

Security and Privacy After September 11: The Health Care Example

Peter Swire* & Lauren Steinfeld**

In September 2000, the Wall Street Journal published a poll that asked Americans what they feared most in the upcoming century.¹ The poll included a number of frightening concerns, such as international terrorism, global warming, and world war. Ranking first among the dozen serious issues, and listed as the first or second choice of 29 percent of respondents, was “erosion of personal privacy.” No other issue scored above 23 percent.

Only a year later, in the wake of the September 11 attacks on the World Trade Center and the Pentagon, security issues clearly became far more important in the public mind. Although no poll has re-asked the precise question posed by the Wall Street Journal, a range of polls in the months after the attacks showed significantly greater concern about public safety and noticeably lower salience for privacy issues.²

As one sign of the changed times, the Bush Administration proposed new legislation, ultimately named the USA-PATRIOT Act, just four days after the attacks. In the area of wiretaps and electronic surveillance, the proposal contained a number of provisions that had been previously rejected by Congress as too pro-surveillance.³ It included other new surveillance powers that had not ever been subject to any hearing or debate in Congress.⁴

Just the previous summer, the Clinton Administration had proposed updating the same laws in ways that also updated law enforcement authorities while being more protective of privacy. The House Judiciary Committee, with an overwhelming bipartisan majority, had amended the bill substantially further toward the privacy side. Now, following the attacks, the previous legislative momentum toward greater privacy protections suddenly shifted to greater government surveillance powers than anyone would have seriously proposed a year earlier. The USA-PATRIOT Act passed on [date]. Critics of the Act were able to make few amendments during its rushed consideration, although some of the most worrisome surveillance provisions will sunset in four years.⁵

This legislative about-face in the area of surveillance law raises a linked series of questions that we address in this Article. First, we explore the relationship between protecting privacy, an especially

hot issue before September 11, and protecting security, an especially hot issue since then. We do this by exploring the situations in which the two goals are antagonistic, what we call “privacy *vs.* security,” and other situations in which the two goals are complementary, what we call “privacy *and* security.”

A next issue to consider is the extent to which the shifting public sentiment about the relative importance of security and privacy should lead us to re-examine privacy initiatives put into place before September 11. The most far-reaching of these is the medical privacy regulation issued in 2000 under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and scheduled for compliance by health care providers, insurers, and others by April, 2003. In the wake of the September 11 attacks, for instance, we might wonder how well the HIPAA privacy rule allows for reporting to law enforcement officials about terrorist or other security threats. In the wake of the anthrax incidents from the fall of 2001, we might similarly wonder how well the public health reporting rules would work during a period of heightened security concern.

Fortunately, a careful inspection of the medical privacy rule shows that extensive public health and public safety protections were built into the final rule, even though it was drafted before September 11. Indeed, the scope of these protections is not surprising, in light of the extensive participation of both public health and public safety officials in the drafting of the regulation. In light of these existing protections, considerable skepticism is appropriate when examining new proposals to alter public health or public safety provisions in the HIPAA privacy rule. There should be concrete showings of particular need, not broad assertions that “everything is different after September 11.”

This inspection of the medical privacy rule is distinctly heartening, as is the conclusion in this article that implementing security can provide a useful opportunity to implement privacy. The statutory call for privacy protection in HIPAA was a result of an understanding in Congress that the shift to electronic medical records required that security and privacy be built in at the same time, as part of a unified upgrading of medical information systems. To an extent not often enough realized to date, this upgrading of systems means that we more often face a situation of security *and* privacy, working together, than we might otherwise have suspected.

II. “Security *vs.* Privacy” or “Security *and* Privacy”

In recent years, there has been a great deal of public debate on what measures to take to protect individual “privacy.”⁶ The term “privacy” is quite general and has been given a plethora of definitions. For our purposes, we define “privacy” as providing individuals some level of information and control regarding the uses and disclosures of their personal information.

In recent years, and even more since September 11, there has been a similarly intense debate about how to protect “security.” This term is also quite general and covers broad subcategories ranging from cybersecurity to airport security to national security. The primary focus of this article is information security – which we simplify to mean the prevention of unauthorized access, use and disclosure of information.

