

**Sharing is (S)caring on the Digital Frontier:
The Challenges of Information Technology Governance in
Health Care Organizations¹**

Mark C. Suchman
Department of Sociology and School of Law
University of Wisconsin - Madison
(Visiting in 2006-2007 at Cornell Law School)

February 20, 2007

Draft, February 2007: Please do not cite without permission

¹I wish to thank Karen Schaepe, Matthew Dimick and Sarah Swider for their invaluable insights and research assistance. Funding for this project has been provided by the National Science Foundation's programs in Sociology and in Law and Social Science (Grant SES-0242033), by an Investigator Award from the Robert Wood Johnson Foundation (Grant #047734), and by seed grants from the Wisconsin Alumni Research Foundation and the University of Wisconsin Center for the Demography of Health and Aging. Please address all correspondence to Mark Suchman, Department of Sociology, University of Wisconsin, 1180 Observatory Drive, Madison, WI 53706 or suchman@ssc.wisc.edu.

**Sharing is (S)caring on the Digital Frontier:
The Challenges of Information Technology Governance in
Health Care Organizations**

Abstract

Clinical information technologies such as electronic health records (EHRs) and computerized practitioner order-entry (CPOE) carry great promise for improving healthcare quality and reducing healthcare cost; however, these technologies also raise the specter of new forms of competition, control and inequality. Consequently, the fate of such systems may ultimately depend less on their technical performance characteristics than on the availability of appropriate “social governance mechanisms” -- laws, rules and norms -- to overcome ubiquitous challenges of system integration (including compatibility and comprehensiveness), system integrity (including privacy and reliability), and system control (including autonomy and transparency). To understand these dynamics, research must attend simultaneously to the economics of standardization, the sociology of trust, and the politics of accountability -- as well as to the endogenous, mutually constitutive relationship between technological, legal and organizational fields. This paper reviews the relevant conceptual issues and presents preliminary results from an ongoing multi-method study of clinical IT governance in American hospitals. Data from expert and lay interviews, ethnographic fieldwork, and a nationwide organization-level survey of hospitals suggest the presence of competing governance logics, varying both across and within hospital organizations. In this milieu, the intra-organizational politics of compliance appear to color not only the legal consciousness of hospital staff members but also the images of law that staff convey to the general public.

Recent advances in computing, telecommunication, and networking -- collectively, “information technology” (IT) -- have profoundly affected large segments of the American economy. As a general rule, the more information intensive the industry, the greater the impact of changing IT conditions. By this standard, one might expect the healthcare sector to experience the effects of new IT with particular force. Somewhat surprisingly, however, this has not been the case. In most areas of practice, advances in IT have so far only lightly touched the core of the healthcare enterprise². Even evangelists for the new technologies acknowledge that the greatest benefits of healthcare IT still lie in the future -- albeit, not quite so far in the future as to be entirely unforeseeable.

Observers of the healthcare sector have attributed the slow pace of IT adoption to a wide variety of factors, including some that are purely technical and others that are purely financial. As system capabilities improve, costs fall, and evidence of long-run savings accumulates, however, technical and financial explanations no longer seem adequate to explain the continuing reluctance of many healthcare organizations to embrace the new technologies. Rather, the primary obstacles to IT adoption seem increasingly to lie in the complex social structure of the American healthcare field, and in the ambiguities, uncertainties, and destabilizing potential of IT when grafted onto that pre-existing institutional matrix.

To build a clearer understanding of such tensions, this paper offers some early findings from an ongoing multi-method investigation of the organizational, professional and legal

²According to one recent estimate, the US lags as much as 14 years behind its OECD counterparts in the pace of clinical IT adoption (Anderson et al. 2006).

challenges surrounding the adoption of new clinical information technologies (CITs) in US hospitals³. Focal CITs include: (1) data acquisition technologies, such as telemedicine and remote out-patient monitoring; (2) data dissemination technologies, such as electronic support groups and health information websites; and, most centrally, (3) data management technologies, such as electronic health records (EHRs), computerized practitioner order-entry (CPOE), and statistical medical data-mining. Together, these technologies carry great promise for improving healthcare quality and reducing healthcare cost. However, the fate of these systems may ultimately depend less on their technical performance characteristics than on the availability of appropriate “social governance mechanisms” -- laws, rules and norms -- to overcome ubiquitous challenges of standardization, trust and accountability. For this reason, the present research focuses, in particular, on the impact of the first major piece of federal legislation designed specifically to reshape IT governance in the healthcare arena: the Health Insurance Portability and Accountability Act of 1996 (or "HIPAA"). Thus, in the most concrete terms, what follows is a preliminary empirical exploration of how American hospitals are handling patient privacy and CIT implementation in the wake of HIPAA.

The intellectual stakes in this inquiry are much higher than such a minimalist formulation might suggest, however. In just the past decade, sweeping technological, organizational, and legal changes have intersected to place central aspects of the institutional logic of American healthcare fundamentally up-for-grabs. While health-policy analysts still often speak in the language of interests and transaction costs, there is, in reality, no longer any firm ground -- no

³As this framing suggests, the study will focus primarily on *clinical* information technologies, rather than on technologies that exclusively affect hospital or insurance administration.

interests, no transactions, no cost structures that are not themselves contingent on other interests, transactions and cost structures, in a complex, circular, endogenously co-evolving ferment.

Healthcare is arguably the single most dysfunctional sector of the American economy; IT governance is arguably at once the cause and perhaps the cure for many of the sector's ills; and law is almost certainly a crucial implement in the IT-governance toolkit. But law's role here is not to regulate and facilitate a pre-existing institutional regime with established actors, fixed preferences, stable expectations, and a well-understood governance logic. Rather, law is constitutively constructing all of these elements from heterogeneous and sometimes incommensurable precursors, promising to fashion a coherent and lasting CIT regime where none existed before. No one yet knows whether that promise will come to fruition; but even (or particularly) in its present state of primordial indeterminacy, IT governance in American healthcare reveals much about law's role in "domesticating" technological and organizational change -- not only in resolving collective-action problems of opportunism and coordination, but also in resolving social-cognition problems of sensemaking and taken-for-grantedness.

The fundamental premise of this study, then, is that, as healthcare organizations make sense of such governance challenges and redefine their operations accordingly, the reciprocal dialog between policy and practice -- between "Law on the Books" and "Law in Action" -- holds the potential to reconstitute some of the bedrock assumptions of healthcare as we know it. Against this backdrop, the purpose of the present exploration is not simply to determine how American hospitals are responding to HIPAA, but also, in the process, to draw out some broader lessons about the role of law in creating and sustaining viable institutional regimes in the face of

technological innovation and social discontinuity -- not just in the healthcare sector but, by extension, in other precincts of social life as well.

This paper proceeds in four parts. Part I, below, presents the substantive focus and policy motivation for the current project. After a brief review of the well-known ills of the American healthcare system, this discussion lays out both the promise of CIT for remedying those ills and the key governance challenges (system integration, system integrity, and system control) that must be overcome if that promise is to reach fruition. Part II outlines the project's theoretical framework, linking the present research to five distinct bodies of social-scientific scholarship: Basic orienting questions come from the literature on technological innovation and diffusion; insights into the policy challenges described in Part I come from three governance literatures, respectively addressing the economics of standardization, the sociology of trust, and the politics of accountability; and predictions about the impact of legal interventions come from the literature on law and organizations. Part III reviews the project's multi-method empirical design, which blends qualitative interviews with expert and lay informants, ethnographic fieldwork in a single large hospital undergoing the HIPAA implementation process, and a quantitative survey of CIT adoption and governance in over 300 general medical and surgical hospitals nationwide. Part IV then presents some of the project's preliminary findings, focusing in particular on competing sector-level governance logics, varied organizational responses to law, differential patterns of intra-organizational decision participation, and the “radiating” effects of intra-professional compliance politics on the legal consciousness of the general public.

I. The Policy Context

The Ills of American Healthcare:

Recent years have witnessed the emergence of a remarkable consensus -- spanning virtually the entire the political spectrum -- that all is not well in American healthcare. Diagnoses, attributions, and remedies vary widely, but the shared sense of crisis has become a palpable part of the nation's political climate. Although the healthcare sector's vested interests still occasionally proclaim that American medicine is "the best in the world," fewer and fewer public figures are willing to defend the proposition that the nation's healthcare system is in a state of sustainable long-run equilibrium. Evidence to justify this pervasive unease abounds: The healthcare sector accounts for over 14% of the American economy, roughly twice the share in any other country on earth {cite}. And healthcare expenditures are escalating rapidly: At close to double the rate of consumer price inflation, the sector is growing faster than any other major segment of the economy -- and this growth rate, too, is among the highest on earth {check and cite}. Yet, more than 15% of all Americans (including over a quarter of American children) have no health insurance {cite}, and Americans report lower subjective satisfaction with their health care system -- and lower objective life expectancies -- than the citizens of many other OECD nations {cites}. By almost any cost-benefit calculation, the US healthcare system is radically underperforming its potential. Indeed, according to one recent estimate, fully 30 cents on every American healthcare dollar does nothing whatsoever to make sick people better {cite}.

Explanations for this poor performance are diverse but abundant. Some waste is clearly due to the inefficient and ineffective ways that healthcare is provided to the uninsured. And

some (probably most) is due to the administrative burdens and transaction costs of an insurance system that involves thousands of geographically dispersed payors, each with its own idiosyncratic reimbursement scheme. Finally, a third component, which has attracted much recent policy attention, is the prevalence of medical errors. According to the Institute of Medicine, preventable medical errors account for 50,000 to 100,000 deaths per year in the United States. To put this figure into context: In the month of September 2001, 3,000 people were killed by Al Qaeda, and at least 4,000 were killed by the American healthcare system -- and then, of course, the American healthcare system went on to kill another 4,000 in October, and another 4,000 in November, and so on, month after month, down to the present.

The Promise of Clinical Information Technology:

Policy prescriptions to address these failings are many and varied. But most relevant to the present topic is the rising chorus of influential voices touting CIT as a panacea for America's healthcare ills. The emerging consensus, as enunciated by the President's Information Technology Advisory Committee (2004) is that "information technology for health care delivery has enormous potential to reduce error, increase efficiency, and improve the quality of care for all Americans."

