

NC STATE UNIVERSITY

Address to the Healthcare and Technology Subcommittee

By David L. Baumer, Ph.D., J.D.,
Attorney at Law,
Head, Business Management Dept.
College of Management,
North Carolina State University,
Raleigh, NC 27695

Poole College of Management
Campus Box 7229
Raleigh, NC 27695-7229

Re: Not What the Doctor Ordered: Health IT Barriers for Small Medical Practices

Date and Location: Thursday, June 2, 2011 at 10:00 A.M. in room 2360 of the Rayburn
House Office Building

My name is David Baumer. It is a pleasure and an honor to address the Healthcare and Technology Subcommittee. Let me give you a little of my background and then address the issues that I was asked to discuss, which are “security and privacy concerns of health IT,” and “possible liability issues associated with small practices.”

For the past 5 years, I have been the Head of the Business Management Department, within the Poole College of Management, at North Carolina State University in Raleigh, North Carolina. My educational background is that I have a Ph.D. in Economics from the University of Virginia and a J.D. degree from University of Miami. I have been a member of the North Carolina State Bar Association for the past 31 years. My area of specialization is law and technology, which also makes use of my training in economics.

Much of my work is summarized by my vita and webpage, which can be accessed at: <http://www.poole.ncsu.edu/index-exp.php/directory/dossier/david-baumer/>. During the past 15 years at NCSU, I developed and taught a graduate course entitled, “Technology, Law and Internet.”¹ In addition to analyzing the interface between IP and the Internet, the course dealt extensively with privacy and security issues, particularly online privacy and security. Referring to my vita, during the past few years I have looked at interventions of the Federal Trade Commission to preserve and promote reasonable consumer and user privacy and security [1, 5, 9, 15].² Among the issues that I have looked at along with colleagues from the Computer Science Dept. at NCSU (and colleagues from Virginia Tech, Georgia Tech and Carnegie Mellon) are the consequences of security breaches by firms that have been entrusted with personally identifying information (PII) [9, 15]. In my work with Professor Annie Anton at

¹ <http://www4.ncsu.edu/~baumerdl/index.htm>.

² The numbers referenced in brackets correspond to Part II. of my vita beginning on page 2.

NCSU, two firms we examined were an airline company (Jet Blue) and a credit bureau (ChoicePoint), both of whom were arguably negligent in their protection of PII and one was subject to substantial fines by the FTC.³

In 2004, along with two NC State colleagues, I wrote an article that was published by *Computers and Security* entitled, "Internet Privacy Law: A Comparison between the United States and European Union" [17]. In writing about privacy laws in the US relative to the EU, it became evident to me that protection of PII is much more comprehensive in the EU than in the US. More recently, in the Winter of 2011, along with colleagues from Virginia Tech and Georgia Tech, I coauthored an article entitled, "Privacy and Security in the Implementation of Health Information Technology (HER): US and EU Compared", published by the *Boston University Journal of Science and Technology Law* [2]. This article extensively reviews US and EU healthcare privacy law in light of recently enacted legislation, including HIPAA Privacy and Security Rules that have modified by the 2009 HITECH Act.⁴

Relying on prior studies, the points we make regarding EHR in the Boston University article are that:

- (1) Adoption of EHR could result in huge savings in national healthcare expenses (possibly as much as 6% of the total of the \$3 trillion spent on healthcare annually) [2],
- (2) EHR will reduce medical errors, and
- (3) EHR adoption result in improved quality of care.

Centralized and accessible healthcare records could bring about a National Health Information Network (NHIN) that will be one result of a public-private partnership that can be used to provide "anytime, anywhere health care information and decision support...via a comprehensive knowledge-based network of interoperable systems."⁵ According to a study by the Rand Corporation the adoption of health information technology (HIT) could save \$77 billion annually from efficiency gains. However, it is important to note that much of these gains can only be achieved if all, or nearly all, of the healthcare organizations participate in sharing EHRs.⁶ In other words, the economic efficiency benefits of using EHR are not linear, but rather accelerate for the entire healthcare system as the percentage of medical records in an electronic format approaches 100%.