In the wake of September 11, the greater focus on information security manifests itself in a variety of ways. First, there is less tolerance for hackers or others who gain unauthorized access to information. Hackers less and less seem like playful young experimenters who are learning computer skills to power the New Economy. Instead, anyone entering a Pentagon or other system more and more seems like a computer criminal deserving of societal sanction. Since the attacks, many of us have a general sense of vulnerability and an accompanying uneasiness about the

unauthorized use of virtually *anything*. Second, there is broader concern about cyber-security and the need to protect critical infrastructures — the telecommunications system, electric power system, banking system, and so on. Many measures to protect critical infrastructures were underway before September 11.⁷ We are now on greater alert. Third, the importance of having effective computer back-ups has become more evident. The attacks on the World Trade Center caused great damage to Verizon’s telephone switching system and utter destruction to numerous firms’ on-site information systems. Fortunately, many of the sophisticated enterprises located at the Center had effective back-up systems offsite, enabling continued processing of banks’ payments and general resumption of access to databases often within hours or days. It seems that many companies had created effective back-ups during the lead-up to Y2K, but the attacks reminded business and government leaders of the need to have such back-ups in the future.

With this greater attention to security, there is a general sense that privacy has become a less important issue. We sometimes see “security vs. privacy”, where the two are antagonistic. Notably, greater security can often be accomplished when security forces have greater information – raising privacy risks. That is, security sometimes means greater surveillance, information gathering, and information sharing. There is greater security when airport personnel search you and your bags, when we know the locations of suspected terrorists, when different law enforcement agencies share information on threats, and so on. Security interests are advanced when law enforcement is able to monitor the online movements of hackers, when hospitals report cases of anthrax infection, when ambulance drivers report possible terrorists. The list goes on. But the heart of it is that greater information flows can promote security by getting information to the proper decisionmakers.⁸ As these information flows increase, privacy decreases.

The surveillance provisions of the USA-PATRIOT Act, in our view, generally illustrate “security vs. privacy.” To take only a few examples, the Act:

- Increases the scope of roving wiretaps, where law enforcement can access communications from any device used by a suspect, rather than needing to get a new order for each phone or computer;
- Broadly increases the scope of emergency orders to trace communications, which apply before a judge approves a court order;
- Allows one court order for tracing communications to apply nationwide, rather than requiring a new order in the district where a communications provider operates;
- Allows a much broader category of cases to use information developed under the Foreign Intelligence Surveillance Act, where those subject to wiretaps are not informed of the surveillance even after the fact;
- Permits information developed by a grand jury in a law enforcement proceeding to be shared with intelligence agencies;
- In a “computer trespasser” provision that was never the subject of a Congressional hearing, permits law enforcement officials to set up extended residence at a communications provider to surveil the communications of unauthorized users.⁹

The focus on surveillance, so evident in the USA-PATRIOT Act, nonetheless captures only part of the story. In many instances we see “security *and* privacy”, where the two are complementary. Under the standard approach to privacy protection, good security is an essential fair information practice. After all, good privacy policies are worth very little if hackers or other outsiders break into the system and steal the data. Both privacy and security share a complementary goal — stopping unauthorized access, use, and disclosure of personal information. Good security, furthermore, does more than keep the intruders out. It creates audit trails about which authorized users have accessed particular systems or data. These audit trails allow an accounting over time of who has seen an individual’s personal information. The existence of accounting mechanisms both deters wrongdoing and makes enforcement more effective in the event of such wrongdoing. To take one example, the HIPAA medical privacy rule requires an accounting (a log) of who has seen a patient’s data for other than treatment, payment, or health care operations purposes. Patients can see these logs, and the existence of the accounting mechanism will likely support both privacy (patient confidentiality) and security (prevention of unauthorized uses of the system).

The importance of security *and* privacy is heightened by an institutional dynamic that becomes especially salient after September 11. Our experience in implementing privacy in the U.S. Government and in the private sector suggests that the most cost-effective and thorough implementation of privacy occurs at the time of a computer system overhaul. This approach was fundamental to the way that Congress designed and the Clinton Administration implemented HIPAA. HIPAA required standardized electronic formats for most health transactions. Implementation of the HIPAA transaction rule, which defined those formats, was joined together with implementation of the security and privacy rules.¹⁰ In this way, both security and privacy could be included as part of the system overhaul of moving many medical records from paper to electronic formats.

