2003

Electronic Signatures in E-Healthcare: The Need for a Federal Standard

Ashoke S. Talukdar

ELECTRONIC SIGNATURES IN E-HEALTHCARE: THE NEED FOR A FEDERAL STANDARD

I. PREFACE: A UTOPIAN SCENARIO FOR PORTABLE HEALTHCARE

I was on my dream vacation in remote beautiful rural Alaska. As luck would have it, I had barely had time settle into my hotel room in Anchorage for the afternoon when the chills and high fever started. It rang bells from a distant semester in college and a rather nasty bout of pneumonia. My primary care physician ("PCP"), like me, had decided to take some of her precious time off and go off hiking to Lake Moshannon State Park in rural Pennsylvania; hopes of reaching her were bleak.

It was 4:00 in the afternoon. With my chills under the dubious control of over-the-counter Naproxen, I bravely walked into to a local library with free Internet access for patrons. With practiced ease, I signed on to a terminal and typed in the universal resource locator ("URL") for the patient portal of my hospital in Cleveland,

Ohio – The MetroHealth System ("MHS").[1] This portal would allow me to view the relevant parts of my medical record, contact the physician who was handling my PCP's cases in her absence, request an acute care referral to the University of Alaska Medical Center ("UAMC") in Anchorage, with pre-authorization from my insurance company.[2] I signed on to the portal with my name and was immediately prompted to place my thumb on an optical fingerprint scanner attached to the terminal. An image of my thumbprint showed up on the screen - the system had legally validated that it was indeed me. The site then transmitted a Secure Sockets Layer/User Authentication ("SSL/UA") digital certificate to my terminal, which would be my passport to use the system for the rest of the session until I signed out.[3] Finding the supporting physician was easy enough – she was my allergist. I could tell that she was also online. I wrote a brief message giving her the specifics of my symptoms along with my federally mandated electronic signature on the request, which she acknowledged.[4] I returned to my hotel.

While I waited, the machinery of a thoroughly modern, national electronic healthcare information infrastructure was set in motion. The physician had been connected to MetroHealth from her home in Mentor, Ohio, via MetroHealth's secure remote access services. With an optical fingerprint attachment on her laptop, she provided her electronic authentication; she then electronically signed a referral to the Acute Care division at UAMC with a request for an appointment on my behalf. The system of course was smarter. Before dispatching the referral, it retrieved my list of insurance carriers. First, it performed a live eligibility verification query with Medical Mutual of Ohio ("MMO"), my health insurance carrier, to ensure that my coverage extended to out-of-state acute care services. To do this, the system used an ANSI X12 v4010 ("X12") 270 Eligibility Inquiry transaction mandated by the Health Insurance Portability and Accountability Act ("HIPAA").[5] After verification, MMO's records system responded with a return X12 271 Eligibility Response transaction. The MHS system then submitted the entire referral to MMO for pre-authorization using the X12 278 Health Services Review transaction also mandated by HIPAA.[6] The insurance counselor who opened the referral request at her terminal in Columbus, Ohio, used a two-factor authentication system to electronically sign her

---

[1]Copyright © 2004 The MetroHealth System, 2500 MetroHealth Drive, Cleveland, Ohio 44109-1998.

[2]For an example of a typical patient portal solution, *see* Shared Medical Record for Patients, at ¶2 (Copyright © 2004 Epic Systems Corporation), *at* http://www.epicsystems.com/software/mychart.htm, [*hereinafter Patient Portal*] (describing similar features available in Epic's MyChart© patient portal software).

[3]*See infra* section V.D.

[4]*See* Patient Portal, *supra* note 2. See also *infra* section VII.A.

[5]For HIPAA *see* Pub.L. No. 104-191, 110 Stat.1936 (1996). For the specific regulations regarding standard transactions and code sets, *see* 45 C.F.R. §§ 160, 162 (2002). ANSI is the American National Standards Institute located at http://www.ansi.org. Technical implementation documentation on all ANSI X12 transactions under HIPAA are available through the Washington Publishing Company, *at* http://www.wpc-edi.com/.

[6]*Id*.

approval of the referral.[7] MMO then transmitted a completed and approved X12 278 transaction including the pre-authorization data, and all the electronic signatures to UAMC, and an acknowledging copy to MHS. All transactions occurred through encrypted connection tunnels over the public internet, secured in accordance with the Security provisions of HIPAA ("HIPAA Security Rule").[8] Ten minutes later a care management specialist at UAMC was reviewing the request and setting up an appointment for my visit.

