conflict at jurisdictional boundaries (Barley, 1986; Ferlie *et al.*, 2005). So it is not surprising that the discourse of professionalism can be used as a source of resistance to threats to a profession (Adler and Kwon, 2013; Champy, 2006; Evetts, 2006).

For example, Kellogg (2011) documents how surgeons use the discourse of professionalism to justify their resistance to new laws governing the training of residents. However, the discourse of professionalism is also sometimes used as an instrument to challenge professional control, particularly by forces outside of the profession (Fournier, 1999; Hafferty and Light, 1995). Factors that affect the professional control of information thus challenge not only the authority of the profession, but professional identity itself. How do different professional groups use discourse of professionalism to deal with changes that affect information control?

Information control, ICTs, and law

Expectations that more or better information will improve health care stem in part from the promise of new information technologies to deliver higher quality and more efficient clinical care (e.g. Blumenthal, 2010; Canada Health Infoway, 2014; Institute of Medicine, 2001; Hendy *et al.*, 2007). "Big data," that is the bringing together of vast amounts of patient, medical and genomic information to be analyzed by advanced technologies and algorithms, is expected to revolutionize health care by delivering precision and personalized medicine directly to patients (Giambrone *et al.*, 2015; Topol, 2015). Similar expectations exist throughout the industrialized world despite significant differences in health system organization and financing, as well as in definitions of key IT terminology and functionality (Adler-Milstein *et al.*, 2014; Hiller *et al.*, 2011).

The significant push for provider-centric EHR systems has been relatively recent in the USA, such as through the significant financial incentives offered via the 2009 Health Information Technology for Economic and Clinical and Health Act (HITECH) Act, but government attention and regulation has been focussed on control of patient electronic health information for nearly two decades. In 1996, the US Congress enacted legislation (the Health Insurance Portability and Accountability Act (HIPAA)) that addressed, among other provisions, the privacy and security of patients' health information. Since then, health care providers have pursued various professional and organizational strategies to accomplish compliance with regulations for managing patient information (Anthony *et al.*, 2014).

New ICTs and the potential of big data raise concerns as well as possibilities for providers, at least in part because such advances often challenge professional decision making and use of information (e.g. through clinical templates, decision-support tools) (Anderson, 2001; Dodek and Dodek, 1997; El Emam, 2013; Harrison *et al.*, 2007; Koppel, 2013). New information technologies also blur previously established social understandings and expectations of privacy because ICTs affect what, how, and to whom information is transmitted, challenging established information norms and practices (Campos-Castillo and Anthony, 2014; Nissenbaum, 2010). However, we understand little about how health care professionals think about the legal and technological changes that have created new imperatives for them, particularly for their control over patient information. Though a number of studies have analyzed the privacy concerns of patients (e.g. Campos-Castillo and Anthony, 2014; Grol *et al.*, 1999; Sankar *et al.*, 2003), few have looked at how health care professionals think about how new technologies or regulations affect their professional control of patient information. How do different professional groups in health care perceive information control in the face of new ICTs and new legal requirements to protect patient privacy?

In this study, we explore how different types of health care professionals think about and protect privacy in the practice of medical care. First, what reasons do health care providers give for protecting patient privacy and who do they think is primarily

responsible for the privacy of patient information? Second, how do they protect privacy in practice, i.e., what kinds of actions do they (not) take to ensure patient privacy while delivering health care? Third, how do recent changes, both the introduction of ICTs and new legal requirements, affect their professional control of patient information? We explore these questions to examine whether and how different professional groups in health care use the discourse of professionalism to accept, resist and/or justify changes to the control and use of patient information in health care. In the next section we describe the qualitative methods and data used in the study. Next we present our results for how different types of professionals address the three questions above, noting differences between professional groups. Finally, we discuss the implications of the findings both for different professional groups in health care, and also for information control more generally in health care.

Methods

To explore how health care professionals think about and protect privacy in practice, we conducted 83 in-depth, semi-structured interviews with doctors ($n = 30$), and nurses ($n = 32$) from three specialty groups (cardiology, primary care, and radiology) from three health care settings (two academic medical centers and one federal Veterans Affairs (VA) Hospital and Clinic), and health information staff associated with medical records and IT ($n = 21$) from the two academic medical centers, all located in the Northeastern USA (see Table I). (The timing of our study in the VA did not allow us enough time to include health information staff interviews at that site.) We selected these particular medical specialties so that we could explore the views and practices of clinicians (physicians and nurses) who have significant contact with patients for both primary and specialty (cardiology) care, as well as clinicians who have more limited contact with patients, but a great deal of contact with patient information via tests and records (radiologists). We also selected administrative staff who work directly with patient information, including medical records analysts and coders, as well as IT administrators and staff responsible for EHR systems.

The three sites provide some similarities and differences in organizational settings. Academic Medical Center 1 (AMC1) is located within ten miles of the VA Hospital and Clinic, and there is some cooperation and sharing of clinical staff across the two settings. The second academic medical center (AMC2) is in a separate state but all in the same region (Northeastern USA). All three provider organizations have an EHR system. The VA Hospital and Clinic has the oldest system, which operates nationally across all VA settings. AMC1 had a home-grown EHR system that had been in use for over ten years at the time of our interviews, though it was in preparation to transition to one of the prominent vendor-EHR systems. AMC2 had implemented a prominent vendor-EHR system approximately two years prior to the interviews.