A typical scenario begins with the accumulating body of research suggesting that CIT systems -- such as electronic health records (EHRs), which replace paper charts with central computer files, and computerized practitioner order-entry systems (CPOE), which allow clinicians to specify treatments electronically rather than verbally or in handwriting -- could dramatically cut the rate of medical errors. In in-patient settings, the resulting reduction in mis-medication alone could save over 3,000 lives and \$1 billion annually (Kohn et al. 1999:27, 192

ff.). The data that these systems would generate could then be compiled through electronic data interchange (EDI) among providers, payors, and public health agencies, to create a vast and flexible national health-data network, akin to the networks that currently undergird the nation's financial system. Networking of this sort could, in turn, support further IT refinements, such as outcome-based provider scoring and e-commerce open-bidding -- ultimately generating system-wide economies that, by some recent estimates, might run as high as \$80 billion per year (Hillestad et al. 2005). If the resultant savings were then re-invested in reduced insurance rates (or in direct services for the uninsured), one might ultimately be able to achieve the healthcare “trifecta” of contained costs, enhanced quality, and expanded access (cf. Scott et al. 2000) -- all without having to take the politically-unpalatable step of moving toward a British-style national health service or a Canadian-style single-payer financing system.

While undeniably optimistic, such proposals are hardly confined to academic policy institutes or futurist think-tanks. In fact, the scenario outlined above largely mirrors the logic of the 1996 HIPAA statute, which sought to facilitate electronic claims processing as a way of mollifying insurance-industry objections to expanded coverage mandates. More recently, this vision has also motivated a remarkable strange-bedfellows alliance between conservatives such as Newt Gingrich and George Bush and liberals such as Hilary Clinton and Patrick Kennedy, who have united to call for an expanded “Health Information Infrastructure.”

The Pitfalls of Information Technology Governance:

Despite this impressive political pedigree, the American health-information infrastructure is still more an aspiration than a reality: The best empirical evidence suggests that the cornerstone technologies -- EHRs and CPOE -- are each in place at no more than 15%-25% of

the nation's hospitals (Jha et al 2006), and the kind of full-scale nationwide interconnection envisioned by the most ambitious scenarios still lies far in the future (Hillestad et al. 2005; Anderson et al. 2006). While the sheer cost of these systems is clearly a factor in the slow pace of adoption, most research finds that their return on investment is fairly high, and their payback period relatively short {cite}. Given this, much of the gap between potential and reality may reflect the fact that, while these new systems promise to improve the timeliness, accuracy, efficiency and rigor of American healthcare, they also threaten to disrupt the sector's established order, raising the specter of new forms of competition, coercion, surveillance and inequality. Consequently, implementation efforts often falter as various professions, organizations, social movements and public authorities vie for control, each pursuing its own distinctive vision of healthcare's "inherent" technical, economic, clinical and ethical "imperatives."

As an illustration, consider the case of electronic health records (EHRs): Although EHR technology has been available for several decades, less than a quarter of all healthcare providers currently have such systems in place (Chin 2001; Jha et al. 2006). In a highly mobile society, this widespread reliance on paper can have disastrous consequences, often requiring physicians to "fly blind" when treating out-of-town patients. In theory, the introduction of a uniform EHR could remedy this situation; however, in practice the organizational, professional, and regulatory hurdles have proven to be substantial. With insufficient privacy safeguards, for example, patients may resist storing health data in an easily disseminated format (Health Privacy Project 2002); yet with excessive privacy safeguards, data access could become too cumbersome to meet legitimate clinical needs. Further, to achieve its full potential, an Ehr system would require at least a modicum of standardization; but, as detailed below, standard-setting is often at odds with the workings of competitive markets. An Ehr system might also raise novel liability issues, with

the transparent flow of information across organizational boundaries sparking complex disputes over data integrity and system design. Finally, even if privacy, standardization, and reliability issues were eventually resolved, the resulting treasure trove of health data could, itself, create unprecedented turmoil (and opportunity) in the healthcare sector, by radically reconfiguring the foundations of professional expertise, public health promotion, and insurance compensation. Similar patterns of promise and pitfall extend across the entire range of CIT initiatives, from computerized practitioner order-entry to telemedicine to health information websites.

Scholarship in Science and Technology Studies suggests that the fate of these new CITs, like the fate of any innovation, will depend on economic, cultural, and political forces, as much as on design specifications and technical performance capacities. Consistent with this position, the present study explores the role of social governance mechanisms in determining the course of even the most compelling CIT innovations. Broadly speaking, “governance” refers to the ways in which individuals, organizations and societies manage interdependence and sustain cooperation in the face of vulnerability. Law is one familiar form of governance; but so, too, are professional ethics, industry standards, organizational rules, and informal norms. New CIT systems pose an array of specific issues at each of these levels. The resistance to CIT adoption, however, largely stems from the interplay of three more general and recurrent governance themes that permeate legal, industrial, organizational, and interpersonal discourses simultaneously. These themes could be labeled the challenges of “*system integration*,” “*system integrity*,” and “*system control*.” I discuss each in turn in the sections below.

System integration: “System integration” refers to the challenge of developing and enforcing standardized, inter-compatible data formats, so that information can flow more freely both

among the various IT systems in any given healthcare organization, and across the boundaries between one healthcare organization and the next. In the words of one doctor:

As more stuff is computerized, there's going to be a need to figure out how to interface information across systems. Not just across vendors within a given institution, but across institutions, possibly with different vendors. If there are standards, you can all create messages that each other can recognize. But that doesn't really exist right now. Even if everybody computerizes, if the computers can't talk to one another, we're still going to be sending paper back and forth.⁴

Currently, CIT systems employ a welter of competing data formats, as well as many non-standard site-specific variants. The magnitude of the incompatibility problem is illustrated by the fact that until 1999, Massachusetts General Hospital -- a recognized IT leader -- had five different sets of computer records just for credentialing its *own* physicians. And, of course, the problem grows exponentially across the myriad interfaces in each provider network, let alone in the healthcare sector as a whole. With no individual vendor possessing sufficient market power to impose a single *de facto* standard, any solution to the integration challenge will require substantial feats of collective coordination -- on a scale that seems virtually impossible without legal intervention. And, indeed, this is precisely what the HIPAA regime envisioned: In order to facilitate the electronic claims processing that would, in turn, produce enough savings to pay for expanded insurance, the statute's "administrative simplification provisions" mandated that healthcare data henceforth be transmitted in a single set of standardized "transaction code-sets," determined by the Department of Health and Human Services and backed by the force of law.

⁴The quotations in this section are drawn from a series of expert-informant interviews conducted by the author intermittently between 2001 and 2007. The methodology for these interviews is described in greater detail below. The quoted portions are presented without ellipses or other editorial markings, although some material has been edited to improve readability. In all cases, however, care has been taken to preserve both the substance and the tone of the original remarks. Unedited transcripts are available from the authors upon request.

System integrity: As soon as standardization removes the obstacles to data-sharing among previously incompatible IT systems, however, one encounters a new set of pitfalls, involving patient privacy and data accuracy. This second cluster of governance issues compose the challenge of “system integrity.” Here, the concern is how to channel and filter the flow of medical information, so that records only circulate to those entities that have a legitimate need to see them, and so that errors and inaccuracies don’t propagate down the data stream.

The increasing scale, specialization, and commercialization of American medicine has already largely replaced the traditional personal physician with a more anonymous and transient “care team.” The introduction of standardized records and electronic data interchange, however, opens the door to a radically deeper impersonalism, by allowing (or even encouraging) more arms-length and ad hoc relations within the care team {cite Schaepe}, and by speeding the propagation of healthcare data away from the site of production. In the utopian vision of IT advocates, this is an unalloyed good, allowing greater competition among far-flung service providers and more well-informed decision-making by providers, payors, practitioners, policy-makers and patients alike. But if patients and practitioners cannot trust the integrity of the new IT systems -- if, for example, doctors fear liability for relying on test results of unknown provenance, or if patients fear discrimination for reporting symptoms of unknown origin -- then these technologies will never be used with the kind of consistency that would be necessary in order to reap the technology’s full benefits. And, in fact, this is exactly what the drafters of HIPAA encountered: The original bill, containing data-standardization provisions alone, faced growing opposition until its sponsors agreed to add integrity-bolstering language on patient privacy and computer security.

System control: Finally, a third set of pitfalls involve challenges of “system control.” The concern here is that new information technologies may erode some of the traditional bases of autonomy, authority and exchange in the healthcare arena. Because CIT often changes how healthcare organizations receive and communicate medical information, the implementation of CIT systems creates numerous opportunities for covert monitoring, for information control and de-skilling, and for adverse selection and creative accounting. While such concerns are rarely overtly articulated in the policy literature, they surface in comments such as the following -- from a physician who is widely considered an IT *proponent* within his hospital:

You really can control what people are doing in a much more powerful way than you could before. You could always have informal rules, but computers are very good at actually implementing them. It really does feel a little bit more like Big Brother is in control of what you do. And you’re just sort of hoping that Big Brother is going to be kind and benevolent, rather than evil and wicked. The dark side that I worry about is the potential for the system to be very coercive.

Stated more generally, the healthcare system that we see today has grown up around a particular historical configuration of information asymmetries and transaction costs, and changes in those “leverage points” hold the potential to radically reconfigure medical organizations, professions, and markets, alike. Significantly, this is one set of governance challenges that HIPAA leaves largely unaddressed, and few policy-makers have yet begun to think through all the control implications of the new health information regime. Calls for more and better information appeal to our Enlightenment sensibilities, but advances in IT raise significant questions about whether the healthcare system could someday become *too* transparent: In a “better” information environment, insurers might better skim low-cost customers; HMOs might better restrict clinical discretion; doctors might better pad their track records with low-risk patients; lawyers might better construct class action suits; and consumers might better engage in

adverse selection. Ultimately, these cross-cutting impulses would presumably reach some sort of equilibrium. However, the resulting regime could look quite different from medicine as we know it today.

II. A Multi-Disciplinary Theoretical Framework

Together, the challenges of CIT governance map into five largely distinct bodies of scholarship, on innovation, standardization, trust, accountability, and organizational responses to law. At the most basic level, any investigation of new technology is, almost by definition, a study of innovation and diffusion. CITs, however, depart significantly from the conventional image of discrete inventions spreading among autonomous potential adopters. Rather, CIT developments implicate complex multilateral governance issues within an organizational environment characterized by substantial legal and regulatory activity. To understand these dynamics, research must attend not only to traditional accounts of innovation and diffusion, but also to the economics of standardization, the sociology of trust, and the politics of accountability. Moreover, analysis must consider each of these topics not only on its own, but also in light of the growing body of scholarship on the intimate, mutually-constitutive relationship between legal and organizational fields.

