Social Science & Medicine 72 (2011) 545–552

Contents lists available at ScienceDirect

Social Science & Medicine

journal homepage: www.elsevier.com/locate/socscimed

The “biosecuritization” of healthcare delivery: Examples of post-9/11 technological imperatives

Jill A. Fisher*, Torin Monahan

Vanderbilt University, Nashville, TN, USA

ARTICLE INFO

Article history:
Available online 27 November 2010

Keywords:
Technological imperative
Hospitals
Radio frequency identification (RFID)
Healthcare
Security
Information and communication technologies
9/11
Biosecuritization
USA

ABSTRACT

This paper develops the concept of “biosecuritization” to describe new instantiations of the technological imperative in healthcare. Many discourses and practices surrounding hospitals’ new investments in information and communication technologies tend to revolve around security provision. Oftentimes, however, scenarios of extreme and exceptional circumstances are used to justify the implementation of identification and tracking technologies that may be more about managerial control than patient care. Drawing upon qualitative research in 23 U.S. hospitals from 2007 to 2009, our analysis focuses on hospitals’ deployment of identification and location technologies that manage patients, track personnel, and generate data in real-time. These systems are framed as aiding in the process of managing supplies and medications for pandemic flu outbreaks, monitoring exposure patterns for infectious diseases, and helping triage or manage the location and condition of patients during mass casualty disasters. We show that in spite of the framing of security and emergency preparedness, these technologies are primarily managerial tools for hospital administrators. Just as systems can be used to track infection vectors, those same systems can be used on a daily basis to monitor the workflow of hospital personnel, including nurses, physicians, and custodial staff, and to discipline or reward according to performance. In other words, the biosecuritization modality of the technological imperative leads to the framing of medical progress as the “rationalization” of organizations through technological monitoring, which is intended to promote accountability and new forms of responsibilization of healthcare workers.

Introduction

Healthcare in the United States has been undergoing a quiet transformation since 9/11. As with other sectors of the economy, the terrorist attacks provided justification for the insertion—and large-scale investment—of the security industry into healthcare delivery (McGlown, 2004). The vast majority of resources for these purposes has gone into capital investments, especially information and communication technologies (Harrison, Harrison, & Smith, 2008). The federal government alone has spent $10 billion to improve the emergency response of the U.S. healthcare system (Katz & Levi, 2008). Rather than bolstering the public health system overall, these measures have instead mobilized a post-9/11 rhetoric of emergency preparedness for catastrophic events (e.g., Jagim, 2007; Snee & McCormick, 2004). While these efforts have led to the development of new markets within healthcare, they do not necessarily provide immediate benefits to most providers or patients (Blumenthal & Glaser, 2007). Moreover, the extent to which public safety and health infrastructures failed the people of Louisiana and Mississippi following Hurricane Katrina in 2005 evinces the limited responsiveness of these technological systems (TFAH, 2007). Unabashed, the security industry has folded the mismanagement of Katrina into its push for the healthcare sector to adopt additional high-tech “solutions” for the delivery of care (Harrison et al., 2008). These changes are symptomatic of larger shifts in the broader U.S. political economy, wherein neoliberal policies dictate priorities for investments in health (Fisher, 2009; Frank, 2002), education (Giroux, 2004; Monahan, 2005), welfare (Gilliom, 2001; Schram, 2006), and national security (Monahan, 2010).

This paper explores manifestations of these changes in healthcare on the ground. It focuses on hospitals’ deployment of identification and location technologies that manage patients, track personnel, and generate data in real-time. These technologies are part of what we refer to as the “biosecuritization” of healthcare delivery, which can be seen as evidence of infrastructural changes in healthcare that accompany emergent patterns of biomedicalization. Drawing upon qualitative research, we argue that this new

* Corresponding author.
E-mail address: jill.fisher@vanderbilt.edu (J.A. Fisher).

0277-9536/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.socscimed.2010.11.017

orientation within healthcare signals a reinstantiation of the technological imperative that is more focused on the rationalization of organizations than on the provision of care. Nonetheless, the concept of care gets woven into the deployment of new technologies in problematic ways, which we illustrate by examining the cases of triage systems, staff and patient tracking, and implantable microchips for patients. While these information systems are designed to serve different functions within hospitals, they each demonstrate ways in which healthcare is being shaped by the development and implementation of new types of technologies.

Technological imperatives in healthcare

The history of medicine can be told in part by tracing the development of medical technologies and their effects on patient care. Although technological change is only one facet of medicine, scholars have been commenting for decades on the important role of technology in the evolution of the doctor-patient relationship (e.g., Reiser, 1978; Rothman, 1986), the cost of healthcare (e.g., Mechanic, 1977, 2002; Rothman, 1997), and the medicalization of everyday life (e.g., Illich, 1976), to name a few. The term "technological imperative" was coined by economist Fuchs (1968) to describe the tendency within medicine to prioritize the development and use of new technologies regardless of their cost. Since Fuchs defined the term, many scholars have further developed the concept, with attention both to greater complexity in their understandings of technologies and to better situating the phenomenon within different social contexts. The first stream of research has focused on the contingent, socially embedded process of technology design and the agential force that technologies exert upon social practices and institutions, including but also extending beyond healthcare (Bijker & Law, 1992; Latour, 1992; Pinch, 1996; Sclove, 1995; Smith & Marx, 1994; Winner, 1986). Importantly, technological systems require considerable organizational and material investments in order for them to become part of standard practice, which when implemented well can prompt the imperative for those systems to be used (Bowker & Star, 1999; Sandelowski, 2000). In the stream of research more focused on the social context of medicine, scholars have also explored the underlying features of the technological imperative. For instance, Koenig (1988) has described the moral meanings that physicians attach to technologies as part of the care they provide to patients, which generates a *moral* imperative in the use of those technologies. Moreover, patients as much as physicians fuel this orientation within medicine by expecting if not demanding high-tech care (Hofmann, 2002). Quality of care is often conflated with access to the latest, cutting-edge technologies, regardless of how their performance compares to more established tools or methods (Gelijns & Rosenberg, 1994; Schneiderman & Jecker, 2000).