This idea of linking privacy with a system overhaul becomes even more important after September 11. Government and private computer system owners are now making security a much higher priority, and many systems will be overhauled in the interest of improved security. Instead of this being a systematic threat to privacy, as suggested by the “security *vs.* privacy” perspective, these new systems present an important opportunity to build good data handling practices generally into the new systems. The Privacy Commissioner for the Province of Ontario, Ann Cavoukian, has launched an initiative called [cite] that is designed expressly to team security upgrades with good technological practices for privacy protection. When greater resources are devoted to computer security, there is a strategic opportunity to upgrade good privacy and other data handling practices at the same time.

I. The HIPAA Privacy Rule, Public Health, and Public Safety

The discussion thus far has shown that it is possible for security and privacy to work either together or at cross-purposes. To the extent the latter is true, a worrisome question after the World Trade Center attacks is whether the HIPAA privacy rule was drafted without sufficient attention to the public health and public safety concerns that became so prominent after the attacks. We now briefly describe the privacy rule and then examine the extent to which it already incorporates these public health and public safety concerns.

A. The HIPAA Privacy Rule

As discussed above, the Health Insurance Portability and Accountability Act of 1996 required health providers and plans to shift toward standardized, electronic formats for sharing medical records. Congress initially contemplated that it would enact medical privacy legislation by the summer of 1999. When it did not do so, the Department of Health and Human Services assumed the power to issue a HIPAA privacy regulation. The proposed rule was announced in October, 1999. After a round of 53,000 public comments, President Clinton announced the final regulation in December, 2000. In April, 2001 President Bush confirmed that the rule would go into effect essentially as drafted, with actual compliance by April, 2003.

To summarize key aspects of this far-reaching rule, the federal regulation will now require health care providers, health plans, and health care clearinghouses to:

- Provide notice of their information practices;
- Use and disclose protected health information only with patient permission, except in cases where designated national priorities warrant otherwise;
- Permit patients to access and request correction of their records;
- Provide patients an accounting of to whom their protected health information has been disclosed;
- Limit the use and disclosure of protected health information to the minimum necessary amount;
- Implement security safeguards to protect against unauthorized access or disclosure; and
- Obtain satisfactory assurances, via a written contract, that their business associates using protected health information are protecting the privacy of that information.

A central feature of the privacy rule is a set of limitations on uses and disclosures of protected health information. In general, the rule prohibits protected health information (“PHI”) from being released to third parties, or used by the health care industry, except as directed by the patient in signed consent or authorization forms.¹¹ If the rule did not have exceptions, it would indeed impose serious obstacles to anti-terrorism efforts. Any government agency would be refused access to medical information unless the subject of the record provided written documentation permitting such release. Permission might be difficult to get, to say the least, if the individual were engaged in terrorist activities.

The rule does have exceptions, however. Patient permission is not required for defined national priority purposes.¹² It is only by examining these exceptions carefully that we can determine the extent to which the HIPAA privacy rule, drafted before September 11, remains appropriate in light of heightened concern about terrorist activities.

B. Disclosure for Public Health Purposes

In October 2001 the appearance of anthrax spores in the U.S. mails, and subsequent infection of dozens of people, created an array of important challenges for the public health community. It was abundantly clear that use and disclosure of considerable personal health information would be needed to respond to these challenges.

Public health officials, for instance, needed to understand the scope of the anthrax impact, including knowing the number of anthrax-infected people. To determine the scope of the problem, PHI was needed from physicians, hospitals, emergency rooms, and laboratories, as well as from public health authorities and anyone else possessing information on the threat.