³ ChoicePoint was fined a total of \$15 million, \$5 million to a consumer injury fund and \$10 for unfair and deceptive trade practices. <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.

⁴ Health Information Technology for Economic and Clinical Health (HITECH) Act, sec. 13402, Pub. L. No. 111-5, 123 Stat 115 (2009).

⁵ Hiller, McMullen, Chumney, and Baumer [2]. Thanks to my mother-in-law who lives in Delray Beach, FL, also note voluntary efforts by organizations such as the South Florida Regional Extension Center (SFREC), which is a non-profit organization created last year to assist health-care providers, especially those with limited resources, staff and time as they convert to electronic medical records. Daniel Vasquez, SunSentinel.com, Monday, May 9, 2011.

⁶ Network externalities are created when there is near universal use of a system. The importance of network externalities has been discussed and validated in a number of studies, S. J. Liebowitz & Stephen E. Margolis, "Network Externality: An Uncommon Tragedy, 8.2 of *Journal Econ. Perspectives* 133, 134 (Spring 1994) In healthcare the significance of network externalities has been discussed in John W. Hill et al., "Law, Information Technology, and Medical Errors: Toward A National Healthcare Information Network Approach to Improving Patient Care and Reducing Malpractice Costs," 2007 *U. Ill. J.L. Tech. & Pol'y* 159 (2007).

There is plenty evidence supporting the proposition that in addition to reducing healthcare costs directly, widespread adoption of EHR would reduce variability in the healthcare provided due to dissemination of best practices and more sophisticated use of healthcare data. Accessible healthcare data could provide more reliable analysis of hospital and physician performance outcomes, monitoring chronic diseases, monitoring medication adherence, promotion of safety metrics and a host of other secondary efficiency benefits [2, at 6]. The improvement in healthcare should be accompanied by a reduction in medical malpractice for the reasons state above, though this result is contested by other researchers.⁷

Huge efficiency gains in the delivery of healthcare as well as medical research, potentially achievable through near-universal adoption of EHR, are offset by possible increased risks to the privacy of individual medical records. Polls indicate that a majority of the U.S. public is skeptical of the ability of healthcare providers and organizations to ensure medical records will not be abused or facilitate medical identity theft (MIT) [2]. Among the abuses mentioned by survey respondents are providing unauthorized access to private medical data by marketing firms, employers, and insurers. In addition, survey respondents mentioned significant concerns about loss of control of their medical records and having to rely on the security practices of unknown firms to protect their sensitive medical information [2].⁸ Medical identity theft can be defined as the use of personally identifying medical information to gain access to health treatment or to file for reimbursements for false medical treatments, which could result in both diminished healthcare quality and financial losses, among other risks [2, at 7]. Regardless of the form of the abuse of medical records, having electronic, rather than paper, medical records enables identity thieves and fraudulent or unethical medical firms to potentially cause far more harm to patients. To state the obvious, once security is breached, thousands and even millions of records are available to skilled hackers.

In the EU, privacy laws are more comprehensive and deal with various scenarios, such as the right to compile personal information about citizens, the sensitive status of medical records, and document destruction policies [17]. In our recent Boston University article [2], we point out that EU medical privacy law is more wide-ranging than such privacy protection in the US and further, that use of EHR is much higher in the EU than in the US. It is certainly not clear that more comprehensive privacy laws led to greater adoption of EHR in EU countries, but there is some evidence that EU privacy laws have not deterred adoption of EHR.

Based on my work, all of which is coauthored with other leaders in the fields of online privacy and security issues, I can confidently make the following statements:

1. There are enormous potential efficiency gains in healthcare if electronic healthcare records become the norm,
2. The barriers to more widespread adoption are technical, economic, cultural, and legal,

⁷ See article by Jean DerGurahian, <http://searchhealthit.techtarget.com/healthitexchange/healthitpulse/liability-and-ehrs-how-electronic-information-changes-legal-landscape/>.

⁸ In [2] we note that, "HIPAA contains so many exceptions to when a patient's consent is needed to share information, that in practice is offers limited instances for patient choice;..."