The technological imperative is not a new trend in medicine, but because healthcare is not a static institution, the timbre of the technological imperative shifts with political, social, and economic changes. Changes in the technological imperative can be mapped onto two successive, yet overlapping, paradigms of medical culture in the U.S.: medicalization and biomedicalization. These paradigms provide the terrains upon which healthcare actors battle for authority in medicine. They also represent the changing investment priorities that characterize the healthcare sector. Specifically, they reveal the dynamic nature of the profit motive in healthcare as providers and companies seek to expand what is included for sale in the medical marketplace and who counts as consumers.

Medicalization refers to the post-World War II expansion of the scope of medical practice in the U.S. By the end of the war, the (allopathic) medical profession through decades of professionalization and domination of the market had established its legitimacy and made itself (culturally) indispensable in treating disease and illness (Starr, 1982). With augmented post-war federal funding in the sciences, medical researchers and practitioners were poised to expand the range of bodily conditions to be treated from birth—and increasingly conception—to death, as well as to develop new scientific and technological interventions into the body (e.g., chemotherapy, antibiotics, transplantation) (Clarke, Shim, Mamo, Fosket, & Fishman, 2003; Conrad, 2007). Additionally, the expansion of services provided by practitioners broadened the scale of medicine such that healthcare developed into a complex industry (Starr, 1982). Within the context of medicalization, the technological imperative is directed at sustaining and prolonging life, with an emphasis on postponing death when the amelioration of disease is not possible (Barger-Lux & Heaney, 1986). "Medical progress" becomes defined by and measured in life expectancies, infant mortality, and survival rates, statistics that are blunt measures of life and death with little allowance for less quantifiable factors such as quality of life.

In contrast, the paradigm of biomedicalization shifts emphasis away from treating patients' illnesses to providing services for consumers. Clarke et al. (2003) have referred to it as the "Biomedical TechnoService Complex, Inc." in their in-depth exploration of the characteristics of biomedicalization. Marking 1985 as the beginning of biomedicalization, they describe this transformation in terms of medicine's colonization and commodification of health and concomitant expansions in the political economy of healthcare sectors. A key component of biomedicalization is the increased surveillance of health and risk behaviors in order to prevent, postpone, or manage serious illness (Clarke et al., 2003). While this surveillance is often represented within popular culture as both life- and cost-saving, Mechanic (2002) reminds us that preventive medicine and health-promoting care are not always cost-saving at the aggregate level. This is often the case for breast and prostate cancer screening, which frequently includes individuals with low risk profiles, so the chance of detecting single cases of cancer is quite low at a significant cost. Biomedicalization, however, is not about cost-saving; rather it is about profit-generating. Seen from this perspective, the high cost of diagnostic tests and procedures that are conducted in the name of health promotion should be no surprise because the purpose of this mode of medicine does not serve to cut total healthcare expenditures but to create and profit from new markets. Likewise, the many so-called "lifestyle" pharmaceutical products that have been developed for cholesterol, insomnia, and anxiety/depression are designed to alleviate symptoms only while patients consume them and so need to be consumed long-term (Dumit, 2002). The technological imperative within biomedicalization can thus be understood in terms of the expansion of healthcare markets to products and services for healthy consumers and for long-term use by patient populations. "Medical progress" within this frame becomes defined by and measured in terms of consumption: the number of individuals subscribing to treatment and prevention regimens and accessing illness-prevention and health-promotion services.

Developing upon Clarke et al's. (2003) framing of biomedicalization, we identify *biosecuritization* as a type of technological imperative operating within the "Biomedical TechnoService Complex, Inc." and transforming U.S. healthcare infrastructures. A key component of the biomedicalization paradigm is the redefinition of who is a consumer and what products are available for consumption. In its biosecuritization mode, this manifests as massive investments in information and communication technologies. The term biosecurity is often mobilized as a response to perceived risks of contagion from biological agents, with an emphasis on risks introduced by bioterrorism, even if such a focus occludes more mundane threats to biosecurity (Collier, Lakoff, &

Rabinow, 2004; Cooper, 2006; Lentzos, 2006; Vogel, 2008). Nonetheless, within the context of healthcare delivery, biosecuritization draws upon the dominant national-security frame of emergency preparedness to alter organizational practices and priorities in interesting and complex ways. Rather than having its orientation toward the provision of services to patients, biosecuritization targets hospitals and other healthcare organizations to consume information, communication, and security technologies.

While much media attention has focused on federal, state, and local efforts to stockpile supplies and medications for pandemic flu outbreaks, less public are the infrastructural investments that have received high priority, from software applications such as FluSurge 2.0, distributed by the U.S. Department of Health and Human Services (DHHS), to advanced monitoring systems designed to detect exposure patterns of infection (Radonovich, Magalian, Hollingsworth, & Baracco, 2009; Thuemmler, Buchanan, Fekri, & Lawson, 2009). Some of these systems are purported to enable more efficient distribution of services to patients in emergency situations while others are designed to help triage or manage the location and condition of patients (Curtis et al., 2008). As media coverage of outbreaks of severe acute respiratory syndrome (SARS), avian flu (H5N1), and most recently swine flu (H1N1) spreads fear about the presumed scale of contagion (Davis, 2005; Lakoff & Collier, 2008), what get eclipsed are the relative risks of these "new" viruses in relation to the risks of more quotidian illnesses, especially in terms of the strains they create on the healthcare system.

In other words, hospitals are urged to consume technologies for low-probability disaster situations as part of a security discourse that privileges the spectacular or exceptional cases of mortality and morbidity in healthcare. On one hand, these investments turn cost-benefit calculations on their head because the systems tend to be expensive and have little benefit for routine practices and procedures. On the other, these investments illustrate the extent to which a new type of technological imperative is operating within healthcare settings. Even without occasion to be used to manage catastrophes, technologies within this domain offer significant symbolic value because of the promise they provide for the public's health and safety, and this type of value often prompts investment in them (TFAH, 2007). The media, federal government, technology vendors, and the hospital rankings published by the American Hospital Association all contribute to the urgency that hospital administrators might feel to adopt these technologies.