Public health officials, especially during the height of the anthrax scare, needed to identify people who might be at risk for infection, and thus had reason to learn about the activities and contacts of individuals whose infection was already suspected or confirmed. This identification effort required disclosing PHI to co-workers, neighbors, family members, and at times the general public. These “warning” disclosures often come with the victim’s permission. One can easily envision, however, situations where the permission will not be provided. Sometimes there are administrative snags, such as when the patient is no longer easily available to give signed permission. Law-abiding people might choose not to give permission, including unusually private people, people in denial of their illness, those seeking to guard loved ones from painful information, and those suspicious for whatever reason about turning over information to government agencies. Those on the wrong side of the law, from undocumented aliens to criminal conspirators or terrorists, would generally be unwilling to disclose their activities or confederates.

The need for information sharing would be even greater if the public health threat came from a highly communicable and deadly disease, such as smallpox. In some instances, such as an epidemic or the detection of infectious carriers of the disease, public health authorities might require PHI of thousands or even more people to contain the disease, vaccinate exposed populations, and take other counter-measures.

With the importance of information sharing clearly in mind, we turn to the relevant language in Section 512(b) of the privacy rule. The rule generally authorizes a covered entity such as a hospital to disclose PHI for defined “public health activities and purposes.” Notably, disclosure is allowed to any

“public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions.”¹³

Going beyond public health authorities, the rule authorizes disclosure to a

“person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the covered entity or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.”¹⁴

The effect of this regulatory language is great flexibility in the release of public health information. The term “public health authority” is defined broadly.¹⁵ PHI can flow to any public health authority that is “authorized by law” to collect or receive such information for public health purposes. These purposes include, but are not limited to, the reporting of disease and injury and the conduct of three undefined but apparently broad categories of activity — “public health surveillance, public health investigations, and public health interventions.”

Applied to an anthrax or smallpox outbreak, it would appear that the current privacy regulation would permit a hospital to share information with local, state, and federal authorities in ways that would further the public health. The only important limit under the regulation appears to be the requirement that the public health authority be “authorized by law” to collect or receive the information. One can imagine a particular state or local authority that currently lacks this sort of formal authorization. In such instances, there is a logical basis for exploring whether to update the law to provide authorization. Such updating, however, is entirely within the discretion of the relevant legislature and the HIPAA privacy rule does not constrain that decision.

In many ways, as we examine further below, the more serious legal issue arises from a different gap in the HIPAA legislation. The statute applies directly only to “covered entities,” which are health providers, health plans, and health care clearinghouses. It applies indirectly to the business associates of those entities, such as agents who handle health information on behalf of one of the covered entities. The statute does not, however, apply to public health agencies or those who receive information from such agencies. In drafting the regulation, HHS simply lacked authority to craft privacy and security protections once the data was in the hands of the public health agencies. In light of the liberal rules for supplying public health information to the agencies, the biggest privacy and security issues going forward are likely to arise in the largely-unregulated instances once the public agencies have received the data.¹⁶

C. Reporting Suspicious Activity

We now turn to the provisions under the HIPAA rule that govern the release of health information to law enforcement and other public safety officials. Prior to the rule, professional ethical codes and some state laws limited the disclosure of health information to these officials. There was no national law limiting disclosure, however, and police officers could simply walk into a doctor’s office or emergency room in many jurisdictions and receive patient information without the patient’s consent and without legal limits. The privacy rule created new requirements before covered entities could share health information with law enforcement officials.

In considering whether the new privacy rule went too far, consider how health information might be important to national security in the following examples:

- Suppose as an emergency medical technician you rush to the scene of a terrorist bomb attack. You observe, only minutes after the blast, an individual who appears to have been wounded by the attack, who is agitated, and who asks you to treat him but not report to anyone that you have seen him.
- Suppose that you are a nurse treating an individual for possible anthrax exposure, and learn that the patient is a scientist with strong anti-American views.

In both of these cases you might reasonably believe that you have evidence that the person is a terrorist who has already struck or who is planning to strike. But you are also a health care professional, with a general duty to protect the confidentiality of patient data. If evidence of every crime becomes a reason to disclose information to the police, then underage drinkers, users overdosing on drugs, HIV-positive people who have not practiced safe sex, and people who may be a danger to themselves or others all may avoid getting needed health care.