Innovation and Diffusion:

The literature on technological innovation and diffusion is large and diverse, with research dating back over 50 years (see, e.g., Ryan & Gross 1943, Coleman et al. 1966; Hagerstrand 1967). Work in this tradition examines both (a) the factors that determine whether

individual organizations create and/or adopt new technologies (“innovation”), and (b) the factors that determine how new technologies spread within multi-organization collectivities (“diffusion”).

On the topic of innovation, research finds that organizations innovate most readily when they possess ample resources, a substantial base of prior technical knowledge, a decentralized authority structure, and open communication channels (for reviews, see Damanpour 1991; Drazin & Schoonhoven 1996). Evidence also suggests that whereas culturally legitimate and politically unthreatening innovations generally originate from high-status players at the core of the inter-organizational network, more radical breakthroughs generally originate from more peripheral entities -- particularly from entrepreneurs spanning the “structural holes” between otherwise disconnected cliques (Menzel 1960; Burt 1992).

Not surprisingly, initial endowments, communication capacity, and network position play crucial roles in the second half of the innovation-and-diffusion agenda as well -- with what looks like innovation at the level of single firms often looking more like diffusion at the level of multi-firm collectivities (see generally Strang & Soule 1998). Reconsidered in these terms, the fate of a new technology clearly depends not only on the native adaptability of individual organizations, but also both on the capacity of particular social ties to transmit information across organizational boundaries, and on the overall pattern of ties in the interorganizational matrix. When the efficacy of a technology is uncertain and plausible alternatives abound, even technically superior innovations can vanish under the wheels of on-rushing bandwagons, unless those innovations manage to secure strong, visible and well-connected champions (Abrahamson & Rosenkopf 1993, 1997).

Healthcare has long been a popular setting for studying each half of the innovation-and-diffusion dichotomy (see e.g. Menzel 1960; Russell 1977). Thus, the present research begins with the baseline prediction that innovation and diffusion of new CITs will resemble innovation and diffusion of new technologies in other sectors -- and of non-CIT technologies in healthcare: Wealth, expertise, decentralization, and open communication should make an organization more likely to adopt any given CIT, and more likely to diffuse that CIT to surrounding organizations. Further, an organization's position in interorganizational networks should affect whether that organization will tend to lead, follow, miss, or block diffusion bandwagons.

Complementing these arguments, a more recent line of analysis examines not the causes of innovation but the consequences. Ethnographic studies -- including several in healthcare (e.g., Barley 1986; Prasad 1993) -- demonstrate that the introduction of new technology often initiates a period of intense sensemaking and restructuring, as various stakeholders try to frame and tame the ambiguities of the innovation, in order to render it cognitively tractable and pragmatically useful (Weick 1990, 1995). If similar sensemaking surrounds the introduction of new CITs, research must attend not only to when and why organizations adopt the new systems, but also to how particular groups make use of the adoption process to solidify or precipitate larger changes in organizational culture and structure. Significantly, the mutually-constitutive relationship between organizations and technology is, in this regard, quite similar to the mutually-constitutive relationship between organizations and law, described below.

Technology Governance:

As instructive as the literature on innovation and diffusion may be, it nonetheless paints a somewhat simplistic picture of the dynamics of CIT adoption. Traditional innovation and

diffusion scholarship focuses primarily on discrete technologies with relatively clear performance advantages and relatively few “external” side-effects (e.g., Ryan & Gross 1943; but see Abrahamson 1991, Strang & Macy 2001). This approach eases the analytic task, but only at the cost of obscuring potential governance issues. Most new technologies change the structure of social relations in ways that undercut established regimes for managing interdependence and for securing cooperation in the face of uncertainty, vulnerability and opportunism. As a result, technical innovations often pose substantial governance challenges, and often instigate substantial governance innovations in reaction. Of course, not all technologies are equally disruptive, and the simplifying assumptions of traditional innovation and diffusion research may represent reasonable trade-offs in studies of, for example, hybrid corn (Ryan & Gross 1943). But such simplifications hardly seem appropriate for investigations of CIT. As described above, innovations in this domain inevitably implicate complex issues of integration, integrity, and control, not only within individual organizations but throughout the healthcare sector as a whole. These governance issues reflect at least three major social dynamics -- standardization, trust, and accountability -- each with a substantial theoretical literature of its own.

The economics of standardization: The challenge of “system integration,” discussed above, is far from unique to the healthcare sector. And in other settings, this challenge has given rise to a substantial body of work on “standards competitions” (Farrell & Saloner 1985) and “dominant designs” (Tushman & Anderson 1986). This literature explores the complex dynamics that can develop when (a) the value of a technology to each adopter depends in part on interoperability with other adopters, but (b) decisions about which design to adopt are dispersed across a network of autonomous actors.

In brief, researchers have argued that the benefits of interoperability (known as “network externalities”) can generate a self-reinforcing feedback loop, in which each user’s adoption of a particular design increases the incentives for other users to adopt that design as well -- to the point where the design drives its rivals from the field and becomes “locked in” as the dominant standard (Katz & Shapiro 1985; Arthur 1989). At least three classes of benefits that may contribute to this feedback loop (see, e.g., Farrell & Saloner 1985, 1986; Katz & Shapiro 1985, 1994): First, and arguably most importantly, if a technology exhibits “direct network externalities”-- i.e., if the utility of the technology to any given user depends in part on that user’s ability to connect to other users -- then standardization can serve the salutary purpose of coordinating all users on a single technical option, maximizing the technology’s value to all. This would be the case, for example, if the standardization of electronic medical records allowed healthcare providers to transmit critical patient data to any treatment location throughout the world, wherever a need might arise. Second, standardization can also create “market-mediated network externalities,” by generating a uniform customer base for ancillary goods and services. Common examples of such benefits include expanded markets for accessories, maintenance services, and consulting -- but the class could encompass expanded resale markets and expanded R&D efforts as well. In healthcare, a particularly important variety of market-mediated externality would be the expanded customer base for data-mining services, and the resulting infrastructure for evidence-based medicine and/or provider scoring⁵. Finally, the emergence of a

⁵A more sinister aspect would be the expanded “resale market” for patient data, if standardization facilitated data interchange among insurers, employers, credit agencies, and the like.

technical standard often -- but not always -- commodifies the underlying technology, benefitting consumers by facilitating price competition among alternative suppliers.

Significantly, however, standardization carries risks as well as rewards. Standardization can, for example, shift the balance of power among competing producers and also between producers and consumers. More importantly from a societal standpoint, standardization also imposes at least two noteworthy costs on the system as a whole: The first is the cost of creating a workable standard; the second, the cost of lost diversity for those users who would have received more utility from one of the extinguished options⁶. Significantly, these two costs are inversely proportional to one another: The greater the investment in constructing a standard that satisfies all users, the smaller the number of users who will retain a strong preference for some foregone alternative.⁷

These costs and benefits make standard-setting a complicated multiple-equilibrium game. While standards competitions promise winner-take-all rewards for the victors, they also pose substantial risks of market failure, coercion and stalemate. In essence, would-be standard-setters must overcome two hurdles: The first is the challenge of mobilizing enough resources to

⁶The cost of lost diversity is a bit hard to gauge, because it depends on counterfactual assumptions about what the size of the user base for each technology *would have been*, if no standard had emerged or if the losing standard had, instead, won.

⁷An additional cost of standardization may develop over time, if network externalities discourage users from switching to a better technology that emerges at some later date (cf. Arthur 1989). Significantly, however, such “excess inertia” (Farrell & Saloner 1986) is only a “cost” when measured against an ideal world in which users could choose between the two technologies *de novo*, in the absence of network effects. In the real world, excess inertia reflects the fact that, in all periods, users are actually *better off* sticking with the shared standard than striking out on their own. This logic suggests that demonstrably sub-optimal standards will persist only when the benefits of the “better” standard are either too small or too unevenly distributed to outweigh the transaction costs of coordinating a critical mass of users all to shift at once.

construct and promote a viable entry in the standards competition; the second, the challenge of attracting enough adherents to make that entry the eventual victor. Proprietary strategies (in which the developer retains ownership of the standard and charges other adopters a licensure fee) serve the first goal quite well, but at a substantial detriment to the second; non-proprietary strategies (in which the developer releases the standard into the public domain) strike just the opposite balance. In practice, this means that proprietary standards generally originate from large oligopolists seeking to leverage an existing customer base into increased market dominance, while non-proprietary standards generally originate from second-tier oligopolists seeking to join forces in self-defense. Small firms and consumers, for their part, usually simply free-ride on these efforts, waiting for the standards-competition to resolve, rather than committing resources early and risking being stranded with an orphan technology.

Together, these considerations imply that the private sector will achieve standardization - - whether proprietary or not -- only in the presence of substantial oligopoly. Market power is, in a sense, both the lure and the threat that gives firms an incentive to play the standard-setting game. In contrast, when industry concentration is low, proprietary standards will have trouble attracting a critical mass of adherents, and non-proprietary standards will have trouble attracting an adequate level of investment. As a result, the private sector generally has difficulty separating standardization from monopolization. Either standards fail to emerge, or they emerge because the market is already oligopolistic and the stand-setters hope to make it even more so. Under these circumstances, public-sector intervention -- which substitutes state power for market power -- may be the only way to ensure that common standards and competitive markets can successfully co-exist.

CIT offers an excellent arena in which to observe these standard-setting dynamics in action. Historically, the healthcare sector's IT issues arose and were resolved locally rather than globally, and standards were few and far between. Indeed, until Medicare introduced Diagnosis Related Groups (DRGs) in the 1980s, basic clinical categories varied substantially from site to site, and to this day, standardization across medical, financial and administrative records remains limited at best, even within single organizations. In the era of paper records, such heterogeneity carried only limited disadvantages; but as computerization progresses, the value of interoperability becomes increasingly clear. By facilitating data interchange and aggregation, uniform IT standards could foster better-integrated patient care, more comprehensive system management, more empirically-informed health promotion, and more transparent quality and price competition among health care providers. For better or worse, though, the American healthcare system has so far lacked a set of private actors with enough power to impose such uniformity. To date, most standardization has involved substantial public sector leadership, and unless the provider market becomes significantly more concentrated than it is today, any future standardization seems likely to require a similar degree of public intervention as well. The EDI provisions of HIPAA are cases in point.