More than this, however, is that these technological systems often provide tangible resources for hospital administrators. Rather than seeing these technologies as having primary uses in emergency situations, it is instead possible – and likely preferable – to view these technologies in terms of the managerial tools they offer administrators. Just as systems can be used to track infection vectors, those same systems can also be used on a daily basis to monitor the workflow of hospital personnel, including nurses, physicians, and custodial staff, and to discipline or reward according to performance (Fisher, 2006; Fisher & Monahan, 2008). In other words, the biosecuritization modality of biomedicine leads to the framing of "medical progress" as the "rationalization" of organizations through technological monitoring, which aims to promote accountability and new forms of responsibilization of healthcare workers. With biosecuritization, the benefits of technological change are not as easily felt by patients or providers as they are by hospital administrators.

In the social sciences, empirical case studies of medicalization and biomedicalization have provided analytic insights into the complex manifestations of these phenomena in healthcare settings (Clarke, Mamo, Fosket, Fishman, & Shim, 2010; Conrad, 2007; Klawiter, 2008; Mamo, 2007; Sullivan & Weitz, 1988). In contrast, there has been little work to date exploring the process of biosecuritization of healthcare (e.g., King, 2003, 2005; Lakoff & Collier, 2008), and as a result, media portrayals dominate, providing inadequate critical appraisal of the trends. This paper serves as a partial corrective by illustrating some of the ways in which security discourses are used to justify the implementation of identification and tracking technologies in U.S. hospitals.

Methods

This paper is based on qualitative research conducted from March 2007 to December 2009 as part of a broader empirical project analyzing the organizational effects of the implementation of identification and tracking technologies in hospitals. The methods for this project were observational studies and semi-structured interviews with personnel at hospitals that have implemented systems that are used to identify or track patients, staff, and/or equipment. The ethics boards at Arizona State University and Vanderbilt University approved this research. The project included 23 U.S. hospitals that were selected based on their use of a qualifying system (as identified through personal contacts, press releases, or media coverage) and their receptivity to participating in the research. One or both authors visited each hospital, were given demonstrations of the systems, and observed the systems in use. In addition, we conducted 80 semi-structured interviews with hospital staff, including physicians, nurses, administrators, information technologists, and biomedical engineers, as well as vendors involved with these systems. Interviewees were recruited from hospital employees who make decisions about or are targeted users of the systems. Interviews were recorded, transcribed, and stripped of personal identifiers. The hospital sites and personnel have been kept confidential in the study.

We analyzed all transcribed interviews and observational notes to identify core themes, such as key ethical concerns associated with these systems. Although the research was not designed to investigate the effects or characteristics of biosecuritization per se, the themes of security, emergency, and fear repeatedly emerged in interviews even as the managerial benefits of these technologies were observed. This paper explores three examples of such systems that ostensibly lend themselves to increased patient security and care.

Technologies of care: examples of biosecuritization

Just as discourses of insecurity cultivate fear more broadly in American culture and galvanize support for technologies of fortification and surveillance (Altheide, 2006; Glassner, 1999; Monahan, 2010), so too are such discourses mobilized to support the deployment of new systems of identification and tracking in hospitals. In the process, the concept of "care" becomes conflated with that of security, not just of individual patients, but of entire populations. As will become evident, care is reconstructed as the security that can be provided by new systems of managerial control, which is a framing that, in turn, marginalizes and even displaces other possible understandings of care. This section introduces the technologies in question, reviews a few examples of this discursive pattern from our field research, and critically explores the implications for healthcare relations more broadly.

Routine functions of identification and tracking systems

Many U.S. hospitals are planning for disasters through significant infrastructural investments, such as separate ventilation systems, quarantine zones, and points of entry and egress to contain disease – and disease vectors – in the event of a disease pandemic or biological terrorist attack (Katz & Levi, 2008). Hospitals are also revising evacuation and patient management procedures to minimize points of contact between personnel and potentially contagious individuals (TFAH, 2007). In this vein, new identification and tracking systems may assist with the process of maintaining security and safety in the event of a disaster, whether biological or otherwise. Disaster management may be one of the goals of "real-time location systems" (RTLS), but, as our examples will demonstrate, their current uses are geared toward managerial control. Such systems typically use electronic tags on equipment or name badges, which can then be tracked by detectors that are placed throughout hospitals and monitored remotely through computer software interfaces. These are wireless systems, meaning that the tags are tracked through radio, sonar, or other spectrum waves. Radio frequency identification (RFID) systems are currently the most prevalent. The technologies gained prominence in manufacturing and distribution industries, but technology vendors understood the potential for a profitable market in healthcare and have teamed up with software companies to offer products that are more suitable to healthcare (Fisher & Monahan, 2008). In a 2008 survey of U.S. hospitals, 15% of administrators indicated that their hospitals already had these technologies in place and another 43% expressed their intent to purchase these systems within the next two years (HIMSS, 2008).

At present, RTLS is being implemented primarily for inventory tracking and "workflow management". Given that many hospitals now operate as "just-in-time" facilities, meaning that they carry only sufficient medical supplies for a few days worth of patient care, hospital administrators are embracing high-tech inventory management systems as a way to intelligently micromanage the daily functions of hospitals without acquiring excess supplies. According to this rationale, all significant pieces of hospital equipment, ranging from infusion pumps to wheelchairs to X-ray machines, should be tagged with RTLS transmitters so that their exact location and unique identification (i.e., model and serial numbers) can be known at all times. This will supposedly assist hospital staff with quickly locating items when they are most needed for medical procedures or when they are targeted for regularly scheduled maintenance or product recalls. One patient safety aspect of this is that should a piece of equipment belatedly be found to be faulty, it can be identified, located, and removed from service to prevent additional problems or medical errors.