How does the HIPAA privacy rule address this tradeoff between reporting the information and keeping it confidential? The answer is that HIPAA specifically treats public safety as a national priority that, under certain circumstances, trumps the need to obtain patient permission for disclosures of health information. For the bomb attack, anthrax scientists, and other security threats it does so through three primary provisions, for national security, emergency circumstances, and disclosure to law enforcement more generally.

1. *National security provision.* To begin with, the little-discussed national security provision in HIPAA provides one way for the emergency medical technician or nurse to report their suspicions. Section 512(k)(2) of the rule states that a covered entity “may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities” authorized by the National Security Act and implementing authority.¹⁷

We hope and expect that the vast bulk of medical professionals will go through their career without ever having any reason to disclose information under the HIPAA national security provision. Its presence in the regulation, however, makes clear that national security information can be reported by medical professionals even without patient consent.¹⁸ The reassuring corollary, for those wondering whether the privacy rule undermines national security, is that the drafters of the privacy rule had in fact contemplated possible national security implications before September 11.

2. *Emergency circumstances.* Section 512(j) of the privacy rule permits a covered entity to come forward with health information in certain serious situations, including the nurse and possibly the EMT case. The covered entity must comply with applicable law and standards of ethical conduct. If it does, then it may disclose PHI if it believes, in good faith, that the use or disclosure “is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person *or the public*; and is to a person or persons reasonably able to prevent or lessen the threat”¹⁹ (emphasis added). Reporting about a person apparently engaged in spreading anthrax would seem clearly to lessen such a threat to the public safety. Reporting the possible terrorist bomber would qualify if, in good faith, the covered entity believed that capture of the bomber would lessen a serious and imminent threat to the public safety.

Section 512(j) has a second potentially relevant provision. Disclosure is permitted by the covered entity if it would be “necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim.”²⁰ The relevant factual question here would be whether the apparent terrorist bomber had, through his attempt to have the medical provider hide his identity, made “a statement by an individual admitting participation in a violent crime.” The mere statement of wanting confidentiality likely would not be such a statement, because there are so many other reasons an individual might want confidentiality.²¹ Nonetheless, if the EMT’s patient actually confessed to participating in the terrorist attack, the EMT could certainly report to law enforcement.

3. *General Law Enforcement Provisions.* The national security and emergency circumstances provisions each provide possible ways for the nurse or the EMT to volunteer information to the authorities about possible terrorist activities. The general law enforcement provisions in the privacy rule, by contrast, generally govern how a covered entity may disclose information in response to questions from law enforcement.

The basic rule is that a covered entity may supply PHI to a law enforcement official based on a court order, grand jury subpoena, or special administrative subpoena that certifies compliance with privacy-protective criteria.²² This approach is less strict than the standard requested by many privacy advocates and industry groups, which would have been the Fourth Amendment standard of probable cause as found by an independent magistrate. The approach is stricter, however, than the previous federal rule that allowed medical providers to turn over medical records without any legal process. As applied to our nurse and EMT examples, the general rule would permit covered entities to supply the records to law enforcement officials if and only if they made a lawful request to the covered entity that had the relevant information.

The rule is a notch less strict where a law enforcement official requests information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. In such instances, the covered entity may supply basic identifying information, but not the entire medical record, even in the absence of legal process.²³ This provision might be very useful to law enforcement, for example, in finding a suspected terrorist with a known description, without the need to get legal process for each emergency room or doctor's office in a large city.²⁴

4. *Summary on reporting suspicious activity.* The existence of the national security, emergency circumstances, and law enforcement provisions indicate that there was extensive deliberation in the drafting of the HIPAA privacy rule about how to achieve both privacy and protection of public safety. When the Clinton Administration made detailed legislative recommendations in 1997, it supported the status quo for law enforcement, with no federal legal limits on the disclosure of health information to police. After public debate on the issue, the proposed HIPAA privacy rule in 1999 added the general law enforcement provisions much as they exist today. After further public debate and extensive written comments, including from the Department of Justice, the final privacy rule in 2000 added the emergency circumstances provision. At the time the rule was announced, President Clinton also issued an Executive Order that limited the way that information gathered for health oversight purposes could be used in law enforcement activities.²⁵