The present study builds on the standardization literature by examining standard-setting in midstream, from the perspective of potential users who must make difficult investment decisions in an environment of considerable uncertainty. Although existing scholarship offers numerous game-theoretic analyses of technology competitions in the abstract (and several influential histories of such competitions in the past) few researchers have directly observed organizational decision-making in the midst of an ongoing standardization battle. Moreover, the literature tends to skew toward the perspective of technology producers rather than technology

users, highlighting issues of market strategy but rarely addressing issues of adoption and implementation. By examining CIT decisions during a time of significant technological and legal change, the current project begins to explore such key variables as: (a) the signals to which users attend, in making purchasing decisions under conditions of network externality; (b) the balance that users strike between systems that are well-suited to local uses and systems that promise global compatibility; and (c) the degree to which users undercut integration by making idiosyncratic modifications to standard designs.

The sociology of trust: The challenges of healthcare IT are not, of course, purely economic. Typewriter keyboards, videocassette recording formats, and computer operating systems all pose issues of standardization, but none come freighted with much emotional, interpersonal, or sociocultural resonance. Health information, on the other hand, touches on primal human concerns about mortality, identity, stigma, competence and authority, and these concerns, in turn, implicate fundamental questions of social vulnerability and confidence. Thus, just as the challenge of system integration implicates the largely economic literature on standardization, the challenge of system integrity implicates the equally substantial sociological literature on trust.⁸ Most relevantly, work in this tradition explores the various ways in which social institutions can

⁸Although perspectives vary, a reasonable sociological definition of trust would be: *“Trust” is a taken-for-granted presumption that one’s relationship partners will behave in accordance with mutually recognized norms of conduct (whether those norms are global or local, role-based or generic), and that, when such norms leave room for interpretation, one’s partners will adopt interpretations at least as protective of one’s own interests as one would have adopted oneself.* In contrast to this sociological framing, economists often reduce trust to a rational recognition that sufficient deterrents exist to prevent one’s transaction partners from engaging in opportunistic behavior. This definition, however, denies the possibility of altruism and obscures the extent to which trust may rest on untested assumptions and social cues, rather than on careful consideration of incentives and deterrents.

foster “impersonal” trust between parties who have little immediate experience or informal reputational information on which to base decisions about one another's trustworthiness (e.g., Zucker 1986; Shapiro 1987).

The importance of trust in clinical settings has formed a central tenet of medical sociology for over 60 years (e.g., Parsons 1939). Although traditionally applied to treatment decisions, this concern extends to IT issues as well: In the examining room, physicians must trust patients to disclose intimate information, and patients must trust physicians to hold such information in confidence. At an organizational level, managers must trust physicians and patients not to waste scarce resources, and physicians and patients must trust managers not to withhold needed support. And at a systemic level, the public must trust practitioners to weed out incompetence, to guard against error, and to advance the state of the art, while practitioners must trust the public to respect medical authority, to defend medical autonomy, and to invest in medical research. Given this, one could hardly construct a meaningful account of healthcare IT without exploring how emerging technological developments may affect the sector's reservoir of trust.

As Zucker (1986) notes, trust can rest on at least three distinct bases. The first type of trust is “process-based,” grounded on local knowledge of a partner's reliability, gleaned through either first-hand experience or second-hand reputation. The second type of trust is “characteristic-based,” grounded on social markers such as ethnicity, sex, or age, that mobilize tacit assumptions about shared socialization, linked fate, or reputational exposure. The third type of trust is “institutional,” grounded on embeddedness in an impersonal system of formal institutions that either enforce desirable behavior or repair deviations or both (see also Shapiro 1987). Although much of the literature argues that process-based trust is the strongest and most compelling of the three (e.g., Granovetter 1985; Uzzi 1996), this personalistic governance

strategy is also the most difficult to maintain in a modern, mass-market society. Indeed, Shapiro (1987) goes so far as to suggest that one of the defining features of a complex economy is its ability to provide procedural norms, policing mechanisms, and insurance arrangements that solve (or at least palliate) agency concerns in the absence of more personal bases for trust.

Traditionally, American medicine has depended on all three forms of trust. When healthcare is concentrated in local communities, repeat interaction and the easy flow of reputational information create an assumption, if not a reality, of competence, ethicality and good faith. Historically, this process-based trust has drawn further reinforcement from other, more characteristic-based structures, such as ethnically-homogeneous practitioner groups, religiously-affiliated hospitals, and occupation-specific insurance funds. Institutional factors, such as licensure regimes and malpractice laws, have also played a role; however, these formal constraints have often served primarily symbolic purposes, with local social networks and characteristic-based ascriptive ties creating a buffer against such external controls even while imposing more local and informal controls of their own.

Arguably, the depersonalizing effects of urbanization, bureaucratization and geographic mobility have already strained such communal bases of trust, independently of any changes in technology. New CIT systems, however, may aggravate these strains in at least four ways. First, high-speed broadband communication promises to erase many of the proximity constraints that have, to date, kept the healthcare sector economically decentralized and geographically segmented. If service provision consequently takes on a more national (or even international) scope, first-hand experience and second-hand reputation may quickly become too dispersed to provide meaningful assurances of reliability. Second, as advances in data processing expand the administrative capacity of healthcare bureaucracies, the sheer number of practitioners and

patients affiliated with each organization may grow to the point where the last vestiges of characteristic-based solidarity are lost. Third, if disintermediation follows the course envisioned by proponents of open-market “roll-your-own” health plans, patients may lose the familiar referees -- primary care physicians, insurance agents, employee benefits officers, etc. -- who have, to some degree, provided a human face for the larger system. Finally, and perhaps most importantly, new information technologies have the potential to become a sort of one-way mirror, making detailed personal histories available to computer-savvy inquirers, while hiding this surveillance from the individuals being observed. Thus, the same technological advances that promise to enhance the scale, scope, speed and precision of medical care also threaten to vitiate the traditional, communal bases of medical trust -- perhaps to the point where many potential gains from the new technologies will be lost.⁹

Given these hazards, the long-run fate of healthcare IT may depend on the sector’s ability to build additional mechanisms of institution-based trust, to compensate for the attenuation of process-based and characteristic-based alternatives¹⁰. Such institutional governance regimes can

⁹Some observers find hope in the ability of IT to facilitate new forms of community, such as internet support groups and electronic referral systems, that transcend the traditional boundaries of geographic and social space. As beneficial as these “virtual communities” may be, however, they seem unlikely to fully counterbalance IT’s less salutary effects on process- and characteristic-based trust – at least unless augmented with new institution-based safeguards and assurances.

¹⁰In the short-run, symbolic gestures may help to preserve public confidence in the system; however, enhancing trust without strengthening the substantive bases for trust is only a temporary solution. Trust, like standardization, carries costs as well as benefits, and although no healthcare system could function without ample reserves of trust, neither could any healthcare system function if unmerited trust left participants vulnerable to incompetence and fraud. Thus, if the objective bases of trust diminish, the system’s performance is likely to suffer, whether or not participants display a corresponding decline in their subjective willingness to extend trust to one another. In the long run, fundamental changes in the social organization of healthcare require equally fundamental changes in the underlying mechanisms of trust production.

take any of several forms (cf. Shapiro 1987; Scott 1995). Most commonly, the literature discusses devices for deterring malfeasance through institutionalized *monitoring and sanctioning*. This, for example, is the strategy embodied in malpractice law and in much regulatory enforcement activity, as well as in less formalized media scrutiny. In addition, however, institutions can seek to minimize wrongdoing through *selection*, preventively weeding out actors who cannot or will not maintain adequate levels of performance. Such selection efforts blend the cautionary effects of general deterrence with the precautionary effects of specific (and often preemptive) incapacitation¹¹. Finally, institutional structures can also foster trustworthy behavior through technical and ethical *socialization*: If actors learn appropriate skills and internalize appropriate values, the likelihood of both accidental and intentional norm-violations will decline, even in the absence of external selection and enforcement efforts. In essence, each of these devices for creating institution-based trust serves, in one way or another, to move process- and/or characteristic-based trust “up” to an organizational level of analysis: In-house selection, socialization and sanctioning potentially allow healthcare organizations to construct coherent identities and reputations as *collective* actors, even in the face of increasing instability and anonymity at the level of practitioner-patient relations (Coleman 1990).¹²

¹¹It is perhaps worth noting that selection criteria are often overly stringent compared to what would be dictated by optimal deterrence. A selection regime need only reinforce the taken-for-granted assumption that certified practitioners possess expected levels of motivation and competence; the motivation and competence of those *denied* certification is of little concern.

¹²At the organizational level, sanctioning, selection and socialization may sometimes work at cross-purposes. For example, large organizational size clearly enhances reputational controls through brand formation and publicity – but, at the same time, organizational size often complicates the process of individual-level socialization and renders firms themselves impervious to many selection pressures.

Two further variants of institutionalized trust, however, operate not by reconstructing personalistic processes at an organizational level, but rather by interposing the reliability of the larger institutional system as a buffer against the unreliability of any given transaction partner (cf. Shapiro 1987: 643-645). The first such mechanism of “trust without reliability” is *compensation*: Even when actors do not fully trust one another, they may nonetheless engage in trust-like relations, if the larger institutional regime guarantees them adequate recompense, should the transaction go awry. The second such mechanism is *containment*: Even in the absence of assured reliability or full compensation, actors may nonetheless shoulder some degree of vulnerability, if the larger institutional regime promises to limit any resulting damage. Insurance provides a familiar example of the former device (Heimer 1985); bankruptcy, of the latter (Halliday & Carruthers 1998).

In the end, the sociology of trust, like the economics of standardization, implies that the fate of CIT initiatives may depend heavily on the extent and nature of public involvement. Admittedly, government is hardly the only provider of institutionalized trust – indeed, Zucker (1986) argues that institution-based trust is distinguished in part by its unique suitability for purchase and sale on a certification market. However, ultimately, any set of private trust-producing institutions must face the question of who is watching the watchers (Shapiro 1987). The state, of course, is rarely an unproblematic watcher itself; but because it operates under a different institutional logic from the private sector (Friedland & Alford 1991), it can often render assurances of openness and democratic responsiveness that private actors are ill-equipped to provide. Certainly, in the near term, consumers seem unlikely to accept any CIT governance structure that does not involve substantial elements of enforcement and reinforcement from the public sector.

The present study builds on the trust literature by examining trust-maintaining institutions in the CIT arena. Although existing scholarship has catalogued strategies for building and protecting trust, few investigations have examined how these strategies connect to other aspects of organizational culture, technology or environment. Thus, our knowledge of trust tends to be more taxonomic than causal, offering relatively few lessons about how trust affects -- and is affected by -- innovation and technological change. By examining the governance regimes that hospitals employ to ensure confidentiality and reliability during a period of significant restructuring, the current project begins to explore such issues as: (a) the relative role of sanctioning versus socialization in maintaining trustworthy behavior; (b) the relative primacy of organization-level versus societal-level protections; (c) the degree of homology between societal governance of organizations and organizational governance of individuals; and (d) the extent to which governance mechanisms are endorsed or resisted by the various groups to whom they apply (cf. Dornbusch & Scott 1975).