Additionally, software-based alarms can be added to alert staff when expensive pieces of equipment are leaving the premises, whether because they are being stolen, accidentally thrown away, or necessarily accompanying a patient who is being transferred to another facility. Preventing inventory from leaving hospital grounds can save money for hospitals. Similarly, hospital administrators aspire to reduce the amount of rented, unused, or redundant equipment, and they feel that the ability to generate detailed reports based on RTLS data will assist them with this mission. In practice, however, staff members often ignore alarms about equipment because they are already overburdened with significant responsibilities, of which policing equipment is but one more, and because there are frequent legitimate reasons for equipment to leave hospital premises, such as patients temporarily going outside (with their IVs, wheelchairs, etc.) to smoke.

Workflow management represents the second key area for the use of identification and tracking systems in hospitals. Some hospital administrators engage in this activity by requiring hospital staff (and increasingly patients) to wear RTLS tags that will transmit identification, location, movement, and proximity data to a central computer system by means of detectors installed within specific departments or throughout the facility. As might be expected, those employees with lower professional status, such as nurses and clerks, are much more likely to be tracked in this way than are those with higher status, such as physicians and administrators. Workflow management regimes of this sort reinscribe the rational control of Taylorism, replete with "efficiency studies" for the reduction of staff labor and the reduction of staff (Taylor, 1911). Through such information systems, administrators hope to identify objectively "bottlenecks" in the coordination and execution of care-giving activities and to take decisive action, such as re-training, redeploying, or eliminating staff, to contend with what they perceive to be inefficiencies in the system. As one hospital administrator succinctly stated in an interview: "If you can measure it, you can manage it." Therefore, one goal is to use these systems to translate all hospital activities into discrete, measurable units that can be soberly managed from afar.

Elsewhere we have called attention to the power dynamics and surveillance potentials of hospital systems for inventory tracking and workflow management (Fisher, 2006; Fisher & Monahan, 2008; Monahan & Fisher, 2008). Namely, such systems tend to intensify labor and add additional responsibilities for nursing staff who lose degrees of control over their workplaces when administrators implement RTLS. Whereas typical hospital settings allow for complex social arrangements with nursing staff often stashing and sharing equipment as needed, inventory management systems seek to circumvent existing hospital cultures by establishing—or reasserting—top-down control over departments. Moreover, low-level staff are often tasked with the data-entry, tag management, and equipment roundup activities of RTLS, which may reduce some of the labor associated with finding items – or what administrators disparagingly refer to as "hunting and gathering" – but also add additional work in the form of responding to alarms, replacing batteries in tags, adding new inventory into the database, and so forth. Although, in interviews, administrators state that they are not interested in tapping the "Big Brother" capabilities of these systems, informants have communicated to us telling examples of people being disciplined and fired because RTLS data proved that they were taking breaks when they were not supposed to or were lying about their locations. Thus, it is not all that surprising that some nursing staff are reluctant to wear location tags and that some have even sabotaged the systems (Fisher, 2006). Identification and tracking systems clearly lend themselves to surveillance and control functions. Instead of approximating any totalizing or panoptic form of discipline (Foucault, 1977), however, the ad-hoc and partial deployment of RTLS, coupled with material and cultural constraints, attenuate overt surveillance uses.

Systems for exceptional circumstances

What we would like to draw especial attention to here, however, are the ways in which administrators and others justify identification and location systems in hospitals. At industry conferences, hospital administrators, biomedical engineers, and technology vendors all emphasize the "return on investment" (ROI) potential of such systems. As indicated above, they feel that RTLS will enable them to reduce superfluous inventory, minimize equipment loss, and efficiently manage personnel in order to speed patients through the system, thus enabling hospitals to handle a greater number of patients and improve profitability. But in interviews *at hospital sites*, this discourse shifts radically away from concerns about management needs and capital accumulation and toward those of patient care and security provision. It is almost as if the rationale of ROI is too crude in an institutional setting devoted to helping and healing patients, so administrators and physicians conjure alternative narratives that resonate better with the mission of patient care. Moreover, administrators and physicians offer what can only be called *extreme and dramatic examples* to justify identification and location systems in terms of care, such as assisting hospitals in responding to disease pandemics, natural disasters, and terrorist attacks.

For instance, one large public hospital in the northeast we visited had funding to pilot a triage-management system to assist emergency departments with handling swarms of patients in disaster situations. Patients agreeing to participate in this study were equipped with a belt-pack with a location transmitter, EKG electrodes, blood-pulse oximeter, blood pressure reader, and a small PDA device to track vital signs and wirelessly transmit them to a central monitoring station. Software-based alarms were programmed into the system to alert staff (through a computer terminal or wireless devices) if someone who was hooked up to the system "went critical", as well as to provide staff with the vital signs and exact location of the patient in need. Hypothetically, if all patients were hooked up to such a system in a disaster situation, staff would benefit from a more objective reading of who was the most in need and would be able to prioritize the treatment of those patients.

At the time of our visit, the pilot study was in its final month, several of the wireless detectors in the ED waiting room were no longer operational (meaning that the exact location of patients could not be determined), and no new patients were being enrolled in the study. In the words of those involved, the study was probably a failure. The reasons for this are complex, though, ranging from territoriality and non-cooperation among departments at the hospital; prior commitments on the part of hospital administrators to a competing RTLS company; equipment unreliability; and the absence of a clear-cut case of system efficacy – or "proof of concept". In an interview, the physician who was overseeing the study explained the rationale and outcome:

> I think conceptually in a disaster situation [the system] would be much easier to justify… If you think about even [Hurricane] Katrina, the Dome, and people saying you would go to the patients who cried out louder rather than the ones that were in most need or something, and you wouldn't know who was taking care of what… There were some anecdotes of patients collapsing in the bathroom [of our hospital and no one knowing]… The system would detect that because it would have both the vital signs and their location. [This situation] didn't happen to us, but then we had just 160–170 patients [during the trial], so the likelihood of that happening with our patients was very small.
>
> *Interviewer*: Well, you don't want it to happen.
>
> You don't yes, but on the other hand, you want to show that it works.