This history in the law enforcement area matches the discussion above about public health. In both instances, there was substantial consideration of the issues during the drafting of the privacy rule. Individuals in good faith may disagree with the outcome of the final rule. Some will believe that the law enforcement provisions are too strict, frustrating efforts to protect the public safety. Others will believe them too loose, allowing police to rummage too easily into individuals' confidential medical records without the requirement of an independent magistrate first issuing a warrant. The examples of the nurse and the EMT, however, suggest that existing law would allow disclosure of medical information in situations involving evidence of terrorism. Any change to the law enforcement provisions should be based on particularized arguments about specific flaws, not vague assertions that the relevant issues are entirely new since September 11.

IV. Proposed Changes to Public Health Laws

The article to this point has discussed how the existing HIPAA privacy rule already reflects extensive consideration of the public health and public safety issues that came to the forefront after the 2001 terrorist attacks. On October 23, 2001 symposia co-authors Lawrence Gostin and James Hodge released their Model State Emergency Health Powers Act to provide comprehensive guidance to state lawmakers looking to be better prepared for public health emergencies. The Model Act

would appoint a planning Commission to develop a public health emergency plan. It would establish criteria and processes for declaring a “state of public health emergency.” It would provide for special powers during such a state of emergency, including for example: access to and control of materials, facilities, roads, and public areas; safe disposal of infectious waste and human remains; protecting persons via medical examination and testing, vaccination and treatment, and isolation and quarantine.

In terms of information policy, James Hodge at the Symposium proposed what he called a “model of information sharing” for health information rather than the model of information privacy that he sees reflected in the current HIPAA rules. The Model Act mandates a great deal of information sharing at all times, and not just during the state of public health emergency that is addressed in some other provisions. Section 301 provides for mandatory reporting by health care providers (including laboratories), coroners, and medical examiners of “all cases of persons who harbor any illness or health conditions that may be potential causes of a public health emergency.” It requires that pharmacists report any unusual or increased prescription rates, unusual types of prescriptions, or unusual trends in pharmacy visits that may be potential causes of a public health emergency. Section 302 addresses “Tracking” and requires public health authorities to identify all individuals thought to have been exposed to an illness that might cause a public health emergency, interviewing such individuals to identify exposed individuals and “develop information relating to the source and spread of the illness.” Section 303 allows information sharing between and among the public health authorities, public safety authorities, tribal authorities, and federal health and public safety authorities. These provisions, in sum, call for substantial, ongoing and often legally required information collection and sharing of medical data by relevant authorities.

Along with these new information collections, the Model Act includes provisions incorporating privacy principles. Section 303 limits information sharing among relevant agencies to the amount “necessary for the treatment, control, investigation, and prevention of a public health emergency.” Section 607 permits access to PHI only for those having a legitimate need for the information to provide treatment, conduct epidemiological research, and investigate the causes of transmission. This section also limits disclosure to defined classes such as family members, federal agencies pursuant to law, court orders, and to identify a deceased individual or determine the manner or cause of death.

In examining the Model State Emergency Health Powers Act, we begin with agreement that existing state public health law, often drafted in response to communicable disease epidemics of a century ago or more, may well need updating in numerous respects. We also note that the authors Gostin and Hodge have previously worked extensively on medical privacy issues in their Model State Public Health Privacy Act of 1999. Their December 21, 2001 draft addressed a number of the privacy criticisms that were made of the original October 23, 2001 draft and they have indicated that they would support considering the model privacy act with the model emergency health powers act.

With that said, however, we have a number of concerns about the current form of the project. The first concerns its title. It is called the “Model State Emergency Health Powers Act”, yet many of its provisions, including the mandatory information sharing provisions, would apply on a permanent basis and not only once an emergency had been declared. It does a disservice to the public debate to pretend that a bill is about public health emergencies when its provisions instead apply much more generally.

Second, the current draft is still very incomplete in the area of privacy protections. The Health Privacy Project has submitted detailed comments showing how the Model Act lacks standard privacy protections including: access and disclosure requirements for data collected prior to a public health emergency; limits on the amount and type of PHI needed to accomplish specific purposes; limits on which sort of government agencies can access the data; enforcement and penalty provisions for violations; information security requirements; and so on.