3. Economic issues are addressed in the Patient Protection and Affordable Care Act by subsidizing healthcare firms that transform their records to an electronic format.⁹
4. There is substantial legal uncertainty as to the liabilities firms face if a mistake is made in the acquisition, storage, or transmission of medical PII.

I was asked to comment on 4., immediately above, but the technical, economic, and legal issues are inextricably intertwined. For example, a major technical issue that affects small firm adoption of EHR is interoperability and the consequences thereto. As stated above, the benefits of EHR take place when a patient's medical records can be accessed in a relatively short period of time and these records are complete or nearly complete. Quite obviously, for a small firm whose system may not be completely interoperable with other EHR systems, adoption of EHR can result in a double penalty: firstly that incur substantial startup costs in time and money to create an EHR infrastructure, secondly these are not receiving the benefits of information sharing.

According to anecdotal information that I have gathered and received, EHRs are increasingly being pooled, but accessing the pooled data is still problematic for some firms, particularly small healthcare providers. It was mentioned to me by doctors and some patients who talked physicians and other medical staff, that codes used by contributors to the pooled medical information were not standardized and therefore sharing of data and interoperability remains a goal, but is not reflective of current reality.

Let me close by making several points:

1. At least in the short run, widespread adoption of EHR will not reduce legal uncertainty. According to a recent article in the *New England Journal of Medicine*, "EHRs hold considerable promise for preventing harmful medical errors and associated malpractice claims, but on the other hand, despite experts' optimism, there is no evidence that that use of EHRs reduces diagnostic errors." In a Nov. 23, 2010 article by Jean DerGurahian, which cites the *New England Journal of Medicine* article, "The question is whether EHRs will help providers defend against such claims [malpractice and medical liability] or leave them more vulnerable—the answer seems to be, they will do both."
2. In an article [1] that I recently coauthored with Professor Travis Breaux of Carnegie Mellon, we explored what firms can do to avoid liability in the form of fines from the FTC [1]. We state that "Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes 'reasonable' security measures for several reasons, including:"

⁹ [Pub.L. 111-148](#), 124 [Stat.](#) 119, to be codified as amended at scattered sections of the [Internal Revenue Code](#) and in [42 U.S.C.](#)

- A. Compliance (creation and use of reasonable security measures) changes with the emergence of new security vulnerabilities due to innovations in IT. In other words, it is not enough simply to invest in IT infrastructure, users must be alert to changes in IT that make existing security measures possibly superseded,
 - B. Compliance requires knowledge of specific security measures and current best practices. For example, note that Microsoft was prosecuted by the FTC in 2002 when it claimed that security for its Passport Wallet products [5, at 292] was improved relative to its existing products.¹⁰ In the consent decree, the FTC required that Microsoft implement administrative, technical, and physical safeguards appropriate for the respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers." In effect, the FTC claimed that Microsoft's current security was not "state of the art" and that the FTC had some definite ideas from improvement. No customers of Microsoft's Passport products were ever victimized by identity thieves or other abusers, such as spammers. Again, if Microsoft is subject to a suit based on its description of its security for its Passport Wallet products, it is no wonder that small healthcare firms are leery about adopting EHR and then describing the system to their patients and customers.
3. It is inevitable that even the most high-tech firms are going to be victims of hacking incidents. In the recent IT security break-ins involving Sony PlayStation Network, the CEO Howard Stringer said in a May 17, 2011, Wall Street Journal article that "...maintaining the service's security is a 'never-ending process' and [he] doesn't know if anyone is '100%' secure."¹¹ If Sony is unable to guarantee security to its customers, then surely doubts creep in to small healthcare providers who do not have near the IT expertise that Sony possesses.¹²

NC State Associate Professor in Business Management, Fay Cobb Payton, et al., recently wrote an article entitled, "Health Care IT: Process, People, Patients and Interdisciplinary Considerations," in which it was stated that, "Despite this great promise, the impact of IT on healthcare over the past decade has so far been modest. Currently, almost 80 percent of the physicians—the majority in small, independent practices—lack even rudimentary digital records. Where electronic records do exist, they are typically limited in functionality and poor in interoperability."¹³ According to Professor Payton et al., "Compared to other industrialized nations, the United States lags far behind in the use of electronic health records and global economies can and have benefited from the implementation of information technology in

¹⁰ Microsoft Corp., No c-4069, 2002 WL 31881313 (Fed. Trade Comm'n Dec. 20, 2002).