This is an interesting articulation on several levels. First, the system is being framed explicitly in terms of disaster preparedness and management. The concern for "care" is not mundane or abstract – instead, it is exceptional, visceral and fear-based. Second, and in tension with the emphasis on care, the physician expresses regret that the system did not capture a critical incident of someone collapsing during the trial period. When we pointed out the fact that one should not desire for a patient to collapse or be in dire need (and especially not for a physician to wish such a thing), she responded pragmatically that "You don't yes, but on the other hand, you want to show that it works." Because this pilot study failed to establish proof of concept, the investigator would probably not be able to market it or receive future funding for this particular project. Rather than interpret this as an unusual form of instrumentality on the part of this physician, it might make more sense to see this as a telling example of the pressures physicians face to succeed professionally and financially in a heavily commercialized American healthcare context. Indeed, other physicians gave us extensive tours of state-of-the-art operating rooms, dined with us, and spent countless hours pitching their innovations to us and inviting us to "partner" with them in some way, so the culture of entrepreneurialism is dominant in hospital settings, much like it is in other healthcare contexts (Fisher, 2009; Gray, 1993).

A second prominent discourse mobilized by hospital administrators is one of staff safety and public health in the face of disease pandemics. Administrators and others suggest scenarios of using RTLS to determine precisely which staff members came into contact with patients carrying dangerous infectious diseases, such as SARS, and then effectively treating or isolating people based on those data. For example, a nurse administrator at one large hospital in the south described in foreboding tones a close call her hospital had when – without their knowledge – they treated the roommate of someone diagnosed with SARS. If the hospital had an advanced RTLS system, she continued, they would have been able to quarantine everyone who was exposed to that patient and thereby minimize the potential spread of the disease. This particular hospital had already constructed a quarantine zone, complete with a separate ventilation system and separate exits from the building, so this vision of isolating risky patients, and staff exposed to them, was consistent with the existing infrastructure and culture of this hospital.

This discourse of fear (of pandemics, disasters, terrorist attacks) becomes a powerful rationalization for systems designed to increase profitability and managerial control. The technologies, in other words, are touted for their "dual-use" functionality. Thus, the primary objective of the system described by the nurse administrator is to automate hospital billing procedures, not to improve disease surveillance and management. The goal is for patients, physicians, nurses, and other hospital staff to wear unique identification and location tags so that "dynamic associations" can be made among them, allowing for the automatic generation of data and filing of paperwork. If, for instance, the system detects a physician entering the room of a patient, it can automatically register a "billing event" so that no paperwork needs to be filed – the events will be compiled through software and electronically submitted to the appropriate insurance company, or delivered to the patient, as the case may be. One hospital we visited in the southwest employed a similar system to assign nurses and physicians to patients. So, when a nurse steps into a patient's room, for example, he or she is digitally linked to that patient in the system and is responsible for the care of that patient for the duration of his or her stay (or until the end of the nurse's shift, at which point a new nurse must be assigned). One can imagine persuasive objections to a dynamic-association system used for these purposes, such as errors in billing that are difficult to contest or patients who are eschewed by hospital employees who would like to avoid being assigned to another patient. Yet, the discursive framing of "control of disease pandemics" deflects criticism from the systems and these other uses because the threat is constructed as absolute and universal: pandemics threaten to spread in a frighteningly unpredictable manner and decimate populations, so controlling them is for the good of all humanity. Such articulations neatly eclipse the profit motives behind such systems.

As a final example, discourses about the use of RFID implants similarly emphasize care – over capital – through a discourse of extreme situations. RFID implants are marketed by the VeriChip Corporation and were approved by the FDA for human use in 2004. They function similarly to microchipping systems used for identifying lost pets. In humans, a small, glass-encased RFID chip is injected into the triceps region of the right arm of patients, after which it can be scanned to reveal a unique 16-digit identifying number that can be entered into an online system (called "VeriMed") to access a patients' medical records (Monahan & Fisher, 2010). The VeriChip company and physicians administering RFID implants lend support to the system by saying that it can provide safeguards for patients who might arrive at hospitals incapacitated in some way and be unable to communicate effectively about their medical histories. Individuals with epilepsy, heart disease, diabetes, or Alzheimer's disease might fall into this category. In such situations, the system could provide medical professionals with vital information about a patient's identity, medical history, drug allergies, and so on.

The origin story that VeriChip tells about their medical device is directly linked to security and disaster narratives. According to the company's promotional material,

> The roots of VeriChip trace back to the events of September 11, 2001 when New York firemen were writing their badge ID numbers on their chests in case they were found injured or unconscious. It was evident there was a desperate need for personal information in emergency situations and that an injectable RFID microchip could help patients. (VeriChip Corporation, 2007)

Unlike the RTLS triage case described above, VeriChip had a lucky break of a real-world "proof of concept". Fairly early in the dissemination of implants, a sensational news story broke about a New Jersey police officer who had been RFID chipped before becoming badly injured in an accident resulting from a high-speed car chase. According to one report archived on VeriChip's website, "Suffering head trauma after his cruiser hit a telephone pole while on a stolen-car chase, the 44-year-old diabetic was in no shape to give doctors his medical history. That job was left to a tiny microchip buried beneath the skin of his right arm" (Stewart, 2006). The press release also quotes the police officer as having said, "Until the accident, I actually forgot it was there." What the press release did not mention was that when the officer arrived at the emergency room he *was* able to identify himself and explain that he was a diabetic. In addition, the officer himself informed the medical team that he had an RFID implant (Personal communication with a hospital employee, 8/6/07). Nonetheless, the medical team was able to access his medical information through the unique identifier on the chip, and the fact that the first patient to benefit from an RFID implant was a police officer made the story all the more mediagenic.