The importance of including these privacy protections is made even clearer in light of our discussion, above, of “security *and* privacy.” A key point there was that privacy protections will be implemented more effectively and at lower cost if they are included at the time of a system overhaul. The anthrax incidents have focused far greater political attention on the public health system, creating what may be a once-in-a-generation opportunity to update public health laws. The Model Act would require large new categories of information sharing. For the new public health system to handle data appropriately, effective privacy protections should be created at the same time. If we don’t, we can readily anticipate incidents where state and local public health agencies are embarrassed in the media by incidents of sloppy handling of the increased flows of confidential health data. The result, in turn, could be greater reluctance on the part of many patients to share data with their providers and providers to share data with the public health agencies, undermining the mission of public health. For these reasons of public health protection and cost-effective overhaul of the systems, privacy protections should be an integral part of new initiatives to increase public health data flows.

A third concern addresses the “model of information sharing” that James Hodge advocated at the Minnesota Law Review Symposium. We do not agree that “information sharing” is the way to describe how to handle patients’ medical records. The United States is now in a period of implementing the HIPAA privacy and security rules, a large effort that underscores the importance of treating patients’ records with care and confidentiality. We believe that confidential treatment of medical records is a vital norm, widely shared by medical professionals and almost universally favored by individual patients. To abandon that norm, and shift to a “model of information sharing” for medical records, would be to undermine the implementation of HIPAA and the public confidence that patients can trust their medical providers.

The existing HIPAA privacy rule offers a better way to conceptualize the relationship between confidentiality and data sharing. The rule begins with an assumption that PHI will be treated confidentiality. It then contemplates that PHI can be shared for the basic purposes of treatment, payment, and health care operations. Patients want and expect their medical records to be used by those engaged in treatment and these other basic purposes. The rule in addition contemplates a series of national priority purposes, including public health, law enforcement, national security, medical research, and so forth. For each of these purposes, there was an extensive public process to determine the situations in which PHI could be used or disclosed without patient consent.

This article’s examination of the public health and reporting suspicious activity indicates that the HIPAA privacy rule appears to stand up well to the changed circumstances after September 11. At the Minnesota Symposium, one of the co-authors (Swire) asked James Hodge if he could name a single instance where the HIPAA provision on public health posed an obstacle to sensible sharing of information. Mr. Hodge could not name a single instance, although this questioning occurred on the spot and greater research might reveal such an instance. In the absence of identifiable problems in

the current privacy rule, it seems premature to say the least to claim that an entirely new paradigm, the “model of information sharing”, is somehow needed at this time.

V. Conclusion

In the days, weeks, and months after the attacks on the World Trade Center and the Pentagon, many of us have had the feeling that we wanted to “do something” to help respond to the tragedy and ensure that similar attacks do not happen again. Politicians seeking public approval and possible re-election are probably at least as prone as ordinary citizens to want to show that they are “doing something” to face the new circumstances. One understandable result was to pass new laws that demonstrate the strong, and often sincere, feelings of political leaders and the public.

The new surveillance provisions of the USA-PATRIOT Act are one example of the political response to the September 11 attacks. Time will tell us much about the desirability of the new government powers. By the time the sunset expires in 2005, we will be in a better position to assess whether the new powers are a valuable response to the new threats of a dangerous world or else an overreaction to a terrible, one-time tragedy. Between now and 2005 those of us who care about these issues have an important homework assignment. We should help the Congress to understand the strengths and weaknesses of the USA-PATRIOT surveillance provisions, and take advantage of the intervening time to have a thoughtful and informed public debate on how to achieve security *and* privacy in this area.

In the area of medical privacy, this article’s analysis indicates that the rule stands up well to the concerns of the post-September 11 era. Concerns about public safety are met by existing provisions that permit disclosures to protect national security, to react to emergency circumstances, and to respond to law enforcement inquiries. Concerns about public health, as suggested by the anthrax incident, are also met by the current rule. We are not aware of any needed disclosures for public health purposes that are prohibited by the medical privacy rule.