Approximately an hour after I returned to my hotel room from the library, the phone rang - the concierge informed me that that a UAMC Acute Care transport would be arriving to pick me up at 6:30 PM. By 7:15 PM, I was at UAMC being interviewed by a Patient Services Representative ("PSR"). On the screen in front of her she had an open electronic consent form which she asked me to read. She also handed me a copy of the UAMC Notice of Privacy Practices ("NPP").[9] I was instructed to click a checkbox next to each item on the form if I agreed with the provision. At the end of the last screen of the three-screen form I verified my personal information, and placed my signature using a digital signature capture device. The picture of my signature appeared on the screen, but the system had also collected and stored handwriting metrics unique to me, thereby authenticating me as the true signatory.[10] I had thus signed my acknowledgment of the NPP, my consent to being treated, and my general consent to the release of relevant care information to MMO for billing and claims purposes. The electronically signed claims and care details would be later transmitted by UAMC to MMO using the X12 837 Healthcare Claim and X12 275 Additional Information Request and Response with Attachments transactions mandate by HIPAA.[11]

Because I had a suspected infectious condition, the attending physician wanted me to stay under observation overnight. With two clicks of his mouse, a Notice of Admission was sent to MMO using another X12 278 transaction which was acknowledged using an X12 997 transaction.[12] Twenty five minutes later I was in an observation bed, the first dose of antibiotic administered, turning the pages of Patricia Cornwell's *Blow Fly*.[13] Outside it had started to snow.

II. INTRODUCTION

Healthcare, like many industries, is fast embracing the benefits of modern information technology ("IT").[14] The wide range of available publications on the use

---

[7]*See, e.g.,* OHIO REV. CODE ANN. § 3701.75(B)(2) (Anderson 2002).

[8]45 C.F.R. § 162.312 (2002).

[9]§ 164.520.

[10]*See infra* , note 236, section IX.A.

[11]45 C.F.R. § 162.1101 *et. seq.*

[12]*Id*.

[13]PATRICIA CORNWELL, BLOW FLY (Putnam Pub. Group) (2003).

[14]A Gartner report indicates that "the U.S. healthcare IT market is forecast to grow at a compound annual growth rate of 7.0 percent from $34.1 billion in 2001 to $47.9 billion in

of IT in healthcare indicates that IT provides the promise of faster and more comprehensive information about all aspects of the healthcare delivery process, to all classes of its consumers – patients, doctors, nurses, insurance adjudicators, health inspectors, epidemiologists, and biostatisticians.[15] But the drive towards electronic information in healthcare is not rooted merely in efficiency; more recently, significant emphasis has been placed on patient safety issues raised by the Institute of Medicine's ("IOM") year 2001 quality report on the subject.[16] It is believed that the deficiencies indicated in that report can be substantially overcome by the use of IT in healthcare.[17] However, to make this transition successful and complete, all aspects of healthcare delivery, information management, and business transactions, have to be logically migrated into the electronic world. This includes the function and use of the signature.[18]

The use of signatures in business contexts has traditionally provided two functions of legal significance: 1) evidence that can attribute documents to a particular party, and 2) indication of assent and intent that the documents have legal effect.[19] In the recent decades, state and federal statutes have substantiated these functional attributes to digital or electronic signatures.[20] Many of these statutes derive from model codes, such as the Uniform Electronic Transactions Act ("UETA"), that attempt to standardize use and technology surrounding electronic

---

2006." Geraldine Cruz, *In Unforgiving Times, the U.S. Healthcare Market Boosts IT Spending, 2001-2006*, HEALTHCARE DATA & STATISTICS, Gartner, Inc. (2003).

[15]For instance, a search on the phrase 'information technology' at BioMed Central yields publications that pertain to most of these areas. BioMed Central is an open access publisher located *at* http://www.biomedcentral.com. *See also* the focus areas and reports at Gartner's Healthcare website located *at* http://www4.gartner.com/research/focus_areas/asset_48261.jsp.

[16]Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century*, National Academy Press (2001). The study stated that "[i]ndeed, between the health care that we now have, and the health care we could have, lies not just a gap, but a chasm."

[17]David W. Bates, *The Quality Case for Information Technology in Healthcare*, BMC MED. INFORMATICS AND DECISION MAKING, 2:7, BioMed Central, Inc. (2002), *available at* http://www.biomedcentral.com/1472-6947/2/7. In the Discussion section the author notes that although many healthcare provider organizations use IT, they are yet to realize the efficiencies of similar use in other industries such as airline and parcel services. Furthermore, healthcare has invested at least "50% less of its gross revenues in information technology than other information-intensive industries like banking."