Interviews were conducted over a period of about 18-months (AMC1 in Fall 2010, VA in Spring 2011, AMC2 in Summer 2012), during which government incentives were

	Doctors	Nurses	Medical records/coders	Total
Academic Medical Center 1	13	12	10	36
Veteran's Affairs Hospital	5	8	0	13
Academic Medical Center 2	12	12	11	35
Total	30	32	21	83

Table I. Health professionals: occupations by study sites

implemented to encourage the adoption and use of EHRs. With the permission of department heads and staff managers, we recruited participants by attending department and staff meetings, followed up by e-mail invitations to participate. Participation was voluntary and confidential. (The study was reviewed and received approval by the Dartmouth Committee for the Protection of Human Subjects to be conducted with voluntary verbal consent of respondents). Interviews with each individual respondent were approximately 40-60 minutes long. We used a structured interview guide, modified slightly for each occupational group, to ask about whether and why patient privacy is important in medical care, how they protected patient information, and who was ultimately responsible for patient privacy. We also asked how they experienced new regulations and IT systems, and how such regulations and systems affected their work generally and patient privacy specifically. All interviews were digitally voice recorded and transcribed, then coded and analyzed using Atlas.ti 7, a qualitative analysis software program. We used a modified grounded theory approach (Corbin and Strauss, 2008) that involved simultaneous data collection and analysis, synthesizing theory and data using analytic codes and memo making (Charmaz, 2006). Following an iterative process, members of the research team thematically coded samples of interview data into categorically similar interview text references and then compared code classifications. During this stage, a broad range of agreed on codes were identified in an effort to catalogue interview data into topic-driven classifications. The research team then established a final set of codes, and the remainder of the interviews were then coded by the research team and finally analyzed to elucidate patterns.

Results

Patient privacy: definitions and responsibility

We asked participants to describe what privacy is in medical care and why it is important to patients. We also asked them who they think is primarily responsible for protecting patient privacy in health care. We identified four central concepts described by respondents as important for privacy in health care (see Table II). We coded all concepts mentioned by each respondent so multiple responses were possible, though half of the physicians and about two-thirds of both nurses and administrative staff discussed only one.

Overall, more than half of all respondents cite confidentiality, an ethical belief and standard based in the long-established professional codes of medicine, nursing, and even newer occupations related to medical records and ICT, as central to the expectations of privacy of patient information in health care. Somewhat differently, about one-third of all participants define privacy as appropriate and necessary access to patient information, while about one-quarter each described privacy's importance

Table II.
What are the expectations about patient privacy in health care delivery?

Privacy concepts	Doctors ($n = 30$) (%)	Nurses ($n = 32$) (%)	Medical records/coders ($n = 21$) (%)
Confidentiality	87	47	43
Appropriate access to information	27	53	24
Use of medical records	10	22	43
Legal/patient rights	17	31	20

Note: More than one concept was identified by many participants, so columns do not add to 100 percent

related to the security and protection of medical records specifically, or as defined in legal requirements and "rights" of patients. However, some important differences can be seen across the three professional groups that reveal some different aspects of professionalism and also of how control of patient information is related to an ethic central to professional identity (doctors) vs embedded more directly in ongoing occupational work (nurses and health information staff).

The most prominent concept related to privacy described by physicians was confidentiality, or protecting (not revealing) patient information and treating patient information with respect. For example, a physician at AMC1 said simply:

> I think a patient should be able to feel confident that what I have said to him or her and what they [*sic.*] have said to me […] is going to be confidentially held in every respect.

A physician at the VA indicates not only the expectation of confidentiality but also what that means for the flow of information from the physician to any other recipient:

> My expectations are that anything the patient shares with me is confidential; that it would not be discussed by anyone who's not directly involved in the care of that patient, and that that information would not be sent anywhere outside of the facility or to another potential source without the consent of the patient.

A physician from AMC2 described confidentiality similarly, but also explained some of the consequences of it for the doctor-patient relationship:

> I think the most important thing is that the patient feels their information is secure; it's confidential and that the feeling that they get from knowing that their information is safe allows a certain level of trust where they feel now that they can share anything that they really need to share. And if they don't feel that the information is safe then one of two things happens, either they don't share the information [with me], which is dangerous, or they share it but they ask that it not go on the chart, which can also be dangerous because it means no one else has that information.

The last two quotes show how some physicians saw confidentiality related to information sharing necessary for creating a trusting doctor-patient relationship, consistent with the ethical ideals of the Hippocratic Oath and the centrality of the doctor-patient relationship in the professional identity of the medical profession. It also shows that most physicians' discourse about patient privacy encompasses the professional management and oversight of the information, not only the use of it.

Nurses also identified confidentiality as important, but typically coupled it with the idea not of professional ethics but of occupational use, specifically, the appropriate (limited) access to information, in which only those who needed specific patient information should have access to it. For example, a nurse from AMC1 put it this way:

> I think the expectation is that the information will be absolutely kept private and only available to those people that need it for what they're doing.

Another nurse at AMC1 said similarly when asked to define expectations of privacy:

> [You] don't access the information if you don't need it, if you're not involved in the patient's care.

About half of all nurses defined privacy as appropriate access to information, with one-third of them saying this was the only definition of privacy. In contrast to the physicians, this professional view by nurses does not entail a trusting relationship with patients, or the necessary information sharing between professionals, but rather one of

using patient information in the occupational work that nurses do. It also does not hint at the larger issues of information control and management or even of information flows, other than that care givers not associated with a patient's care do not access that information.

Health information staff involved in medical records and IT also identified confidentiality and appropriate access as important factors, but they were more likely than the other two groups to also define privacy as related to patient records specifically. This makes sense given that the staff we interviewed worked with patient records and so their contact with patient information was only related to contact with records. One medical records staff person at AMC1 cited confidentiality, access, and records as all part of privacy:

> [W]orking in the healthcare field really [means] being aware about keeping that patient's information confidential […]. [Y]ou're only looking at a medical record when it pertains to your job and carrying out your responsibilities of that job and not talking about any content.

Some members of each professional group described the legal or "patient rights" aspects of privacy. For example, a medical records staff person at AMC1 described privacy more narrowly related to the legal aspects only:

> I think the expectation among people in health care […] in Coding, in Administration, in Billing […] that we very strictly live and die by HIPAA [the U.S. law that defines and governs information privacy and security in health care]. It is a big deal, and it's very well respected, and everybody is very conscious of it.