A broader message of this article is that the protection of privacy and security is often best done together. The most effective and least costly way to protect both is to insist on doing so at the time of a computer system upgrade. For medical records, we are in the middle of a one-time shift from the mostly-paper records that existed in 1990 to the mostly-electronic records that will exist by 2010. The 1996 HIPAA statute correctly required that privacy and security protections should be an integral part of this one-time shift. Health care providers and plans will assuredly shift to electronic systems when required to do so in order to qualify for payment by Medicare and other sources. There is no better time to insist on shifting to privacy and security safeguards as well.

This insight teaches a lesson about how state public health laws should be updated as legislatures react to the experience of the anthrax attacks. The anthrax attacks, and the resulting public attention to public health issues, create the possibility of a once-in-a-generation overhaul of public health statutes. These state public health authorities are not generally covered by the HIPAA privacy and security requirements. If and when state legislatures move forward with new public health legislation, it is crucial to create privacy and security safeguards as an integral part of the new information systems that will handle our public health records in the future. This is the best route to achieving the privacy *and* security that most Americans desire and that we can achieve.

(Endnotes)

* Professor, Moritz College of Law of the Ohio State University and Consultant, Morrison & Foerster LLP. From March, 1999 to January, 2001 Professor Swire served as the Clinton Administration's Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that position, Professor Swire was White House coordinator for the proposed and final medical privacy rule and also chaired a White House Working Group on how to update wiretap and surveillance laws for the Internet age. He thanks Larry Glasser for research assistance on this article. Web: www.osu.edu/units/law/swire.htm. This article will be published in final form in the Minnesota Law Review symposium on privacy law.

** Chief Privacy Officer, University of Pennsylvania and Consultant, Morrison & Foerster LLP. From June, 1999 to January, 2001 Ms. Steinfeld served as the Associate Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that position, she headed a number of working groups for the medical privacy rule and worked extensively as well on numerous other privacy issues.

¹ [Cite to WSJ of September 9, 2000]

² [Cite recent polls.]

³ Examples include broader powers to conduct roving wiretaps, expansion of the use of foreign intelligence surveillance wiretaps, and easier access by law enforcement to voice mail messages.

⁴ A notable example is Section 217, which allows law enforcement to monitor telephone and e-mail communications on an ongoing basis to catch suspected computer hackers.

⁵ For analysis of the USA-PATRIOT Act, see [cite Swire Brookings and Atlanta Constitution articles].

⁶ For some of the history, see Peter P. Swire, "The Surprising Merits of the New Financial Privacy Law," [in this symposium].

⁷ Cite National Plan.

⁸ One of the co-authors is engaged in ongoing research into the question of when greater disclosure either helps or harms computer security. For an early version of the research, see Peter P. Swire, "What Should be Open or Hidden in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory," *available at* [cite to TPRC site].

⁹ [Cites for all these to come.]

¹⁰ The linked nature of the transaction and privacy rule can be seen, for instance, in the statement of HHS Secretary Shalala in the August, 2000 announcement of the transaction rule, where she underscored the linkage. [cite] The cost-benefit analyses of the two bills were also conducted in tandem, with the cost savings estimated for the transaction rule more than offsetting the estimated net costs of the privacy rule. [cite]

¹¹ Cite to 164.506 and 164.508 and explain briefly the difference between consent and authorization.

¹² In addition to the public health and public safety provisions discussed below, other exceptions were defined for uses and disclosures: required by law; about victims of abuse, neglect or domestic violence; for health oversight activities; for judicial and administrative proceedings; about decedents; for cadaveric organ, eye or tissue donation purposes; for research purposes; for specialized government functions, including for military activities, protective services for the President, medical suitability determinations for the State Department, correctional institutions, and public benefit programs; and for workers' compensation. Sec. 512. This extensive list, based on extensive comments within the government and from the public, suggests the wide range of issues that were considered in the promulgation of the HIPAA privacy rule. Criticisms of the rule (some of which are undoubtedly valid) should thus be based on particularized attention to its shortcomings as drafted rather than broad assertions that the rulemaking process did not consider a particular issue or concern.

¹³ Section 512(b)(1)(i).

¹⁴ Section 512(b)(iv).