The Politics of Accountability: Although the politics of accountability lack a scholarly literature of comparable coherence and focus to the literatures on standardization and trust, it nonetheless forms an important third leg of the theoretical triad. Closely linked to issues of system control, accountability implicates disparate arguments from several disciplines on the material and cultural bases of autonomy, authority, responsibility, and power.

In brief, the central dynamic is this: When the success of an endeavor depends on institutionalized trust, all players have a strong interest in developing robust mechanisms for assuring one another's accountability. Yet, at the same time, each player has an opposing, sometimes equally strong interest in shifting accountability away from itself and onto others.

The resulting “blame game” elicits complex political jockeying, as the various participants seek to open and close loopholes, to control agendas and discourses, and to position themselves as champions of the collective good (cf. Vaughan 1996).

The issue of patient privacy offers a particularly salient example. Seen in light of the politics of accountability, this domain starkly counterposes standardization against trust. As long as medical records reside in unstandardized and idiosyncratic data formats, the threat to privacy is small. The technical challenges of large-scale translation and reconciliation simply outweigh the likely benefits – especially since such a herculean feat would almost certainly attract substantial publicity, much of it adverse. Only with the introduction of standardized, easily transmitted and easily aggregated records does privacy emerge as a central policy concern. Ironically, though, if privacy protections become so tight that they prevent the transmission of data across organizational boundaries, the positive network externalities that justify standardization largely evaporate. All parties might be better off with a secure system of anonymous (or consent-based) data sharing, but unless someone is willing to take responsibility for protecting the privacy and integrity of medical records as information passes across traditional administrative lines, no one has much incentive to make the technical investments that would bring this vision to fruition. Indeed, at present, privacy advocates have forestalled even the basic initial step of instituting unique and universal patient identifiers -- due to a recognition that, until someone steps forward to assume responsibility for holding patient identities in confidence, the best protection may be not to construct coherent patient identities at all.

The present study develops a more thorough and coherent portrait of such accountability battles. The existing literatures on professional, bureaucratic and institutional politics all suggest that even minor shifts in control may radically alter a sector’s fundamental organizing logic,

radically redistributing autonomy, authority, responsibility, and power. Unfortunately, these literatures stand largely independent from one another, and the subject of accountability plays only a small role in each. By developing an integrative, empirically-grounded model of the politics of accountability, the current project begins to explore the organizational and situational determinants of such issues as: (a) whether accountability is accepted as a “burden of power” or instead imposed onto disempowered scapegoats; (b) whether accountability is enforced substantively or merely enacted symbolically; and (c) whether accountability is embraced as a legitimating resource or resisted a constraining threat.

Law and Organizations:

Read together, the literatures on standardization, trust, and accountability suggest that any lasting resolution to the governance challenges surrounding CIT will almost certainly involve a substantial elements of public-sector involvement, most likely in the form of statutes, administrative regulations, and court decisions. Indeed, the passage of HIPAA and the subsequent adoption of administrative regulations governing electronic data interchange and patient privacy represent significant steps in this direction. Consequently, the present study speaks to the literature on law and organizations at least as much as it speaks to the literatures on innovation, standardization, trust, and accountability.

Recent years have witnessed a proliferation of social science research on organizational responses to legal change. Early work in this tradition generally depicted laws as imposing clear mandates, impervious to dissent and backed by compelling sanction threats. In this view, obedience and resistance are sharply distinct alternatives, each reflecting a calculated assessment of whether the expected cost of compliance outweighs the expected cost of detection and punish-

ment. Since the mid-1980s, however, all elements of this view have come under empirical critique. Informed by the “new institutionalism” in organizations theory and political science (e.g., Meyer & Rowan 1977; Powell & DiMaggio 1991; March & Olson 1989), a growing body of studies have reexamined traditional assertions about law and organizations, and have found a much more intimate and much less unilateral relationship than previous scholarship had assumed (e.g., Edelman 1990, 1992; Edelman et al. 1999; Dobbin & Sutton 1998; Kelly & Dobbin 1999).

As Suchman and Edelman (1996) put it, the materialist image of law as “explicit, authoritative and coercive” has increasingly given way to a more culturalist account of law as ambiguous, contested and largely symbolic. This reformulation begins with the observation that new legal rules are often so vague as to lack any “plain meaning,” at least until they have been tested and refined by repeated judicial, regulatory and managerial experimentation. Consequently, most laws remain hotly debated long after enactment, with competing interests and competing worldviews contending for primacy both within individual organizations and throughout larger inter-organizational fields. Although law retains substantial potential for transforming organizational life, the prevalence of ambiguity and contestation means that most legal impacts arise not through direct enforcement but through moral suasion and cognitive reframing (cf. Scott 1995). In this view, law works primarily by mobilizing a massive “sensemaking” effort (cf. Weick 19{??}) within the affected industry itself, creating a new, more legalized discourse, in which various groups and professions are symbolically empowered to enunciate novel, sometimes critical, understandings of previously taken-for-granted organizational structures and practices.

The present study builds on this conceptual foundation in several ways. As described below, HIPAA's early trajectory fits institutionalist predictions remarkably well. Riddled with

ambiguity, continually under reconsideration, and lacking any enforcement budget, the proposed regulations seem to be working primarily by forcing healthcare providers to consciously examine the policy implications of previously taken-for-granted beliefs and practices, creating discursive space for new arguments, new logics and new understandings. The HIPAA experience, however, also suggests some areas in which the institutionalist literature might benefit from further refinement. To date, most studies of law and organizations have used retrospective designs, have focused on the highly antagonistic world of employment relations, and have assumed that targeted organizations generally view legal intervention as an unwanted intrusion. In contrast, the current project arrived in the earliest days of the compliance process; it focused on a field with substantial elements of positive-sum cooperation; and it encompassed legal initiatives (particularly with regard to EDI) that enjoy powerful in-house constituencies. Consequently, it can begin to illuminate such under-studied dynamics as: (a) the rhetorical deployment of law in internecine conflicts between competing organizational subcultures, (b) the differentiation of targeted organizations into sub-populations of normatively-motivated leaders, mimetically-motivated followers, and coercively-motivated stragglers (cf. DiMaggio & Powell 1983), and (c) the differential translation of legal principles into substantive and symbolic organizational practices among each of these three groups.

III. A Multi-Method Research Design

Despite their many strengths, previous studies of innovation, technology governance and law have generally employed single-wave, single-method designs that are ill-suited to addressing issues of sensemaking and cultural change. In contrast, the present investigation takes the need

for early observation as its cornerstone, and it draws on multiple, complimentary research methods to capture the multi-faceted, multi-level complexity of the CIT governance process.

Design Overview:

The findings reported here represent the preliminary results of an ongoing research program, which began in late 2000 at roughly the time of the initial administrative rulemaking under HIPAA. The research has spanned the entire initial HIPAA implementation period, including intensive fieldwork during the two years surrounding the April 2003 privacy compliance deadline. As a whole, the research program is proceeding in three stages:

The first stage employed open-ended exploratory interviews with healthcare experts and practitioners (along with limited field observations), in order to identify CIT governance challenges that were likely to emerge in the following 3 to 5 years.

The second stage, which is still actively underway, traces the evolution of CIT practices and beliefs during the introduction of the HIPAA regulations on EDI and privacy. This stage incorporates both qualitative and quantitative components, coupling: (a) intensive field observations in a large teaching and research hospital, with (b) a stratified random-sample survey of hospitals nationwide, and (c) open-ended field interviews with a sample of lay-people in two metropolitan regions.

The third stage, several years in the future (and, therefore, beyond the scope of the current paper), will measure the long-run impact of the HIPAA regulations and will monitor subsequent technological, organizational and legal developments. Through intermittent replications of stages 1 and 2 (exploratory interviews, followed by surveys and case studies) this future research will track CIT governance over time, as today's initiatives become institutionalized (or abandoned) and as tomorrow's challenges emerge. In this prospective endeavor, the current research will serve as an empirical baseline, allowing subsequent developments to be placed into longitudinal context

Methods and Procedures:

This section describes the methodology of the four primary data-gathering enterprises conducted (or under way) to date -- the expert-informant interviews, the ethnographic fieldwork, the hospital survey, and the lay-informant interviews.

Expert-informant interviews: The research project began with a preliminary round of qualitative fieldwork in Spring and Summer 2001, with the goal of identifying the central governance challenges posed by new CITs in the American healthcare system. This exploratory work continued at a reduced pace thereafter, to track developments as they unfolded.

The initial fieldwork examined a wide range of technological trends, management practices and policy dilemmas, around which legislation, regulation or case law might coalesce. Data-gathering centered on open-ended interviews with healthcare practitioners, managers, attorneys and consultants. Interviews addressed both specific CIT practices within the informant's own experience and also more general CIT trends in the healthcare sector as a whole. Interviews delved in depth into whichever CIT governance issues the informant deemed particularly important and/or particularly likely to spark legal intervention. On these topics, questioning explored current organizational practices, possible future legal changes, and possible subsequent organizational responses. To supplement these interviews, the research team also conducted several on-site observations of CIT operations and attended a major HIPAA training conference and number of other more policy-focused CIT events. All interviews were tape-recorded and transcribed, and the resulting transcripts and fieldnotes are currently being indexed and coded for analysis using the computer-assisted qualitative data analysis software, *nVivo 7*.

Qualitative fieldwork: Technology governance is a complex and interactive process. Members of the organization must make sense both of changing technologies and of changing governance principles, and the resulting understandings must be incorporated into new work practices -- which must mesh, in turn, with established organizational routines. Given this complexity, a full understanding of governance change requires first-hand, real-time field observation, to capture the longitudinal dynamics of sensemaking, policy formation, and socialization -- as well as reaction and resistance. Although no single organization can illustrate every facet of IT governance, careful ethnography can help to reveal the central human realities of technological standard-setting, institutional trust, and legal compliance, enriching the relatively abstract accounts offered by prior theoretical and statistical work.

To this end, from 2002 through 2004, the project team observed the HIPAA assessment and implementation process in a 500-bed teaching hospital, to develop an ethnographic understanding of how a particular healthcare organization underwent the process of becoming “HIPAA compliant.” Although the field site was a state-of-the-art tertiary-care medical center, its CIT operations were well within the range of normal variation for US hospitals. During the observation period, the facility employed a fairly extensive electronic health record system, but had yet to deploy computerized practitioner order entry. Moreover, when the field observations began in mid-2002, the hospital's HIPAA implementation efforts were still largely in the planning stage, with full compliance not expected (and not achieved) until shortly before the 2003 deadlines.