Finally, one nurse from AMC1 put all four of the concepts together in her explanation of expectations about privacy in medical care:

> A patient has a right to receive medical care and have his privacy maintained. There is a federal law that addresses it. There are other laws that address it. Nursing takes an oath, doctors take an oath, so the expectation is that if you become a patient, then any information that is shared is private. It is available to people who need it to help take care of you. That could be the nurse, that could be the secretary or that could be a radiologist within that system. It should be a closed system and nothing leaves that system until the patient signs a piece of paper agreeing to allow that information to leave the system. It also should mean that within the system, we don't allow information to be exposed for people to look at who shouldn't be looking at it.

Responsibility for privacy

We asked respondents who they thought was primarily responsible for protecting patient information (see Table III). This question was open-ended, and if asked to clarify we said they could name any actor or type of actor, from specific individuals to categories/groups or institutions. The most prevalent response, particularly for nurses

Table III. Who is responsible for protecting privacy of patient information in health care delivery?

Actors responsible for privacy	Doctors ($n = 30$) (%)	Nurses ($n = 32$) (%)	Medical records/coders ($n = 21$) (%)
Providers/physicians	10	0	5
IT Staff, systems	40	3	14
Provider organization	20	9	5
Everyone in the provider organization	30	88	76

and health information staff, was that everyone in the provider organization was responsible for protecting patient privacy. Such statements generally noted that every employee, including themselves and everyone else, was and should be responsible for ensuring patient privacy. This category of "everyone" was coded separately from the relatively few respondents who said that the responsibility rests with the organization as a whole rather than with the employees within the organization. Identifying responsibility in the organization overall suggests it is the leadership rather than the members of the organization who are responsible for protecting patient privacy.

In contrast to nurses and health information staff, the most prevalent response for doctors was that the IT staff/system was the ultimate responsible party for ensuring the privacy of patient information. This response from physicians seems to be in contrast to their views that their core professional ethic of confidentiality was central to the management of patient information. Indeed only a very few doctors identified physicians/providers as having the primary responsibility for the privacy of patient information. This disconnect among physicians, between citing the centrality of the professional ethic of confidentiality for ensuring patient privacy while placing responsibility for protecting patient information on IT staff and systems, may reflect some recognition on the part of physicians that once information is embedded in complex electronic records systems, they no longer have the professional control or expertise to control it or ensure its protection.

Privacy in practice

Our next set of questions asked respondents to describe how they protected patient information and ensured privacy in their "day-to-day work in health care" (see Table IV). Note that three of the six day-to-day practices respondents described, confidentiality, records, and legal rules, are parallel to the ideals for privacy identified above (see Table II). For example, a physician at AMC1 described his practices around confidentiality as follows:

> Do I think about it [privacy] in my day to day work? Well, depends what I'm doing, but information that is disclosed to me, I don't talk about it unless I'm talking to [another provider].

Similarly, another physician at AMC1 noted that workers were expected to refrain from talking and even listening in public areas of the hospital:

> There's a certain level of deliberate oblivion in an institution, within these four walls. I put my earmuffs on and keep going […]. How much can you talk about [a patient's care] with others in order to get your job done, but protect the patient in the best way? It's that balance.

Behavior and practices related to	Doctors ($n = 30$) (%)	Nurses ($n = 32$) (%)	Medical records/coders ($n = 21$) (%)
Confidentiality	33	9	52
Interaction: spatial/personal/family	30	59	9
Records	23	22	57
Nature of work tasks	27	0	9
Technology	17	34	19
Legal (HIPAA)/organizational Rules	30	6	33

Note: More than one concept was identified by many participants, so columns do not add to 100 percent

Table IV.
How do you ensure privacy in your day-to-day work?

A health information administrator from the medical records office at AMC1 explained her practices around confidentiality this way:

> [I]t's [my] responsibility not to disclose inappropriately information from a patient's record and when I say disclose inappropriately, to different people, that means different things […] You certainly don't stand on a lunch line and be talking about it. You certainly don't stand in an elevator and be talking about somebody that you just treated […]. You're being entrusted with it [patient information]. You guard it.

In these examples, control of information via discretion in whether, where and to whom one shares patient information is how health care professionals practiced the ethic of confidentiality.

Nurses were more likely to describe privacy practices related to their direct interaction with patients, either in the clinic or on the phone. Privacy practices in the clinic typically had to do with making sure patients had a private space to disrobe and talk with care givers. Others described talking about personal matters with patients and their family members. For example, a nurse from AMC2 said:

> [When I'm] calling a patient, [first] making sure I have the correct patient that I'm speaking to. [Sometimes we] get a family member who says I can leave the information. So we can look up in the computer if there's a release [form] on file to speak with a family member. So just being careful who you're giving information out to and identifying them before you […] actually give them patient information.

A physician at AMC2 discussed privacy as confidentiality as well as privacy in the clinic environment and in the medical record:

> I think about [privacy] every day. I think about it multiple times a day […] So I think about it every time I am in the room with a patient and making sure that they understand the details about the confidentiality of the computer. I try to give them a little education about yes this is a computer system, but we can track this. I tell them that I think it [patient information in electronic records] is actually more confidential than it was in the past.

Some of the health information staff and the physicians discussed that privacy practices were related to the nature of their work tasks. For some staff who work coding information in medical records, patient privacy was protected because of how busy they were. One coder at AMC1 put it this way:

> I have to code too many individuals to be thinking about that person's business.

Similar to the practice of "not listening" to private information in the context of the physical environment of the clinic or hospital, privacy in the context of EHRs became "not reading" private information in records. Nurses explained that the expectation in a semi-private triage area with multiple computers and multiple staff was that no one would look at a computer screen if a patient record was open. Similarly, health information staff noted that they regulated how they viewed the EHR. Although any personnel authorized to enter an electronic record would gain access to all of the information in that record, nearly all said that they looked at only the parts of the record needed to do their job.

Others talked about the technical and legal issues associated with information sharing in health care delivery. For example a physician at AMC2 described her day-to-day privacy practices as follows:

> I think it's mostly got to do with some of the technicalities of information transfer, at least within the context of an EHR, so if we need records from another doctor's office or hospital

> when we're seeing a patient, it's not a great philosophical thought process, but it's a, "Hey, what do I need to do to get the information that I need? Do I need to get a release of information [form], or don't I, either formally, or informally?" So, it's sort of those kinds of mechanistic things you need to think about.