[18]James A Menke *et al*, *Computerized Clinical Documentation System in the Pediatric Intensive Care Unit*, BMC MED. INFORMATICS AND DECISION MAKING, 1:3, BioMed Central, Inc. (2001), *available at* http://www.biomedcentral.com/1472-6947/1/3.

[19]Peter Brown, *The Validity Of Click-Wrap Agreements*, 765 PRAC. L. INST./PAT. 111, 135 (2003).

[20]*See, e.g.,* Electronic Signature Systems, OHIO REV. CODE. ANN. § 3701.75 (West 2004). *See also* Electronic Signatures In Global And National Commerce, 15 U.S.C. §§ 7001(1), 7001(2) (West 2004), [*hereinafter Federal E-Sign Law*]. These laws are discussed in greater detail in *infra* Section V. For the rest of the discussion, *digital signature* and *electronic signature* are assumed to have the same meaning and used interchangeably.

signatures.[21] Subsequent sections will attempt to identify gaps in the standards which prevent true transaction portability. Lack of portability defeats one of the fundamental goals of healthcare IT solutions – improved efficiency. The discussion will end with a proposal for a uniform federal statutory scheme for standardized electronic signatures for healthcare.

A. The Functions of Signature in the Healthcare Context

As in all business practices, in healthcare too, a physical signature provides evidence of the signatory's identity, intent, and consent.[22] At common law, signatures are used in consents and authorizations,[23] orders and acknowledgments,[24] and receipts and validations.[25] The existence of this body of law strongly indicates that at least in healthcare, written signatures have significant importance in the care delivery process. Hence, as the healthcare industry moves to the electronic information age, some thought is necessary to create reliable equivalent processes that maintain the functionality of the individual signature.[26]

B. Signature Functions at Common Law: Some Modern Case Examples

In *Biddle v. Warren General Hosp.*, the Supreme Court of Ohio was faced with the issue of patient consents with regards to disclosure of non-public health information to third parties.[27] The court held that "in Ohio, an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship."[28] Similarly, in *Berger v. Sonneland* the Washington Supreme Court reaffirmed its recognition of an independent cause of action for the breach of

---

[21]*See* Uniform Electronic Transactions Act, Drafted by the National Conference Of Commissioners On Uniform State Laws (1999), *at* http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm. It is of some interest that UETA and *Federal E-Sign Law* are substantially similar, although the latter has evolved around modern concepts of electronic identity management. The associated technology and the inconsistencies of standards are further discussed in *infra* Section V.

[22]*See* Christopher Reed, *Legally Binding Electronic Documents: Digital Signatures And Authentication*, 35 INT'L LAW. 89, 93 (2001).

[23]*See*, *e.g.*, Moore v. Regents of Univ. of California, 793 P.2d 479 (Cal. 1991) (informed consent required prior to taking tissue samples from patient); Biddle v. Warren Gen. Hosp., 715 N.E.2d 518 (Ohio 1999) (disclosure to a third party without consent is a recognized tort).

[24]*See* Ruefle v. Civil Serv. Comm'n, 2003 WL 22442063 at *1 (Pa. Sep. 04, 2003) (physician FMLA certification form requires physician's signature).

[25]*See* Sharp v. Lewis Ford, Inc., 78 S.W.3d 746 (Ark. Ct. App. 2002) (form acknowledging change of physicians in a Workers' Compensation claim requires signature).

[26]*See generally* BRUCE SCHNEIER, SECRETS & LIES, 96-99 (Wiley Computer Publishing) (2000).

[27]*See Biddle*, 715 N.E.2d at 518.

[28]*Id.* at 523

the physician patient confidentiality under Washington law.[29] Of course, underlying both *Biddle* and *Berger*, is the traditional concept of patient consent documented with a written signature on paper.[30] The typical signed document is usually kept with the patient's paper medical record in a hospital's medical records department.[31]

The common law requirement of the written device has usually resulted in state policy. Hence, in *Garrett v. Young*, a California Court of Appeals refused to find a cause of action against the healthcare provider for disclosure of health information to her employer because the patient had not provided a *written request* prohibiting such disclosure in accordance with California statutes.[32] *Garrett* is a modern illustration of the continued reliance on the requirement of a signed document in healthcare delivery agreements.[33]

C. Statutory Basis For Signatures In Modern Healthcare

The law's tradition of written and signed agreements between patients and healthcare providers is not the only source for its statutory renditions. Various business aspects of healthcare reflect the traditional use of signatures as evidenced in a variety of statutes.[34] Indeed, the decisions cited here are also illustrative of state statutes in appropriate jurisdictions.[35] However, these cases and statutes demonstrate

---

[29]Berger v. Sonneland, 26 P.3d 257, 267 (Wash. 2001). Specifically, the court found that petitioner Sonneland's conduct constituted "health care" under Washington statute because he had disclosed the confidential information "in his effort to discover more information about Respondent's use of pain medications so he could treat, diagnose, or care for [the patient]."