The qualitative fieldwork was open-ended and ethnographic in nature, with both the principal investigator and a senior research assistant¹³ spending significant amounts of time observing hospital activities and talking with hospital staff. In all, the research team conducted over 100 hours of non-participant observation in Privacy and Security policy-planning meetings and training sessions, as well as several “walk-alongs” with the hospital Privacy Officer, as she toured various wards and clinics. These passive observations were supplemented by open-ended interviews with most of the relevant decision-makers in the hospital, as well as by a more limited number of interviews with front-line doctors and nurses. To facilitate comparisons across researchers, across field settings, and over time, all fieldnotes and interviews were fully transcribed and are currently being indexed and coded for analysis in *nVivo 7*.

Quantitative survey: As informative as ethnographic evidence may be, one should nonetheless read it in conjunction with other, more broadly-based data, in order to judge its representativeness and assess its systemic implications. To address this need, the current project couples the single-site ethnography described above with a quantitative survey of hospitals nationwide.

The survey comprises 320 hospitals, selected according to a multi-level stratified random-sample design. To capture the effect of variations in state and federal law, hospitals are drawn from 16 states, two in each of 8 Federal Circuit Court jurisdictions¹⁴. Across Federal

¹³The hospital ethnography was initiated by the PI. However, once initial access to the field site had been obtained, the majority of observations were conducted by Karen Schaepe, an advanced graduate student on the project. The findings reported below incorporate original insights from both researchers, working in collaboration.

¹⁴Although national in scope, HIPAA can be superceded by state law and colored by circuit-level precedent. The survey design exploits this variability to examine legal impact (cf. Guthrie & Roth 1999).

Circuits, states are paired on the basis of socio-economic similarity, as depicted in Table 1. The goal is to tap a wide range of variation in organizational characteristics and market conditions, as well as in the legal environments that the hospitals face.

Table 1: States Sampled								
	North Industrial	North Rural	South Industrial	South Rural	Border	Coastal Cosmopolitan	Suburban	Retirement
2nd						NY	CT	
4th				SC			MD	
5th			TX	MS				
6th	MI				TN			
7th	IL	WI						
8th		MN			MO			
9th						CA		AZ
11th			GA					FL

Although the basic unit of analysis is the hospital, the survey gathers data from two individual respondents within each organization: The Chief Information Officer and the HIPAA Privacy Officer. Separate questionnaires record organizational policies and practices within each representative's purview and gauge each representative's attitudes and beliefs -- as well as each representative's perception of prevailing organizational culture -- on key CIT governance issues. While this data collection strategy admittedly privileges the views of top decision-makers, it substantially improves upon prior organization-level studies of innovation and legal compliance, by allowing for internal heterogeneity within the leadership team. Results from

these interviews are recorded in a format that allows aggregation to the hospital level for most analyses, while preserving the possibility of disaggregated individual-level analysis where appropriate.

Substantively, the survey focuses on four broad classes of data:

IT Practices: The survey collects event-history data on the implementation of several key CITs, with a particular focus on electronic medical records and computerized practitioner order-entry. When a particular technology is present, the survey inquires about various governance-related “best practices,” such as standardization of data formats, adoption of data-sharing guidelines, enforcement of privacy policies, and maintenance of electronic audit trails.

Organizational Culture: Beyond recording objective policies and practices, the survey also employs pre-existing and newly developed attitudinal scales to tap subjective aspects of organizational culture that bear on IT governance. For example, to gauge “technology culture,” the survey includes items on the perceived purposes of key technologies (e.g., access, quality, efficiency, etc.), and on the perceived consequences of those technologies for professionalism (e.g., autonomy, authority, expertise, collegiality, etc.). To gauge “legal culture,” the survey asks about interpretations of legal mandates, acceptance of legal definitions, perceptions of legal threats, and beliefs about whether legal requirements impede or promote sound medical care. Finally, the survey also measures more general attitudes toward patients, colleagues, professional bodies, and the state.

Relational Networks: As possible determinants of both practice and culture, the survey examines intra- and inter-organizational information flows and exchange patterns. Among other things, respondents are asked about internal decision-making and external benchmarking on issues of both technology and law. Other items gauge the level of social capital (social interconnection) both within each hospital and between the hospital and the larger community.

Structural Characteristics: The survey also incorporates an array of traditional measures of organizational and environmental structure. Key organizational concerns include age, size, bureaucratization, ownership structure, and mission of the hospital, while key environmental concerns include market competition, population demography, payer mix, and political climate in the surrounding community. In addition, the survey gauges the power of various internal and external stakeholder groups within the organizational coalition, both through direct reports and through items on the composition of the IT decision-making team and the professional background of the CIO and the HIPAA Privacy Officer.

Lay-informant interviews: The final component of the project is a series of qualitative interviews with lay-people in two metropolitan areas -- Madison, Wisconsin, and Philadelphia, Pennsylvania. Like the expert-informant interviews described above, these lay interviews are largely exploratory in nature. Their primary purpose is to complement the other three components of the project, which focus on the experiences of healthcare insiders, by instead examining CIT from the patient's perspective.

The design for this part of the study involved contacting a random sample of the general population and administering both a brief fixed-response quantitative questionnaire and, if the respondents were willing, a longer in-depth qualitative interview. The interview protocol covered four broad topic areas: (1) general impressions of medical information, including how it is collected and handled, when it is or is not shared, and who should or should not have access; (2) perspectives and experiences with the shift to computerization of medical information; (3) issues surrounding confidentiality, privacy, and trust; and (4) laws governing medical privacy and confidentiality (including HIPAA).

Between October 2005 and August 2006, we completed 92 fixed-response surveys and 46 in-depth interviews. At 64%, the survey response rate was roughly in line with other studies using similar techniques, and although fewer participants agreed to a subsequent in-depth interview, the demographics of the interviewees and the survey respondents showed no significant divergences. Both groups closely approximated the composition of the focal metropolitan areas in gender, age, socio-economic status and insurance coverage -- although, for Madison, this implied a significantly higher SES and a significantly lower uninsurance rate than the national average. Thus, while the results from these lay-informant interviews may not be statistically representative of the nation as a whole, the risk of non-response bias seems relatively

low. The respondents' views and experiences are likely to be fairly representative of the communities from which the sample was drawn.

IV. Preliminary Findings

Given that all four components of the empirical design are currently still either in the field or in the earliest stages of data analysis, any attempt to draw definitive or sweeping conclusions would be premature. Nonetheless, some suggestive preliminary patterns are beginning to emerge, and although these results are tentative at best, they offer intriguing clues about both the empirical path of CIT governance in the wake of HIPAA and the theoretical relevance of the project's motivating conceptual frameworks. This section briefly reviews the most salient of these provisional findings.

Conceptual Validation:

At the most basic level, the preliminary evidence provides fairly consistent validation for the project's general conceptual framework: The challenges of system integration, system integrity, and system control appear to be both empirically prevalent and cognitively salient to subjects in all four components of the research design. As the quotations earlier in this paper indicate, the themes of integration, integrity and control show up repeatedly in the literature and in our expert-informant interviews. These same themes also manifested themselves in many of our fieldwork observations, and they struck a chord with our survey pre-testers. Admittedly, the technical aspects of these governance challenges are less visible to our lay interviewees; but even here, privacy concerns, at least, lurk just below the surface. Indeed, although lay

respondents almost always begin by professing that they have no concerns and no troubles with the handling of their medical information, many then proceed, during the course of the interview, to recount

a range of horror stories, some almost certainly legally actionable. Thus, although lay “legal consciousness” in this area is not (yet) particularly legalized, the governance challenges that might motivate legal intervention seem to be commonly experienced and widely perceived, albeit not always explicitly named.

The preliminary evidence also provides substantial validation for the law and organizations literature's account of legal impact. As this tradition would predict, HIPAA's impact has been neither explicit, authoritative, nor coercive: Rather than being explicit, the regulations are hugely ambiguous. In fact, entire listservers are devoted simply to trying to parse what the new rules mean. Rather than being authoritative, HIPAA remained fundamentally contested for years after its passage, and many of the same political fights that surrounded the original legislation continued into the rule-making stage and beyond. And rather than being coercive, the legislation currently has few effective teeth. Although the penalties for privacy violations look stiff on paper,¹⁵ Congress has appropriated no money for regulatory enforcement activity, and the statute explicitly disallows private causes of action. Yet despite -- or really because of -- this ambiguity, contestation and non-coercive symbolism, HIPAA has, in fact, mobilized quite a bit of “sensemaking” activity within the healthcare community. Uncertain as it is, HIPAA forces healthcare providers consciously to examine the policy implications of previously taken-for-granted beliefs and practices, creating discursive space for new arguments,

¹⁵Section 1177, for example, establishes penalties of up to \$250,000 and ten years imprisonment for a commercial or malicious violation of health privacy.

new logics and new understandings. And, as described below, this sensemaking activity does seem to be slowly realigning how at least some healthcare professionals understand their jobs.

Alternative Governance Logics:

The preliminary evidence is also beginning to paint a clearer picture of how the institutional logic of health information governance may be shifting. Tacit in our interviews and our fieldnotes are at least five alternative metaphors for thinking about (and governing) medical records: The oldest metaphor is that medical records are clinical memos among practitioners, professional work notes to be governed by principles of ethics, comity, and discretion. In this view, the medical community has the primary claim to the record, and all others (including the patient) are at best third-party beneficiaries. A second longstanding metaphor is that medical records are the administrative files of the healthcare organization, bureaucratic archives to be governed by principles of executive authority, routinization, centralization and hierarchical control. A third more recent (but related) metaphor is that medical records are economic commodities, commercializable information to be governed by principles of market exchange and competition. A fourth metaphor is that medical records are patients' intimate documents, personal possessions to be governed by principles of individual privacy and informed consent. Finally, a fifth still emerging metaphor is that medical records are public health resources, communal data repositories to be governed by principles of public accountability and the common good.

Needless to say, these metaphors do not always co-exist happily, and one way to understand the significance of HIPAA is as a fledgling attempt to intercede in the resulting tug-of-war among competing governance logics. In particular, HIPAA symbolically embraces and

in a faltering way attempts to reconcile the logics of individual privacy and public health, while symbolically challenging and attempting to delegitimize the logic of market commoditization. Interestingly, HIPAA's implications for the remaining two logics -- professionalism and bureaucracy -- are a bit less clear. On the one hand, HIPAA symbolically validates and seeks to protect the core professional value of doctor-patient confidentiality; on the other hand, however, HIPAA does so primarily by demanding an *intensification* of administrative oversight and control.