This example illustrates how the control of patient information is deeply embedded in bureaucratic rules and process rather than (or in addition to) the professional judgment of the physician.

Another physician at AMC2 discussed the fact that electronic records can be shared across care givers, which has implications not only for patient information, but also for intra-professional relationships among physicians:

> [When] patients call and say, "who would you recommend for me to see as a specialist?" Well this is a common record and everything is recorded. So, when I say I would recommend Dr A, well, Dr A can read that. Dr B can read it. Dr C can read it. In the past, I would put a message to my nurse telling him to see Dr A So you really have to think carefully about how you're going to put that because in fact Dr A, B, and C are probably all fine. You're just saying for this particular patient, Dr A would be better. It's not like Dr B and C are bad. I think you have to be careful about that.

This extended quote illuminates how technology alters not only the doctor-patient relationship, but also has implications for professional relationships among physicians. Changes in the professional control of patient information, brought about because EHR systems enable sharing the medical record across multiple practitioners, create professional boundary challenges for individual practitioners. What used to be a professional decision – which specialist to recommend to a patient – was not visible outside of the doctor-patient relationship, but now is part of an electronic record accessible by many different parties including competing specialists.

A more troubling practice that clinical providers described to "protect privacy" was to edit the content they entered into the record itself. Some providers (physicians and nurses) noted that because EHRs allowed more and different parties, including patients, to see the record, they were beginning to use vague language, and/or simplifying text in the record because they did not want to expose that information to everyone with access to the record. One radiology nurse observed:

> I'm getting vaguer and vaguer about what I write [in general notes or history] […] because it gets copied and pasted […]. Does the person who does their carpal tunnel surgery really need to know they had a breast implant?

Another physician at AMC2 said:

> Occasionally there will be cases where the patient and I discuss what is going to go on [in] the record […] Let's say they are going through a divorce and they have certain things that are really bothering them. This chart is not just for our clinic now. It can be seen anywhere by any legitimate provider and so you need to be cognizant of that more. You end up just saying "[this patient is] having some marital difficulties" and that's it. No details. That's something that just by the nature of [the record] being no longer just within our clinic that I've made some adjustments.

One consequence of limiting the information in a record this way was observed by a medical coder, who remarked:

> I think the information in the records has become a lot more vague […]. I've seen notes that said absolutely nothing about what the patient came in for, and if an outside doctor [needed] the record to follow up care, they wouldn't have a clue what the patient was seen for.

Historically, the medical record has been a tool for providers, serving as a source of information about patients and a repository of communication between providers, and of course as a tool for billing (Berg and Goorman, 1999; Timmermans and Berg, 2003). EHR alter the artifact of the medical record from primarily a clinical tool for professionals providing medical care, to a more patient friendly instrument facilitating doctor/patient communication, but also enabling organizational and other interests such as insurance billing and quality control. While patient access to medical records has many benefits, including enhanced communication with care givers (Delbanco *et al.*, 2012; Walker *et al.*, 2011), there may also be unintended consequences to changing what the records contain. Changes in the number and type of actors who can view the record, appear to be altering one of the fundamental functions of the medical record, away from a tool controlled by the professions of medicine, particularly physicians, for the inter- and intra-professional control of (the documentation, communication, and exchange of) client information, to something less valuable, at least to the profession.

When asked about how new laws governing health information affect privacy (e.g. HIPAA in the US), some explicitly stated that laws did not change anything. For example, a physician from AMC1 explained, "I just continue what I have always done [regarding patient privacy]." Similarly, a nurse at AMC2 explained, "I think you use your best judgment as a professional [regarding patient privacy]."

Others said that laws highlighted the importance of patient privacy, but did not necessarily or dramatically change any practices. One IT administrator from AMC2 noted, "I think HIPAA introduced that we have to get serious about [patient privacy]."

However, others felt that new legal regulations actually undermined existing professional ethics and practices of privacy in health care by inserting federal law over and above the professional standards that already existed. A physician at AMC1 said:

> The law [HIPAA] suggests to the patient that before this, physicians weren't respecting [privacy], and now they have to because it's the law. I think that is absolutely not accurate.

While none of those we interviewed believed that health information laws alone made privacy important in health care, some said that it caused them to change some practices. For example, nurses used only the first names of patients in waiting rooms. In large group clinics some devised specialized practices to maintain privacy. According to one nurse:

> Our [rehabilitation clinic] is open, and hospital policy is that […] you have patient privacy […]. [To] do proper patient identification […] you identify a patient by their name and date of birth, but you don't want to announce it to the whole room […]. So, we had to come up with little cards that […] has their name and date of birth on it and it's just a way for us to do patient identification without announcing to the whole room who they are.

Others said that new laws along with new technologies like EHRs affected the team-based nature of medical practice. For example, a physician from AMC2 said:

> Before HIPPA came out they used to have this big wall in the front of the ER where everybody can see it where they would put [patient] last name and chief complaint and then everybody would go up there and check off. If I wanted to sign up for [a particular] patient, I would put my initials down [next to the name] […]. It was so hard [moving to] the electronic medical record to create a secure system that protected the patient's health information but still allowed the ER staff to work as a team to share [information].

Finally, some providers simply resisted changing practices in response to new laws. For example, when communicating information across accepted channels within the hospital, one radiologist at AMC1 noted:

> We're always talking about HIPAA compliance and things like that […]. but sometimes when we page people – you can do a text page [and] type in the last name of the patient – people [got] really strict about privacy. [They say] "just enter […] the patient's number." But, I sometimes just enter the last name, and say "Could you call me about Smith? I have a chest x-ray on Smith?" thinking that's not really that identifiable. If that got intercepted by someone, they couldn't really figure out who that was […]. You might think it's a breach of confidentiality if you interpret it kind of strict I guess.