[30]*See Biddle*, 715 N.E.2d at 518; *Berger*, 26 P.3d at 265.

[31]*See*, *e.g.,* CENTRAL STATE HOSPITAL GEORGIA DEPARTMENT OF HUMAN RESOURCES, *Functions of the Health Information Management Department*, *at* http://centralstatehospital.org/Himd2.htm.

[32]Garrett v. Young, 1 Cal. Rptr. 3d 134, 142 (Cal. Ct. App. 2003). The court denied the cause of action in spite of the evidence that the patient had *orally* requested nondisclosure. The court specifically stated its obligation "to interpret the statute in accordance with its plain language and the intent of the Legislature." It went on to hold that because the notice had been oral it did not comply with the statutory prerequisite of a written notice to nondisclosure.

[33]*Id*.

[34]*See*, *e.g.,* Parental Consent To Performing Abortion Upon Minor, ALA. CODE § 26-21-3 (2004); Injection card system; protocols, CAL. BUS. & PROF. CODE § 4065 (West 2002); Notice of lack of malpractice insurance, OHIO REV. CODE ANN. § 4731.143 (West 2004).

[35]In *Berger*, 26 P.3d at 265-66, the Washington Supreme Court substantially relied on WASH. REV. CODE ANN. § 7.70.030(3) (West 2004), which requires the plaintiff to establish that "injury resulted from *health care* to which the patient or his representative did not consent." (emphasis added). In contrast, *see Garrett,* 1 Cal. Rptr. 3d at 142, relies on CAL. CIV. CODE § 56.16 (West 2004) whereby a "specific written request by the patient" is required to prohibit disclosures to unintended parties. In *Biddle*, 715 N.E.2d at 525, the Ohio Supreme Court faced the problem of Legislative silence in distinguishing between the patient-provider and attorney-client relationships. The court placed emphasis on the latter and refused to accept defendant's attempt to use OHIO REV. CODE ANN. § 2317.021 (West 2004) to establish

a lack of consistency in the structure, approach, and resolution of signature related issues in a ubiquitous transactional element of the healthcare delivery process – patient consent.

More recently, federal health privacy and security regulations promulgated by the Department of Health and Human Services ("HHS") under HIPAA represent a national attempt to establish baseline standards for these types of agreements between patients and providers.[36] The requirements for written signatures indicating agreement persist even under these rules.[37] The combination of written signature requirements with statutes that give legal effect to electronic signatures, is at the foundation of modern electronic transactions.[38] In *Medical Self Care, Inc. ex rel. Development Specialists, Inc. v. National Broadcasting Co., Inc.* the Federal District Court for the Southern District of New York faced the issue of whether an e-mail should be "considered a writing for the purposes of enforcing a 'written consent' clause of a contract."[39] The court, interpreting federal regulations under the Electronic Signatures In Global And National Commerce ("Federal E-Sign Law") law, held that it should be.[40] It is thus relevant to consider the implications of electronic transactions in healthcare functions that otherwise require written signatures.

III. HEALTHCARE IN THE ELECTRONIC INFORMATION AGE

In 1991, the Health Information Management Systems Society's (HIMSS) Committee on Improving the Patient Record, convened by the Institute of Medicine, set a goal to make the computerized patient record a standard technology in healthcare by 2001.[41] In a recent article, Joyce Sensmeier, Director of Professional Services for HIMSS, wrote of a "growing consensus that clinical information systems will provide the bridge to advancing the integration of information systems in healthcare."[42] Sensmeier concluded that "enabling access to relevant patient information from multiple settings and encounters at the point of care will have a significant positive impact on the quality, consistency, and timeliness of data and

---

that the hospital's attorney firm was not a third party; the patients' indicated *written* consents therefore did not extend to disclosure to the attorney firm.

[36]*See* 45 C.F.R. § 164.512.

[37]*Id*.

[38]*See*, *e.g.*, Uniform Electronic Transactions Act, OHIO REV. CODE ANN. § 1306.06 (West 2004).

[39]Medical Self Care, Inc. ex rel. Dev. Specialists, Inc. v. NBC Co., Inc., 2003 WL 1622181 at *6, (S.D.N.Y., Mar 28, 2003).