Varied Responses to Law:

Another noteworthy preliminary finding that is that there may be significant heterogeneity in how different hospitals and different groups within hospitals approach this new legal regime and mobilize these competing metaphors. In particular, the exploratory interviews suggest (and the survey analysis will attempt to confirm) that hospitals may vary both (a) in whether they support or oppose the new regulations, and also (b) in whether they take leader or follower roles in their support or opposition. Together, these two dimensions translate into a 2x2 typology, which we designate by the acronym “PARO,” for “**P**roponent,” “**A**cceptant,” “**R**eluctant” and “**O**pponent” (see Table 2).

	Lead	Follow
Favor	Proponents: Lead in Support	Acceptants: Follow in Support
Oppose	Opponents: Lead in Opposition	Reluctants: Follow in Opposition

In the “P” cell, one finds “proponents.” Hospitals in this category take leadership roles in support of the new regime. These organizations are normatively committed to the law, and they embrace the law’s dominant cognitive schemas and metaphors. Even before other hospitals are on board, proponents are willing to innovate and evangelize in order to expand the legal mandate. They are, in a sense, institutional entrepreneurs.

In the “A” cell reside “acceptants” -- entities that take follower roles in support of the new regime. These hospitals devote much less normative commitment and cognitive attention to the law, but for reasons of status and self-identity, they want to be (or be seen as being) “state-of-the-art” on the particular policy dimensions that the law reflects. For this reason, while they rarely take the initiative in pioneering new forms of compliance, they are strongly affected by what others are doing. Like proponents, acceptants strengthen and solidify the legal mandate; however, they do so by imitation rather than innovation and by diffusion rather than evangelism.

The “R” cell contains “reluctants.” These hospitals take follower roles in opposition. Like acceptants, reluctants have only weak normative commitments and low cognitive attentiveness to the law; but unlike acceptants, reluctants have invested their self-interests and self-identities primarily in values other than those embodied in the law. Therefore, although reluctants are strongly affected by what other hospitals are doing, they follow the herd primarily in a defensive, safety-in-numbers way. They may not want to be the straggler that gets picked off by regulatory predators, but neither do they want to be in the vanguard that stampedes headlong over a cliff. Thus, they imitate models of minimal, not maximal, compliance. And while they, like acceptants, may codify and institutionalize the law by such diffusion, the law that they thereby construct is minimized and diluted as a result.

Finally, the “O” cell contains “opponents,” -- entities that adopt active leadership roles against the new regime. These hospitals are normatively and cognitively opposed to the law, rejecting both its value premises and its organizing metaphors. Like proponents, opponents are relatively unaffected by what other hospitals are doing, and relatively willing to innovate and evangelize. Unlike proponents, however, opponents innovate and evangelize to reduce, not to expand, the legal mandate.

Taken as a whole, this PARO typology implies that the discursive fight over a new law will take place mostly between small numbers of proponents and opponents, while the diffusion processes that ultimately determine the law's taken-for-granted meaning will take place mostly among a “silent majority” of acceptants and reluctants. Consequently, to understand the processes of sense-making and social construction that give a new law its impact, one must attend to all four of these groups -- and to the organizational dynamics that differentiate them from one another.

The “Biased Muddle”:

Significantly, although the external PARO stance of any given hospital almost certainly emerges from the day-to-day contours hospital life, preliminary evidence suggest that in internal hospital deliberations, the PARO distinctions play out mostly in subtle, almost subterranean ways. In the hospital where we conducted our fieldwork, at least, HIPAA implementation was a classic “garbage can” process (Cohen, March & Olsen 1972; cf Heimer 1999): Hospital decision-makers used the externally-imposed decision-events of the HIPAA compliance process as opportunities to unload whatever problems and solutions they happened to be carrying around.

However, although this produced a large amount of “sensemaking” activity, participants rarely invoked larger policy agendas or expressed deeply-conceptualized philosophical commitments. Rather, most people most of the time seemed to be simply “muddling through,” in a well-intentioned but very “local” way. The tone of discussion was almost always cooperative and pragmatic, and when differences of opinion arose, they generally reflected differences in practical experiences and constraints, rather than differences in political values or policy goals. Thus, if our fieldsite is typical, organizations become P, A, R, or O not so much through conscious choice as through biases introduced into the implementation muddle by historical legacies, structural and cultural inertia, and the presuppositions of the various professional groups who happen to be sitting around the table in any particular meeting.

This last point merits emphasis, because there were at least two noteworthy things about the “professional groups sitting around the table” in most of the meetings that we observed: The first was the ubiquitous presence in these meetings of the hospital’s HIPAA Privacy Officer. For most hospitals (including our fieldsite), the position of “Privacy Officer” is a previously non-existent role, created purely because it is mandated by the HIPAA regulations. Yet despite the novelty of their jobs (cf. Miner 19??), Privacy Officers are often active representatives of a larger “professional project” (Larson 1977) that is actively seeking to define “health information management” as a distinct field, separate from either general IT or general administration. This emerging profession already has its own associations¹⁶ and its own educational certifications,¹⁷

¹⁶The most prominent professional associations in this field are the American Health Information Management Association (AHIMA), the Healthcare Information and Management Systems Society (HIMSS), the College of Healthcare Information Management Executives (CHIME), and the American College of Healthcare Information Administrators (ACHIA). Other prominent groups include the more academically-oriented American Medical Informatics Association (AMIA) and the more medically oriented Association of Medical Directors of

and it is beginning to develop its own vocabulary, worldview and ethical standards, as well. Although the advent of this professional project predated HIPAA by several years, the law has both elevated the proto-profession to new prominence and helped to implant privacy in the health information management field's ethical canon.

If the first noteworthy pattern of decision participation was the ubiquity of “health information management” professionals, the second noteworthy pattern was the near total absence of active-duty doctors and nurses. Instead, these older professions were present solely as “problems” to be managed. Doctors, in particular, were the subject of recurrent hand-wringing. Repeatedly, proposals would be dismissed with the regretful observation that “the docs will never put up with that.” While nurses, too, were seen as posing compliance problems, doctors emerged as the central cultural bogeymen of these meetings, invariably portrayed as obdurate, territorial, and almost Luddite in their opposition to “sound health information management” practices.

The Radiating Effects of Compliance:

The participation patterns described above are interesting in themselves, as matters of inter-professional politics. They take on added significance, however in light of the preliminary findings of the lay interviews: These interviews revealed, perhaps unsurprisingly, that lay people generally know relatively little about HIPAA. Indeed, roughly a third of our respondents had

Information Systems (AMDIS).

¹⁷Several bodies now offer training and certification as a Registered Health Information Administrator (RHIA) and as a Registered Health Information Technologist (RHIT).

never heard of HIPAA, and another third identified it solely as an organizational policy, not as a law. Moreover, even in large, far-flung HMOs, a largely untested reliance on the personal trustworthiness of particular clinicians predominated over any institutionally-oriented alternatives. Instead of desiring and valuing administrative or legal safeguards, most respondents assumed that their medical records were safe, complete and confidential because the information had been entrusted to clinicians whom the respondent had met face-to-face and who the respondent believed would vigorously defend patient interests. Moreover, to the extent that respondents were conscious of HIPAA, perceptions depended heavily on the views that clinicians conveyed to the patient in both word and in deed. As one interviewee told us:

I've never heard a healthcare worker talk about HIPAA in a positive way. And they're really the only contacts that I've ever discussed it with. I've never discussed it with my friends -- if they feel more safe, or if it makes the experience more pleasurable. But I have heard a handful of healthcare workers say [gesturing scornfully], "Yeah, now because of HIPAA you have to stand behind that line, so please..."

Contrary to the dominant narrative of the policy-planning process, however, such negative views of HIPAA seemed to be coming almost exclusively from nurses, not from doctors. And when we went back and conducted additional interviews with clinicians, we found an interesting thing: Almost without exception, nurses experienced HIPAA as a highly burdensome external intrusion, alien to the "normal" workflows of the healthcare sector and imposed by unwarranted and unwelcome coercive threats. For doctors, in contrast, HIPAA had much lower cognitive salience, and to the extent that it demanded attention at all, it was seen merely as a useful cautionary restatement of longstanding professional practices. Although more research is needed to clarify the sources of this divergence, the pattern suggests an odd inverted echo of the organizational politics of legal compliance: Privacy Officers may worry about

doctors more than nurses not because doctors are inherently more hostile to HIPAA, but because doctors hold too much organizational power to be easily dictated to or sanctioned. As a result, in the implementation process doctors get and internalize normative persuasion, while nurses get and resent coercive deterrence. These tracings of organizational power then radiate outward into public legal consciousness, as doctors and nurses carry their respective experiences of HIPAA into their interactions with the lay public.

V. Conclusion

To summarize, these preliminary findings suggest that although HIPAA was instigated by concern over the challenges of system integration, system integrity, and system control, its real-world impact has been both narrower and broader than that. HIPAA's impact is narrowed by the fact that, like many new laws, large portions of the new health-information governance regime are neither explicit, authoritative nor coercive. Ambiguity, contestation and toothless symbolism create the possibility (or indeed the probability) that HIPAA may not accomplish all that it claims, on its face, to mandate. Yet precisely because HIPAA is ambiguous, contested and symbolic -- precisely because it is cognitively messy but normatively charged -- its long-term, indirect impact may, in fact, be broader than the formal provisions of the law-on-the-books.

In its ambiguity and contestation, HIPAA has mobilized a massive "sensemaking" effort throughout the healthcare sector, exposing old taken-for-granted to new scrutiny, and spawning new opportunities for decision-making and debate. To make sense of HIPAA, healthcare organizations must consciously examine and make sense of their own longstanding assumptions and routines. HIPAA, however, is more than simply a neutral "call to debate." In its symbolism,

HIPAA has also subtly skewed that debate, framing new governance logics, and authorizing new voices to articulate them. As well as forcing people to sit up and take notice, HIPAA has focused their attention in particular directions -- most notably by talking about patient information in ways that make medical records seem less the property of the clinician or the provider organization, and more the property of the patient and the commonweal.