Despite being a clear violation of the law, not to mention actually putting patient confidentiality at some risk, since most patient surnames are not as generic as "Smith," this physician simply continues to follow a practice used prior to the new regulations. This is consistent with the idea of "work-arounds," using technology in unintended or disallowed ways in order to accomplish the work while (at least symbolically) maintaining privacy (Ash *et al.*, 2004; Koppel *et al.*, 2008).

In contrast, some physicians also recognized that new laws and technologies could help protect patient privacy. According to one VA physician:

> People have justifiable concerns about the privacy of their medical information. For instance, a patient of mine came to me because his sister had a stroke at a relatively young age. He had a strong family history of strokes […] so he wanted to get genetic testing done. We talked up and down about it […]. He was concerned that his insurance company would get hold of it and […] would not then cover any stroke because it was a pre-existing condition. He did the test, positive actually, so I put the little secure note on [his record].

In this case, the physician opted to use an extra technical security feature in an effort to address a patient's concerns and as a precautionary measure in case information was exposed to unintended audiences (i.e. private insurance company). It is worth noting, however, that if the patient's insurer was billed for the genetic test, as would typically be the case, they would be aware that a test was done. Insurers then may ask the patient for the results, and failure to be truthful can result in denial of insurance coverage in the USA. The 2012 Affordable Care Act in the USA, however, makes this problem somewhat moot in that insurers are no longer able to exclude pre-existing conditions from coverage.

Discussion and conclusion

Information control is central to professions. Today, professionals in health care face new technologies and new regulations that affect how they use patient information, which challenges patterns of professional control of information. In this study, we set out to explore how different professionals in health care define and describe privacy, i.e., the control and protection of patient information, as well as how they use the discourse of professionalism to discuss information control. Specifically we sought to identify how different types of health care professionals think about and protect patient privacy in the practice of medical care. In addition, we explored how recent changes, both the introduction of ICTs and new legal requirements, affect their professional control of patient information, and whether they use the discourse of professionalism to accept, resist, and/or justify changes to the control and use of patient information in health care.

The health care providers we studied actively sought to uphold the protection (and control) of patient information through professional ethics and practices, as well as through the use of technologies and compliance with legal regulations. They used

discourses of professionalism, as well as of law and technology, to sometimes accept and sometimes resist changes to practice required in the changing technological and legal context of health care. In our study, each professional group believed that patient confidentiality and information protection was important, but generally defined it in somewhat different ways, saw different groups as responsible, and "practiced" privacy somewhat differently in the course of their day-to-day work. For example, nurses, who regularly interact with patients and their families, focussed more on the interactional dynamics of protecting privacy in their occupational work. In contrast, physicians focussed primarily on the professional ethics and practices of confidentiality, while at the same time seeing responsibility for patient information privacy as resting with IT systems and staff. Alternatively, health information staff focussed more on a formal sense of privacy embedded in laws and organizational rules.

For most of the physicians, information control is deeply part of their professional identity, embedded in professional ethics and also in professional practices related to the control of inter- and intra-professional exchange of information. So changes to existing patterns of information control, particularly those via ICTs that enable broader access to patient records (e.g. by all other providers who may receive a referral, not only the referred-to provider) or those that affect communication between providers (e.g. rules about paging patient-identifying information), raise concerns for many physicians, and even resistance among some. Given the professional commitment to confidentiality voiced by most of the physicians in the study, it is somewhat surprising that most physicians seemed to abandon that commitment when asked who was responsible for protecting the privacy of patient information. However, this may reflect that physicians sense a loss of professional control over information once it is entered into complex IT systems over which they have little control or professional expertise to ensure its protection.

For nurses, the professional control of information seems to be mostly embedded in their work practices (e.g. interacting with patients directly or over the phone). Changes to those practices brought about by technology or regulations were accommodated by nurses into their work routines (e.g. information cards in group clinic settings) in ways that retain consistency with their professional identity via their occupational work. In contrast, the respondents from newer professions in information technology and records management had information control via new technologies and regulations as central to their professional identities. Indeed such things were integral to their professional discourse and illustrates a difference from the type of professional discourse espoused by physicians and even nurses. Evetts (2006) identifies such discourse as "organizational professionalism" in which the discourse of control is mostly embedded in bureaucratic structure, incorporating rational/legal decision making, hierarchical structures of authority, standardization of work practices, and accountability and performance review. Evetts (2006) contrasts this form of professional discourse with the more traditional "occupational professionalism" that is the discourse produced within a profession itself that involves discretionary decision making and occupational control of work, collegial authority, and a trusting professional-client relationship. The latter is clearly evident in the physicians' descriptions of privacy, and also to some extent in the nurses. To the extent that health information professionals' practices related to the control of client information are aligned primarily with organizational goals and interests, they are likely to come into conflict with physicians and possibly nurses. In addition, if their professional identity is embedded in the provider organizations of the hospital/clinic rather than a community

of professionals, they may undermine the value and practices of information control embedded in the professions of medicine and nursing.

The entry of new professional groups who aspire to a professional identity by embracing ethical codes of conduct and other aspects of professionalization (Suchman and Dimick, 2010) also create challenges to the control and meaning of the medical record. Because health information professionals, in contrast to physicians and nurses, are more likely to espouse "organizational professionalism" (Evetts, 2006) that is more in-line with the bureaucratic standards and decision making of the clinic or hospital organization rather than the professional obligations of service to the client, they create an intra-professional challenge to the nature of professional information control espoused by more traditional occupational professions of nursing and medicine. The changing nature of information control in health care, and the role of IT as well as state regulation in such changes, have implications not only for the clinical professions but also for health care delivery overall as newer professional groups, with different interests and professional obligations, come to play a larger role in medical care.