The company implemented an interesting application of these technologies during the aftermath of Hurricane Katrina, when mobile units went around "chipping" cadavers with RFID implants and taking digital pictures of the faces of the deceased (Kanellos, 2005). The logic behind this use was that by matching each unique identification number with digital pictures, positive identification of bodies could be made well after significant decomposition had taken place. While this use of implants obviously served an important function to assist people in identifying the remains of their family members in a disaster, it should also be mentioned that VeriChip was also seizing an opportunity to profit from the federal, state, and private dollars pouring into Louisiana and Mississippi as part of disaster relief efforts and further assert the importance of its system.

The narrative of heroic medicine leaves little room for social concerns that might arise from the system. According to Dr. John D. Halamka, chief information officer of Harvard Medical School and one of the first humans to be implanted with an RFID chip: "I'm a rock climber, and I believe that if I fall off a cliff and you find me unconscious, the comfort of being able to scan me and figure out who I am outweighs my concern for privacy" (ABC News, 2006). Although the emphasis with RFID implants is upon identification rather than location, the arguments supporting it reveal a similar politics of displacement, wherein the social ramifications of and profit motives underlying these systems are hidden behind the unquestionable social good of "care" (Monahan & Fisher, 2010).

Patients electing to receive an RFID implant and enroll in the VeriMed system must pay both for the cost associated with being implanted, estimated at $200 to $300 (VeriMed, 2006), and a monthly fee of $9.95 with a minimum of a two-year contract (VeriMed, 2008). At the time of our study, one large insurance company was partnering with VeriChip to cover the costs associated with enrolling a few hundred eligible patients and transferring patients' medical data into the system. This partnership was finite in scope and explicitly intended to jump-start interest in VeriChip through the media attention garnered by this arrangement. Otherwise, patients must commit to purchasing this healthcare commodity in the hopes that it might save their lives some day if hospitals across the country begin routine scanning for RFID implants when patients arrive at emergency departments. Additionally, according to Joseph Feldman, a physician who speaks frequently on the merits of the VeriChip, physicians can easily increase their revenue by offering to patients the service of RFID implants (Feldman, 2007).

These three examples each reveal different dimensions of biosecuritization. The triage-management system points to the intermingling of entrepreneurial logics with those of population security. In this case, and in ones like it, physicians act as research investigators hoping for "proof of concept" to sell their ideas to their own or other hospitals. In the case of using RTLS for dynamic associations, nurses and others dwell on the risks of disease pandemics and the need for robust RTLS to track and quarantine disease vectors. All the while, the actual uses in the hospitals we visited are geared toward automated billing and staff management. The final example of RFID implants indicates the crossover potential of identification and tracking systems for individual consumption by patients. As would be an expected feature of biomedicalization, patients are being sold a medical device and service – not for direct health purposes, but instead for assurances of safety and efficiency in the event of a low-probability crisis where they will show up incapacitated at a hospital without an ID or a person who knows who they are. In all of the examples, these technologies have high financial costs for hospitals or consumers, but they probably add very little to the care provided to patients or the security of hospitals.

Conclusion

This paper has described a new technological imperative in healthcare and provided case examples from empirical research. We have named the changes "biosecuritization" both to situate them within the paradigm of biomedicalization and to highlight the security focus of discourses and practices surrounding new investments in information and communication technologies. Hospital administrators, clinicians, and vendors explicitly mobilize fears about public health and safety that are shaped by the post-9/11 world in which we live. Pandemic flu outbreaks, natural disasters, and even terrorist attacks are not new events, yet within the still emergent biosecuritization frame, they are treated as novel and require new levels of investment in technologies, infrastructure, and personnel as part of a commitment to emergency preparedness.

Real-time location systems are one such emergent technology that is framed as a solution to these security concerns. While much of the implementation of these systems happens piecemeal because different hospitals or hospital departments pick and choose the technological capabilities best suited to their needs and budgets, there is also a federal focus on the potential of these systems. Specifically, in August 2009, the U.S. National Library of Medicine issued a request for proposals that stated:

> The National Library of Medicine will be seeking contractor(s) that shall furnish the necessary personnel, products, materials

> and other services required to plan and implement a Radio Frequency Identification (RFID)/Real Time Location System (RTLS) for the Bethesda Hospitals' Emergency Preparedness Partnership (BHEPP). The BHEPP has identified a critical need for the acquisition of a Radio Frequency Identification (RFID)/Real Time Location System (RTLS) to directly support the current emergency preparedness initiatives of three of its members, namely, the National Naval Medical Center, National Institutes of Health Clinical Center, and Suburban Hospital Healthcare System… The RFID/RTLS solution shall incorporate role-based access so as to provide BHEPP the ability to track patients and assets across all three hospitals, while at the same time providing each of the hospitals the ability to track their own patients and assets. (NLM, 2009)

This announcement is indicative of the resources that will likely be spent on RTLS in the coming years and the framing that accompanies that investment. In spite of the focus on emergency preparedness, the main functions of any RTLS implementation – as we have argued above – will be much more mundane because the systems need to have a quotidian value (i.e., in routine, non-catastrophic situations).

At the heart of biosecuritization is an emphasis on the rationalization of healthcare organizations. On one hand, this can be understood as a desire to impose order and logic on the chaos inherent in disaster situations. For instance, it would be a clear benefit in a disaster to be able to triage patients more intelligently by having a technological means of adapting flexibly to the changing needs of patients. Likewise, discerning the possible pathways of pathogens by mapping contact between patients and clinicians could provide critical information to minimize exposure. On the other hand, while these uses of technology may be salient reasons for implementing expensive systems, they rarely align well with the normal chaos of hospitals. Instead, these technologies become management tools to measure the performance of employees, increase hospital throughput, and/or leverage existing equipment for increased capacity (Fisher, 2006). In other words, the likely examples of how these technologies are used in practice include monitoring clinicians and staff, scaling up on the volume of patients treated, and centralizing equipment so that personnel need to share resources across hospital units. Most of these uses are not intrinsically negative, but the benefits to clinicians and patients are far from obvious.