¹¹ Daisuke Wakabayashi, "Sony's Chief Warns on Security Risks," *Wall Street Journal*, May 17, 2011.

¹² Id., also see my interview with the Technician: <http://www.technicianonline.com/news/professor-sony-playing-with-fire-1.2554264>.

¹³ Fay Cobb Payton, Guy Pare', Cynthia LeRouge, and Madhu Reddy, "Health Care IT: Process, People, Patients and Interdisciplinary Considerations," 12(2) *Journal of Association for Information Systems I* (February 2011).

the health care domain.”¹⁴ Also noted in the Payton et al., article [as well our Boston University article] EHR is patient privacy concerns, which hinder use of EHR for public health and research initiatives.¹⁵

It is my opinion that the adoption of EHR by small healthcare firms has been comparably slow and the true promise of EHRs has not been realized. However, I am limited to commenting about changes in the legal system that could reduce the barriers to more widespread adoption of EHR by small healthcare organizations. As stated above, the barriers to more prevalent use of EHR are combination of economic, technical, cultural, and legal factors.

My legal recommendations are, to the extent feasible, that:

- Small health care organizations should be provided with **safe harbors** in which they can acquire, store, and transmit medical records electronically without fear of lawsuits by either government agencies or class action suits by private citizens.
- Small healthcare organizations should not have to be IT specialists, aware of every nuance the constant battle between corporate IT security specialists and the malware hacking community. Small healthcare organizations should not be charged with knowledge of recent actions by the FTC to protect PII of patients and customers.
- Currently HIPAA does not contain a private right of action, nor should it.
- Identifying reasonable security measures to protect patient medical records stored electronically is an imposing task that time does not permit me to elucidate. A step in the right direction is **software criteria** developed by the Dept. of Health and Human Services so that software used by firms that store medical PII in electronically can be certified.¹⁶ To date, ARRA certification would require periodic tests, whose frequency has not been determined. The bottom line is that small health care firms that used American Recovery and Reinvestment Act (ARRA) certified software ought to be insulated from suits by HHS, the FTC, and class action patient suits. I recommend creation of a **due diligence defense** that is linked to use of ARRA certified software and the FTC should not intervene and contend that the software used by a healthcare provider, though ARRA certified, is nevertheless inadequate.¹⁷

I am convinced that the main barriers to the adoption of EHR by small healthcare firms are due to legal and economic uncertainty. The basic principles of economics and network externalities suggest that pursuant to the Patient Protection and Affordable Care Act, government subsidies to small healthcare firms to promote adoption of EHR are economically justified, though the appropriate magnitude of the subsidies is difficult to estimate.¹⁸ A key technical issue is easy interoperability (access and sharing of

¹⁴ Id., i.

¹⁵ Id., i. and [2].

¹⁶ American Recovery and Reinvestment Act,

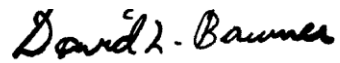
¹⁷ See work of Professor Annie Anton of the NCSU Computer Science Department and her Ph.D. students (Aaron Massey and Jeremy Maxwell) linking HIPAA and HITECH Privacy and Security rules with software code that is used by requirements engineers to comply with medical privacy and security laws.

¹⁸ A discussion of network externalities takes place at: <http://www.utdallas.edu/~liebowit/palgrave/network.html>. Work by Professors Stan Liebowitz and Steve Margolis (at NCSU) suggest that when networks are created users

medical data) that is not plagued by unsynchronized, medical codes. Finally, legal uncertainty can scare away small healthcare providers whose main interests are healthcare not IT, but the potential benefits of ubiquitous adoption of EHR are enormous.

Once again, it has been a pleasure to address this important committee before the House of Representatives.

Sincerely,

A handwritten signature in black ink that reads "David L. Baumer". The signature is written in a cursive, slightly slanted style.

David L. Baumer

derive two values from participation, (1) individual value, which is the value if there are no other users, and (2) synchronization value, the value of being able to interact with other users of the product.