These differences may stem not only from different orientations to professionalism (Evetts, 2006), but also different histories of professional development and institutionalization (e.g. Crompton, 1987; Davies, 1996; Freidson, 1970b; Suchman and Dimick, 2010), as well as to differences in the nature and organizational location of medical work (e.g. Barley, 1986; Heimer and Staffen, 1998). More importantly, such differences suggest that some professional groups may be more likely to (be able to) resist changes in control over their work that stem from new technologies or regulatory policies. According to Suchman and Dimick (2010), "the health information field is becoming increasingly professionalized and […] inter-professional dynamics in the field are becoming increasingly rich, complex, and consequential" (p. 141). That is, some groups may recognize that new IT systems and new regulations challenge the existing social control of information in health care, with the potential to undermine (or alternatively, bolster) professional self-control for some, but not necessarily all, occupational groups. Such challenges may cause shifts in the extent of professional information control in some professional groups (e.g. decreased control among physicians but increased control among health information professionals) thereby shifting the balance of power, authority, or status among groups. However, changes in status or power within one professional group (e.g. physicians) are not equally distributed across all types of professionals in that group (e.g. across all specialty groups) (Barley, 1986), so future research should continue to explore how information control may change within professional groups as well as between them. Finally, challenges to or changes in information control practices within professions, brought about by technology or regulations, will likely require changes in the training of new professionals, which may ultimately alter professional identity as well.

In addition to differences between professional groups, the findings presented here also show that more generally throughout health care, practitioners are changing at least some professional practices because of technological and regulatory changes, but it is not clear what will be the implications of such changes. Changes in technology that affect professional control can disrupt not only professions and occupations, but entire organizations and institutions (Barley 1986; Harrison *et al.*, 2007; Orlikowski and Barley 2001). Early in the twentieth century, the move from treatment casebooks to patient-based case files as a mechanism of information management was both a response to, and a prerequisite for, increasing complexity in medical care (Howell 1995; Timmermans and Berg 2003). This change in complexity brought with it the emergence of new professional

groups (e.g. record librarians) and the disappearance of other actors (e.g. "low quality" surgeons and hospitals) (Howell 1995; Timmermans and Berg 2003). It remains to be seen how current changes to information control in health care may re-order not only the professions, but also the organizations and institutions throughout the delivery system.

New information technologies, such as EHR, are being widely implemented across health care (Adler-Milstein *et al.*, 2014; DesRoches *et al.*, 2010; Hsiao *et al.*, 2013). Though EHRs are expected to play a key role in improving the quality of health care in the USA and elsewhere by facilitating the flow of information, they also introduce challenges to the basic information control practices of the professional groups in health care (Halford *et al.*, 2009; Heath *et al.*, 2003; Vikkelsø 2007). Although a relative late-comer to the information age, the dramatic changes currently underway related to the gathering, management, and control of patient information are producing significant challenges for health care professionals that may transform the very nature of medical professions.

Acknowledgements

The authors thank Emily Carian, Caitlin Hackett, and Chauna Pervis for research assistance. The authors are also grateful to Mary Dixon-Woods, Jason Houle, Kathryn Lively, Emily Walton, and the participants in the 2014 Organizational Theory in Health Care conference at Northeastern University, Boston, MA.

Supported by grants CNS-0910842 from the National Science Foundation, and HHS 90TR0003/01 from US Department of Health and Human Services. The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the National Science Foundation, or US Department of Health and Human Services.

References

Abbott, A. (1988), *The System of Professions: An Essay on the Division of Expert Labor*, The University of Chicago Press, Chicago, IL.

Adler, P. and Kwon, S.W. (2013), "The mutation of professionalism as a contested diffusion process: clinical guidelines as carriers of institutional change in medicine", *Journal of Management Studies*, Vol. 50 No. 5, pp. 930-962.

Adler, P., Kwon, S.W. and Heckscher, C. (2008), "Professional work: the emergence of collaborative community", *Organization Science*, Vol. 19 No. 2, pp. 359-376.

Adler-Milstein, J., Ronchi, E., Cohen, G.R., Winn, L.A.P. and Jha, A.K. (2014), "Benchmarking health IT among OECD countries: better data for better policy", *Journal of the American Medical Informatics Association*, Vol. 21 No. 7, pp. 111-116.

American Academy of Professional Coders (2014), "Aapc Code of Ethics", available at: www.aapc.com/AboutUs/code-of-ethics.aspx (accessed June 20, 2014).

American Nurses Association (2014), "Florence Nightingale Pledge", available at: http://nursingworld.org/FunctionalMenuCategories/AboutANA/WhereWeComeFrom/FlorenceNightingalePledge.aspx (accessed June 20, 2014).

Anderson, R. (2001), "Undermining data privacy in health information", *British Medical Journal*, Vol. 322 No. 7284, pp. 442-443.

Anspach, R.R. (1993), *Deciding Who Lives: Fateful Choices in the Intensive-care Nursery*, University of California Press, Berkeley, CA.

Anthony, D.L., Appari, A. and Johnson, E.M. (2014), "Institutionalizing HIPAA compliance: organizations and competing logics in US healthcare", *Journal of Health & Social Behavior*, Vol. 55 No. 1, pp. 108-124.

Ash, J.S., Berg, M. and Coiera, E. (2004), "Some unintended consequences of information technology in health care: the nature of patient care information system-related errors", *Journal of American Medical Informatics Association*, Vol. 11 No. 11, pp. 104-112.

Barley, S.R. (1986), "Technology as an occasion for structuring: observations on CT scanners and the social order of radiology departments", *Administrative Science Quarterly*, Vol. 31 No. 1, pp. 78-108.

Berg, M. and Goorman, E. (1999), "The contextual nature of medical information", *International Journal of Medical Informatics*, Vol. 56 No. 1, pp. 51-60.

Blumenthal, D. (2010), "Launching HITECH", *New England Journal of Medicine*, Vol. 362 No. 5, pp. 382-385.

Campos-Castillo, C. and Anthony, D. (2014), "The double-edged sword of electronic health records: implications for patient disclosure", *Journal of American Medical Informatics Association*, Vol. 12 No. 17, pp. e130-e140, available at: http://jamia.oxfordjournals.org/content/jaminfo/early/2014/12/17/amiajnl-2014-002804.full.pdf

Canada Health Infoway (2014), "Opportunities for action. Strategic plan", available at: www.infoway-inforoute.ca/en/component/edocman/resources/i-infoway-i-corporate/vision/1822-opportunities-for-action-extended-version?Itemid=101 (accessed August 2015).