In addition, the market forces behind biosecuritization cannot be ignored. Emergency preparedness has become an industry sector straddling defense and information technology, and a very profitable one at that. Whereas Naomi Klein (2007) has written about the exploitation of disasters around the world to create profit for large corporations, our research indicates that these trends also happen on a smaller and less dramatic scale everyday within healthcare. Technology vendors are eager to sell information and communication technologies to hospitals, and hospital administrators are interested in demonstrating their business acumen by gaining returns on their investments. It is the type of investments that differentiates this technological imperative from others in the biomedicalization paradigm. Hospitals themselves – the health of the organizations and their operations – are the target of consumption because the costs of investment are not as easily passed on to patients as they are with the purchasing of medical equipment. While the example of RFID implants seems to complicate this conclusion, the very low adoption and lack of market success of these technologies may prove the point that biosecuritization is driven by a consumer model that operates best on the level of organizations and not individuals. This new form of technological imperative underscores the break that has occurred from medicalization to biomedicalization (Clarke et al., 2003). It must also be stressed that hospitals are working with finite resources, so investments in biosecuritization necessitate a reduction in funding for other aspects of the healthcare enterprise, such as targeted improvements in medical care.

Because the empirical focus of this paper is confined to our study of RTLS, we have touched on only one piece of how biosecuritization currently manifests in hospitals. We expect that future research will uncover other examples and add to the conceptual work we have begun. The challenge for social scientists studying healthcare systems is to unpack the claims that are being made at multiple levels of organizational and institutional structures. It is important to trace simultaneously the convergences and divergences in the discourses and practices that constitute this emerging terrain. Linking national trends regarding security and emergency preparedness with local responses to those developments is an essential place to start.

Acknowledgements

This material is based upon work supported by the U.S. National Science Foundation under grant numbers 0642797 and 0907993.

References

ABC News. (2006). ID health chip. Available from. http://abclocal.go.com/wls/story?section=news/health&id=3974003 (accessed April 2, 2008, transcript corrected by authors).

Altheide, D. L. (2006). *Terrorism and the politics of fear*. Lanham, MD: Altamira Press.

Barger-Lux, M. J., & Heaney, R. P. (1986). For better and worse: the technological imperative in health care. *Social Science & Medicine, 22*(12), 1313–1320.

Bijker, W. E., & Law, J. (1992). *Shaping technology/building society: Studies in sociotechnical change*. Cambridge, MA: MIT Press.

Blumenthal, D., & Glaser, J. P. (2007). Information technology comes to medicine. *New England Journal of Medicine, 356*(24), 2527–2534.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Clarke, A. E., Shim, J. K., Mamo, L., Fosket, J. R., & Fishman, J. R. (2003). Biomedicalization: technoscientific transformations of health, illness, and U.S. biomedicine. *American Sociological Review, 68*(2), 161–194.

Clarke, A. E., Mamo, L., Fosket, J., Fishman, J., & Shim, J. (Eds.). (2010). Biomedicalization: Technoscience, health, and illness in the U.S. Durham: Duke University Press.

Collier, S. J., Lakoff, A., & Rabinow, P. (2004). Biosecurity: towards an anthropology of the contemporary. *Anthropology Today, 20*(5), 3–7.

Conrad, P. (2007). *The medicalization of society: On the transformation of human conditions into treatable disorders*. Baltimore: Johns Hopkins University Press.

Cooper, M. (2006). Pre-empting emergence: the biological turn in the war on terror. *Theory, Culture & Society, 23*(4), 113–135.

Curtis, D. W., Pino, E. J., Bailey, J. M., Shih, E. I., Waterman, J., Vinterbo, S. A., et al. (2008). SMART—an integrated wireless system for monitoring unattended patients. *Journal of the American Medical Informatics Association, 15*(1), 44–53.

Davis, M. (2005). *The monster at our door: The global threat of avian flu*. New York: New Press.

Dumit, J. (2002). Drugs for life. *Molecular Interventions, 2*(3), 124–127.

Feldman, J. (2007). Medical applications for RFID technology. In International Quality and Productivity Center. (Ed.), *6th RFID, barcoding, & emerging technologies for hospitals and health systems*. (Philadelphia).

Fisher, J. A. (2006). Indoor positioning and digital management: emerging surveillance regimes in hospitals. In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life* (pp. 77–88). New York: Routledge.

Fisher, J. A. (2009). *Medical research for hire: The political economy of pharmaceutical clinical trials*. New Brunswick: Rutgers University Press.

Fisher, J. A., & Monahan, T. (2008). Tracking the social dimensions of RFID systems in hospitals. *International Journal of Medical Informatics, 77*(3), 176–183.

Foucault, M. (1977). *Discipline & punish: The birth of the prison*. New York: Vintage Books, Random House.

Frank, A. W. (2002). What's wrong with medical consumerism? In S. Henderson, & A. Petersen (Eds.), *Consuming health: The commodification of health care* (pp. 13–30) New York: Routledge.

Fuchs, V. R. (1968). The growing demand for medical care. *New England Journal of Medicine, 279*(4), 190–195.

Gelijns, A., & Rosenberg, N. (1994). The dynamics of technological change in medicine. *Health Affairs, 13*(3), 28–46.

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.

Giroux, H. A. (2004). *The terror of neoliberalism: Authoritarianism and the eclipse of democracy*. Boulder, CO: Paradigm Publishers.

Glassner, B. (1999). *The culture of fear: Why Americans are afraid of the wrong things*. New York, NY: Basic Books.

Gray, B. H. (1993). *The profit motive and patient care: The changing accountability of doctors and hospitals*. Cambridge: Harvard University Press.

Harrison, J. P., Harrison, R. A., & Smith, M. (2008). Role of information technology in disaster medical response. *The Health Care Manager, 27*(4), 307–313.

HIMSS (Healthcare Information and Management Systems Society). (2008). *19th annual – 2008 HIMSS leadership survey*. Final Report. Chicago: Healthcare CIO.

Hofmann, B. (2002). Is there a technological imperative in health care? *International Journal of Technology Assessment in Health Care, 18*(3), 675–689.