In important ways, though, while this sensemaking effort is sector-wide, it is also organizationally-situated. At the macro level, the division of organizations into Proponents, Acceptants, Reluctants and Opponents determines whether the sensemaking process narrows or broadens the meaning and impact of the law. And at the micro level, patterns of power and participation within each healthcare organization determine not only whether the organization as a whole is Proponent, Acceptant, Reluctant or Opponent, but also what messages about HIPAA the organization's staff conveys to the larger public. In short, we see just the kind of legally-instigated sensemaking that the law and organizations literature might predict; but we also begin to see how organizational factors may matter in the progression of that sensemaking effort.

Obviously, none of this resolves the predictive question of whether or not the health information infrastructure will flourish and whether or not, if it flourishes, it will in fact transform the larger healthcare economy. And even more obviously, none of this resolves the prescriptive question of whether or not an accelerated flow of health information would be a good thing for patient outcomes, for practitioner professionalism, for provider performance, or for public health. CIT is a field with substantial promise for improving the quality, efficiency and accessibility of healthcare, but it is also a field with substantial governance challenges to overcome before it can fulfill that promise.

Fortunately, however, one need not resolve the CIT field's vexing policy dilemmas to recognize the significance of health information governance for socio-legal scholarship. If one wishes to understand the intersection of law, organizations and the economy, one must find settings where there is actually some political appetite for experimenting with new legal, organizational and economic structures. Clinical IT is one such setting, and for that reason, if no other, it is well worth our attention.

Clinical IT is also a field where new laws, new technologies, and new markets undeniably hold the potential to reconfigure a very large and very consequential sector of social life. Traditionally, information technology -- and information technology governance -- has rarely been seen as particularly central either to health policy, to legal policy, or to social science. But in coming years, information technology is likely to play an increasingly important role in shaping the organization of healthcare; governance issues are likely to play an increasingly important role in shaping the organization of information technology; and law is likely to play an increasingly important role in shaping the organization of information technology governance. With luck, the study of these dynamics may play at least a modestly important role of its own in shaping social-scientific understandings of organizations, industries, and their legal environments.

References

- Abrahamson, Eric (1991), "Managerial Fads and Fashion: The Diffusion and Rejection of Innovations," *Academy of Management Review* 16:586-612.
- Abrahamson, Eric and Lori Rosenkopf (1993) "Institutional and Competitive Bandwagons: Using Mathematical Models as a Tool to Explain Innovation Diffusion," *Academy of Management Review* 18(3):487-517.
- Abrahamson, Eric and Lori Rosenkopf (1997) "Social Network Effects on the Extent of Innovation Diffusion: A Computer Simulation," *Organization Science* 8:289-309.
- Arthur, W. Brian (1989) "Competing Technologies, Increasing Returns, and Lock-in by Historical Events," *Economic Journal* 99(1):116-131.
- Barley, Stephen R. (1986), "Technology as an Occasion for Structuring: Evidence from Observations of CT Scanners and the Social Order of Radiology Departments," *Administrative Science Quarterly* 31:78-108.
- Burt, Ronald S. (1992) *Structural Holes: The Social Structure of Competition*. Cambridge, MA: Harvard University Press.
- Chin, Tyler (2001), "Electronic Medical Records: Mastering the Maze," *AMNews*, December 24-31, 2001.
- Carruthers, Bruce G. & Terence C. Halliday (1998), *Rescuing Business : the Making of Corporate Bankruptcy Law in England and the United States*. Oxford : Clarendon Press.
- Coleman, James S. (1990), *Foundations of Social Theory*. Cambridge, MA: Belknap Press of Harvard University Press.
- Coleman, James S., Elihu Katz and Herbert Menzel (1966) *Medical Innovation: A Diffusion Study*. Indianapolis, IN: Bobbs-Merrill.
- Damanpour, Fariborz (1991) "Organizational Innovation: A Meta-Analysis of Effects of Determinants and Moderators," *Academy of Management Journal* 34:555-590.
- DiMaggio, Paul J. and Walter W. Powell (1983), "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* 48:147-160.
- Dobbin, Frank and John R. Sutton (1998), "The Strength of a Weak State: The Rights Revolution and the Rise of Human Resources Management Divisions," *American Journal of Sociology* 104:441-476.

Dornbusch, Sanford M. & W. Richard Scott (1975), *Evaluation and the Exercise of Authority*. San Francisco, CA: Jossey-Bass.

Drazin, Robert and Claudia Bird Schoonhoven (1996) "Community, Population, and Organization Effects on Innovation: A Multilevel Perspective," *Academy of Management Journal* 39:1065-83.

Edelman, Lauren B. (1990). "Legal Environments and Organizational Governance: The Expansion of Due Process Rights in the American Workplace," *American Journal of Sociology* 95:1401-1440.

Edelman, Lauren B. (1992), "Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law," *American Journal of Sociology* 97:1531-1576.

Edelman, Lauren B. and Mark C. Suchman (1997), "The Legal Environments of Organizations," *Annual Review of Sociology* 23:479-515.

Edelman, Lauren B., Christopher Uggen and Howard S. Erlanger (1999), "The Endogeneity of Legal Regulation: Grievance Procedures as Rational Myth," *American Journal of Sociology* 105:406-454.

Farrell, Joseph and Garth Saloner (1985) "Standardization, Compatibility, and Innovation," *Rand Journal* 16:70-83.

Farrell, Joseph and Garth Saloner (1986) "Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation," *American Economic Review* 76:940-955.

Friedland, Roger and Robert R. Alford (1991) "Bringing Society Back In: Symbols, Practices, and Institutional Contradictions," pp. 204-231 in Powell & DiMaggio *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press.

Guthrie, Doug and Louise Marie Roth (1999), "The State, Courts, and Equal Opportunities for Female CEOs in U.S. Organizations: Specifying Institutional Mechanisms," *Social Forces* 78:511-542.

Health Privacy Project (2002), "Health Privacy Polling Data," Institute for Healthcare Research & Policy, Georgetown University (http://www.healthprivacy.org/usr_doc/PollingData9012.pdf).

Hagerstrand, Torsten (1967) *Innovation Diffusion as a Spatial Process* (Allan Pred trans.) Chicago, IL: University of Chicago Press.

Heimer, Carol A. (1985), *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts*. Los Angeles, CA: University of California Press.

- Katz, Michael L. and Carl Shapiro (1985) "Network Externalities, Competition, and Compatibility," *American Economic Review* 75:424-440.
- Katz, Michael L. and Carl Shapiro (1994) "Systems Competition and Network Effects," *Journal of Economic Perspectives* 8:93-115.
- Kelly, Erin and Frank Dobbin (1999): "Civil Rights Law at Work: Sex Discrimination and the Rise of Maternity Leave Policies," *American Journal of Sociology* 105(2):455-492.
- Kohn, Linda T., Janet M. Corrigan, and Molla S. Donaldson eds. (1999), *To Err Is Human : Building a Safer Health System*. Washington, DC: National Academy Press.
- March, James G. & Johan P. Olsen (1989), *Rediscovering Institutions: The Organizational Basis of Politics*. New York, NY: Free Press.
- Menzel, Herbert (1960) "Innovation, Integration, and Marginality: A Survey of Physicians," *American Sociological Review* 25:704-713.
- Meyer, John W. and Brian Rowan (1977) "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* 83:340-63.
- Parsons, Talcott (1939), "The Professions and Social Structure," *Social Forces* 17:457-467.
- Powell, Walter W. & Paul J. DiMaggio, eds. (1991), *The New Institutionalism in Organization Analysis*. Chicago, IL:University of Chicago Press.
- Prasad, Pushkala (1993), "Symbolic Processes in the Implementation of Technological Change: A Symbolic Interactionist Study of Work Computerization," *Academy of Management Journal* 36(6):1400-1428.
- Russell, Louise B. (1977), "The Diffusion of Hospital Technologies: Some Econometric Evidence," *Journal of Human Resources* 12(4):482-502.
- Ryan, B. and N.C. Gross (1943) "The Diffusion of Hybrid Seed Corn in Two Iowa Communities," *Rural Sociology* 8:15-24.
- Scott, W. Richard (1995), *Institutions and Organizations*. Thousand Oaks, CA: Sage.
- Shapiro, Susan P. (1987), "The Social Control of Impersonal Trust," *American Journal of Sociology* 93(3):623-658.
- Strang, David and Sarah A. Soule (1998) "Diffusion in Organizations and Social Movements: From Hybrid Corn to Poison Pills," *Annual Review of Sociology* 24:265-290.

- Strang, David & Michael W. Macy (2001), "In Search of Excellence: Fads, Success Stories, and Adaptive Emulation," *American Journal of Sociology* 107(1):147-182.
- Suchman, Mark C. (1999), "The Evolution of Standardized Venture Capital Financing Contracts in Silicon Valley," in T. Tanase (ed.), *Keiyaku Hori to Keiyaku Kanko [Contract Doctrines and Contract Practices]*, Tokyo: Kobundo.
- Suchman, Mark C. and Lauren B. Edelman (1996) "Legal Rational Myths: The New Institutionalism and the Law and Society Tradition," *Law & Social Inquiry* 21(4):903-941.
- Suchman, Mark C., Daniel Steward and Clifford Westfall (2001), "The Legal Environment of Entrepreneurship: Observations on the Legitimation of Venture Finance in Silicon Valley," in C. Schoonhoven & E. Romanelli (eds.), *The Entrepreneurship Dynamic: The Origins of Entrepreneurship and Its Role in Industry Evolution*. Palo Alto, CA: Stanford Univ. Press.
- Tushman, Michael L. and Philip Anderson (1986) "Technological Discontinuities and Organizational Environments," *Administrative Science Quarterly* 31:439-465.
- Uzzi, Brian (1996), "The Sources and Consequences of Embeddedness for the Economic Performance of Organizations: The Network Effect," *American Sociological Review* 61:674-698.
- Vaughan, Diane (1996), *The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA*. Chicago, IL: University of Chicago Press.
- Weick, Karl E. (1990), "Technology as Equivoque: Sense-Making in New Technologies", pp. 1-44 in P. Goodman and L. Sproull (eds.), *Technology and Organization*. San Francisco: Jossey Bass.
- Weick, Karl E. (1995), *Sensemaking in Organizations*. Thousand Oaks, CA: Sage Publications.
- Westphal, James D., Ranjay Gulati, and Stephen M. Shortell. (1997). "Customization or Conformity? An Institutional and Network Perspective on the Content and Consequences of TQM Adoption." *Administrative Science Quarterly* 42: 366-94.
- Zucker, Lynne G. (1986), "Production of Trust: Institutional sources of Economic Structure, 1840-1920," *Research in Organizational Behavior* 8:53-111.