Champy, F. (2006), "Professional discourses under the pressure of economic values", *Current Sociology*, Vol. 54 No. 4, pp. 649-661.

Charmaz, K. (2006), *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*, Sage Publications, Thousand Oaks, CA.

Chiarello, E. (2011), "Challenging professional self-regulation: social movement influence on pharmacy rulemaking in Washington State", *Work and Occupations*, Vol. 38 No. 3, pp. 303-339.

Chiarello, E. (2013), "How organizational context affects bioethical decision-making: pharmacists' management of gatekeeping processes in retail and hospital settings", *Social Science & Medicine*, Vol. 98, pp. 319-329, available at: http://dx.doi.org/10.1016/j.socscimed.2012.11.041

Corbin, J. and Strauss, A. (2008), *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, Sage Publications, Los Angeles, CA.

Crompton, R. (1987), "Gender, status and professionalism", *Sociology*, Vol. 21 No. 4, pp. 413-428.

Davies, C. (1996), "The sociology of professions and the professions of gender", *Sociology*, Vol. 30 No. 4, pp. 661-678.

Delbanco, T., Walker, J., Bell, S.K., Darer, J.D., Elmore, J.G., Farag, N., Feldman, H.J., Mejilla, R., Ngo, L., Ralston, J.D., Ross, S.E., Trivedi, N., Vodicka, E. and Leveille, S.G. (2012), "Inviting patients to read their doctors' notes: a quasi-experimental study and a look ahead", *Annals of Internal Medicine*, Vol. 157 No. 7, pp. 461-470.

Desroches, C.M., Campbell, E.G., Vogeli, C., Zheng, J., Rao, S.R., Shields, A.E., Donelan, K., Rosenbaum, S., Bristol, S.J. and Jha, A.K. (2010), "Electronic health records' limited successes suggest more targeted uses", *Health Affairs*, Vol. 29 No. 4, pp. 639-646.

Dingwall, R. and King, M.D. (1995), "Herbert Spencer and the professions: occupational ecology reconsidered", *Sociological Theory*, Vol. 13 No. 1, pp. 14-24.

Dodek, D.Y. and Dodek, A. (1997), "From Hippocrates to Facsimile. Protecting patient confidentiality is more difficult and more important than ever before", *Canada Medical Association Journal*, Vol. 156 No. 6, pp. 847-852.

Edelstein, L. (1943), *The Hippocratic Oath, Text, Translation and Interpretation*, The Johns Hopkins Press, Baltimore, MD.

El Emam, K. (Ed.) (2013), *Risky Business: Sharing Health Data while Protecting Privacy*, Trafford Publishing, Bloomington, IN.

Evetts, J. (2006), "The sociology of professional groups", *Current Sociology*, Vol. 54 No. 1, pp. 133-143.

Ferlie, E., Fitzgerald, L., Wood, M. and Hawkins, C. (2005), "The nonspread of innovations: the mediating role of professionals", *Academy of Management Journal*, Vol. 48 No. 1, pp. 117-134.

Fournier, V. (1999), "The appeal to 'Professionalism' as a disciplinary mechanism", *Social Review*, Vol. 47 No. 2, pp. 280-307.

Freidson, E. (1970a), *Professional Dominance: The Social Structure of Medical Care*, Atherton, New York, NY.

Freidson, E. (1970b), *Profession of Medicine: A Study of The Sociology of Applied Knowledge*, Dodd, Mead, New York, NY.

Giambrone, G.P., Hemmings, H.C., Sturm, M. and Fleischut, P.M. (2015), "Information technology innovation: the power and perils of big data", *British Journal of Anaesthesiology*, June 1. doi: 10.1093/bja/aev154.

Grol, R., Wensing, M., Mainz, J., Ferreira, P., Hearnshaw, H., Hjortdahl, P., Olesen, F., Ribacke, M., Spenser, T. and Szecsenyi, J. (1999), "Patients' priorities with respect to general practise care: an international comparison", *Family Practice*, Vol. 16 No. 1, pp. 4-11.

Hafferty, F.W. and Light, D.W. (1995), "Professional dynamic and the changing nature of medical work", *Journal of Health and Social Behavior*, extra issue, pp. 135-153.

Halford, S., Obstfelder, A. and Lotherington, A.L. (2009), "Beyond implementation and resistance: how the delivery of ICT policy is reshaping healthcare", *Policy & Politics*, Vol. 37 No. 1, pp. 113-128.

Harrison, M., Koppel, R. and Bar-Lev, S. (2007), "Unintended consequences of information technologies in health care – an interactive sociotechnical analysis", *Journal of the American Medical Informatics Association*, Vol. 14 No. 5, pp. 542-549.

Heath, C., Luff, P. and Svensson, M.S. (2003), "Technology and medical practice", *Sociology of Health & Illness*, Vol. 25 No. 3, pp. 75-96.

Heimer, C. and Staffen, L.S. (1998), *For The Sake of the Children: The Social Organization of Responsibility in the Hospital and the Home*, University of Chicago Press, Chicago, IL.

Hendy, J., Fulop, N., Reeves, B.C., Hutchings, A. and Collin, S. (2007), "Implementing the NHS information technology programme: qualitative study of progress in acute trusts", *British Medical Journal*, Vol. 334 No. 7608, pp. 1360-1368. doi: 10.1136/bmj.39195.598461.551.

Hiller, J., McMullen, M.S., Chumney, W.M. and Baumer, D.L. (2011), "Privacy and security in the implementation of health information technology (electronic health records): US and EU compared", *Boston University Journal of Science & Technology Law*, Vol. 17 No. 1, pp. 1-39.