Illich, I. (1976). *Medical nemesis: The medical expropriation of health*. New York, NY: Pantheon Books.

Jagim, M. (2007). Emergency preparedness response: building infrastructure. *Journal of Emergency Nursing, 33*(6), 567–570.

Kanellos, M. (2005). RFID chips used to track dead after Katrina. *CNET News*, .

Katz, R., & Levi, J. (2008). Should a reformed system be prepared for public health emergencies, and what does that mean anyway? *Journal of Law, Medicine, & Ethics, 36*(4), 716–721.

King, N. B. (2003). The influence of anxiety: September 11th, bioterrorism, and American public health. *Journal of the History of Medicine and the Allied Sciences, 58*(4), 433–441.

King, N. B. (2005). The ethics of biodefense. *Bioethics, 19*(4), 432–446.

Klawiter, M. (2008). *The biopolitics of breast cancer: Changing cultures of disease and activism*. Minneapolis: University of Minnesota Press.

Koenig, B. A. (1988). The technological imperative in medical practice: the social creation of a routine treatment. In M. Lock, & D. Gordon (Eds.), *Biomedicine examined* (pp. 465–496). Boston: Kluwer.

Klein, N. (2007). The shock doctrine: The rise of disaster capitalism. New York: Henry Holt & Co.

Lakoff, A., & Collier, S. J. (Eds.). (2008). *Biosecurity interventions: Global health and security in question*. New York: Columbia University Press.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. E. Bijker, & John Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 225–258). Cambridge, MA: The MIT Press.

Lentzos, F. (2006). Rationality, risk and response: a research agenda for biosecurity. *BioSocieties, 1*(4), 453–464.

Mamo, L. (2007). *Queering reproduction: Achieving pregnancy in the age of technoscience*. Durham: Duke University Press.

McGlown, K. J. (Ed.). (2004). *Terrorism and disaster management: Preparing healthcare leaders for the new reality*. Chicago: Health Administration Press.

Mechanic, D. (1977). The growth of medical technology and bureaucracy: implications for medical care. *The Milbank Memorial Fund Quarterly, 55*, 61–78.

Mechanic, D. (2002). Sociocultural implications of changing organizational technologies in the provision of care. *Social Science & Medicine, 54*(3), 459–467.

Monahan, T. (2005). *Globalization, technological change, and public education*. New York: Routledge.

Monahan, T. (2010). *Surveillance in the time of insecurity*. New Brunswick: Rutgers University Press.

Monahan, T., & Fisher, J. A. (2008). Scanning the future of hospital radio-frequency identification systems. *Hospital Information Technology Europe, 1*(1), 44–45.

Monahan, T., & Fisher, J. A. (2010). Implanting inequality: empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. *International Journal of Technology Assessment in Health Care, 26*(4), 370–376.

NLM (National Library of Medicine). (2009). *Radio frequency identification (RFID)/ Real time location system (RTLS)*. Solicitation Number: NLM-09-178-RS.

Pinch, T. (1996). The social construction of technology: a review. In R. Fox (Ed.), *Technological change: Methods and themes in the history of technology* (pp. 17–35). Amsterdam: Harwood Academic Publishers.

Radonovich, L. J., Magalian, P. D., Hollingsworth, M. K., & Baracco, G. (2009). Stockpiling supplies for the next influenza pandemic. *Emerging Infectious Dieseases, 15*(6), e1–e6.

Reiser, S. J. (1978). *Medicine and the reign of technology*. Cambridge: Cambridge University Press.

Rothman, B. K. (1986). *The tentative pregnancy: Prenatal diagnosis the future of motherhood*. New York: Viking.

Rothman, D. J. (1997). *Beginnings count: The technological imperative in American health care*. New York: Oxford University Press.

Sandelowski, M. (2000). *Devices and desires: Gender, technology, and American nursing*. Chapel Hill: The University of North Carolina Press.

Schneiderman, L. J., & Jecker, N. S. (2000). *Wrong medicine: Doctors, patients, and futile treatment*. Baltimore: Johns Hopkins University Press.

Schram, S. F. (2006). *Welfare discipline: Discourse, governance and globalization*. Philadelphia: Temple University Press.

Sclove, R. E. (1995). *Democracy and technology*. New York: The Guilford Press.

Smith, M. R., & Marx, L. (Eds.). (1994). *Does technology drive history?: The dilemma of technological determinism*. Cambridge, MA: MIT Press.

Snee, N. L., & McCormick, K. A. (2004). The case for integrating public health informatics networks. *IEEE Engineering in Medicine and Biology Magazine, 23*(1), 81–88.

Starr, P. (1982). *The social transformation of American medicine: The rise of a sovereign profession and the making of a vast industry*. New York, NY: Basic Books.

Stewart, A. (2006). A shot-in-the-arm microchip could save your life. *Star-Ledger*.

Sullivan, D. A., & Weitz, R. (1988). *Labor pains: Modern midwives and home birth*. New Haven: Yale University Press.

Taylor, F. W. (1911). *The principles of scientific management*. New York: Harper Bros.

TFAH (Trust for America's Health). (2007). *Trust for America's health. Ready or not? Protecting the public's health from diseases, disasters, and bioterrorism*. Washington, D.C.: TFAH.

Thuemmler, C., Buchanan, W., Fekri, A. H., & Lawson, A. (2009). Radio frequency identification (RFID) in pervasive healthcare. *International Journal of Healthcare Technology and Management, 10*(1–2), 119–131.

VeriChip Corporation. (2007). *VeriChip Corporation: Company*.

VeriMed. (2006). *VeriMed patient identification*.

VeriMed. (2008). *Intro to VeriMed: FAQ*.

Vogel, K. M. (2008). Framing biosecurity: an alternative to the biotech revolution model? *Science and Public Policy, 35*(1), 45–54.

Winner, L. (1986). *The whale and the reactor: A search for limits in an age of high technology*. Chicago: University of Chicago Press.