Holønd, E. (2012), "Introducing the electronic patient record (EPR) in a hospital setting: boundary work and shifting constructions of professional identities", *Sociology of Health & Illness*, Vol. 34 No. 5, pp. 761-775.

Howell, J.D. (1995), *Technology in the Hospital. Transforming Patient Care in the Early Twentieth Century*, Johns Hopkins University Press, Baltimore, MD.

Hsiao, C.-J., Jha, A.K., King, J., Patel, V., Furukawa, M.F. and Mostashari, F. (2013), "Office-based physicians are responding to incentives and assistance by adopting and using electronic health records", *Health Affairs*, Vol. 32 No. 8, pp. 1470-1477.

Institute of Medicine (2001), *Crossing the Quality Chasm. A New Health System for the 21st Century*, National Academy Press, Washington, DC.

Kao, A.C. and Parsi, K.P. (2004), "Content analyses of oaths administered at US medical schools in 2000", *Academic Medicine*, Vol. 79 No. 9, pp. 882-887.

Kellogg, K. (2011), *Challenging Operations*, University of Chicago Press, Chicago, IL.

Koppel, R. (2013), "Demanding utility from health information technology", *Annals of Internal Medicine*, Vol. 158 No. 11, pp. 845-846.

Koppel, R., Wetterneck, T., Telles, J.L. and Karsh, B.-T. (2008), "Workarounds to barcode medication administration systems: their occurrences, causes, and threats to patient safety", *Journal of the American Medical Informatics Association*, Vol. 15 No. 4, pp. 408-423.

Larson, M.S. (1977), *The Rise of Professionalism*, University of CA Press, Berkeley, CA.

Miles, S.H. (2005), *The Hippocratic Oath and the Ethics of Medicine*, Oxford University Press, New York, NY.

Nissenbaum, H. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA.

Orlikowski, W.J. and Barley, S.R. (2001), "Technology and institutions: what can research on information technology and research on organizations learn from each other?", *MIS Quarterly*, Vol. 25 No. 2, pp. 145-165.

Parsons, T. (1951), *The Social System*, Free Press, New York, NY.

Parsons, T. (1954), "The professions and social structure", *Essays in Sociological Theory*, Free Press, Glencoe Illinois, NY, pp. 34-49.

Roberts, J. and Dietrich, M. (1999), "Conceptualizing professionalism: why economics needs sociology", *American Journal of Economics and Sociology*, Vol. 58 No. 4, pp. 977-998.

Sankar, P., Moran, S., Merz, J. and Jones, N. (2003), "Patient perspective on medical confidentiality: a review of the literature", *Journal of General Internal Medicine*, Vol. 18 No. 8, pp. 659-669.

Scott, W.R. (2008), "Lords of the dance: professionals as institutional agents", *Organization Studies*, Vol. 29 No. 2, pp. 219-238.

Starr, P. (1982), *The Social Transformation of American Medicine*, Basic Books, New York, NY.

Suchman, M.C. and Dimick, M.D. (2010), "A profession of its own: the rise of health information professionals in American healthcare", in Rothman, D. and Blumenthal, D. (Eds), *Medical Professionalism in the New Information Age*, Rutgers University Press, East Rutherford, NJ, pp. 132-173.

Timmermans, S. and Berg, M. (2003), *The Gold Standard: The Challenge of Evidence-based Medicine*, Temple University Press, Philadelphia, PA.

Topol, E.J. (2015), *The Patient Will See You Now*, Basic Books, New York, NY.

Turner, B.S. (1995), *Medical Power and Social Knowledge*, SAGE Publications, London.

Van Maanen, J. and Barley, S.R. (1984), "Occupational communities: culture and control in organizations", *Research in Organizational Behavior*, Vol. 6, pp. 287-365.

Vikkelso, S. (2007), "In between curing and counting: performative effects of experiments with healthcare information infrastructure", *Financial Accountability and Management*, Vol. 23 No. 3, pp. 270-288.

Walker, J., Leveille, S.G., Ngo, L., Vodicka, E., Darer, J.D., Dhanireddy, S., Elmore, J.G., Feldman, H.J., Lichtenfeld, M.J., Oster, N., Ralston, J.D., Ross, S.E. and Delbanco, T. (2011), "Inviting patients to read their doctors' notes: patients and doctors look ahead", *Annals of Internal Medicine*, Vol. 155 No. 12, pp. 811-819.

Wilensky, H.L. (1964), "The professionalization of everyone?", *American Journal of Sociology*, Vol. 70 No. 2, pp. 137-158.

About the authors

Dr Denise L. Anthony, PhD, is Vice Provost for the Academic Initiatives, and a Professor and a past-Chair (2007-2011) in the Department of Sociology, at the Dartmouth College. She is also an Adjunct Professor in the Department of Community and Family Medicine at the Geisel School of Medicine, and a Faculty Affiliate at The Dartmouth Institute for Health Policy and Clinical Practice. Dr Anthony's work explores issues of cooperation, trust and privacy in a variety of settings, from health care delivery to micro-credit borrowing groups to online groups such as Wikipedia and Prosper.com. Her multi-disciplinary research has been funded by grants from the National Science Foundation and others, and published in sociology as well as in health policy and computer science journals, including among others the *American Sociological Review*, *Social Science and Medicine*, *Journal of the American Medical Association*, *Health Affairs*, and *IEEE Pervasive Computing*. Dr Denise L. Anthony is the corresponding author and can be contacted at: denise.anthony@dartmouth.edu

Timothy Stablein, PhD, is an Assistant Professor in the Department of Sociology at the Union College in Schenectady, New York. He received his PhD. from the University of Connecticut. His research explores the role technology plays in shaping views about health information privacy, and health information exchanges. He also researches deviant populations, and adolescent behavior, health care experiences, and health disparities. He is currently a Principal Investigator in a study supported by the Agency for Healthcare Research and Quality (AHRQ) which explores the role of electronic health records in pediatrician-adolescent patient interactions. His research has appeared in the *Journal of Contemporary Ethnography*, *Emerging Adulthood*, and *Sociological Studies of Children and Youth*.