[40]*Id.* (citing *Federal E-Sign Law*, §§ 7001(1), 7001(2)).

[41]Institute of Medicine, *The Computer-based Patient Record: An Essential Technology for Healthcare*, R. S. Dick and E. B. Steen, eds. National Academy Press (1991).

[42]Joyce Sensemeier, *Advancing the State of Data Integration in Healthcare*, 17 J. HEALTHCARE INFO. MGMT. 4, 58 (2003), *available at* http://www.himss.org/content/files/jhim/17-4/sensmeier.pdf.

information."[43] This general trend of increasing reliance on electronic information in healthcare is reflected in cases that have begun to emerge in the lower courts involving direct healthcare delivery.[44] Similar issues have also emerged in allied healthcare related businesses.[45]

A. Migrating Healthcare Information Management From Paper to Electronic Records

The first suggestions of benefits of the use of electronic records in healthcare trace back to the work of Tang.[46] Recent efforts to foster migration of the paper health record to electronic form have focused on "how the physicians work, and develop the software with an eye toward solving real problems."[47] In the opinion of some physicians, electronic documentation requirements for healthcare records in the United States are more complex and "a coordinated national effort to identify the required components of an [electronic medical record system]"[48] is necessary.

In 1997, in a statement before the United States National Committee on Vital and Health Statistics ("NCVHS"), the Chair of the Association For Electronic Health Care Transactions ("AFEHCT") emphasized the need for national standardization for healthcare transactions.[49] The statement was made in support of the proposed HIPAA Administrative Simplification legislation.[50] It characterized the legislation

---

[43] *Id.* at 61.

[44] *See, e.g.*, Schmidt v. U.S. Dep't of Veterans Affairs, 218 F.R.D. 619 (E.D. Wis. 2003) (putative class action against the Veterans Administration by employees alleging that the VA violated the employees' rights under the Privacy Act by disclosing their Social Security numbers (SSNs) on VA computer system to employees who had no need for the SSNs); Detroit Medical Center v. Provider Healthnet Services, Inc., 269 F. Supp. 2d 487, (D. Del. 2003) (breach of contract action against health information management company seeking rescission of asset agreement and service agreement).

[45] *See* Martello v. Blue Cross and Blue Shield of Maryland, Inc., 795 A.2d 185 (Md. 2002) (sole proprietor of medical claims clearinghouse that furnished electronic connectivity services brought anti-trust action against larger electronic connectivity provider and insurer that sold provider its electronic connectivity business).

[46] P.C. Tang et al., *Traditional Medical Records As A Source Of Clinical Data In The Outpatient Setting*, PROC. ANN. SYMP. COMPUTER APPLICATIONS IN MED. CARE 575 (1994).

[47] Jacob Reider, *The Electronic Medical Record: Promises and Pitfalls*, MEDSCAPE GEN. MED. 5(3), *at* http://www.medscape.com/viewarticle/460247.

[48] *Id*.

[49] Benjamin Curtis, *Statement Before The National Committee on Vital and Health Statistics (NCVHS)*, Subcommittee on Health Data Needs, Standards, and Security (1997), *available at* http://www.ncvhs.hhs.gov/970210t5.htm. Pursuant to 42 U.S.C. § 242k(k), the NCVHS serves as the statutory public advisory body to the Secretary of Health and Human Services in the area of health data and statistics. NCVHS is located *at* http://www.ncvhs.gov.

[50] Subtitle F of Title II of HIPAA consists of sections 261 through 264. § 262 amends Title XI of the Social Security Act, 42 U.S.C. § 1301 *et. seq*., to add a Part C, entitled "Administrative Simplification," with sections 1171-1179, codified at 42 U.S.C.A. § 1320d through § 1320(d)-8 (West Supp. 2002). Section 261 is a note to 42 U.S.C.A. § 1320(d) and

as "an opportunity for the development and use of a uniform implementation process of the standards intended for transmitting and receiving electronic data [and] the increased availability [and] use of electronic health care transactions."[51] Realization of these opportunities depends on a standardized electronic signature.[52]

B. Making the Signature an Electronic Process

To realize the opportunity of standardization for electronic signatures, it is useful to revisit the example on consent.[53] Peter Brensilver writes that there are significant potential benefits of using interactive electronic methodologies in the expression of consent.[54] Regulatory frameworks have been proposed for electronic informed consents.[55] However, these proposals mention, but do not successfully address, the complexity of the one device that embodies such consent – the electronic signature.[56] Brensilver states that although the "[Federal E-sign Law] further exemplifies the acceptance of technology in setting legal standards,"[57] to stay within the scope of congress's constitutional authority, the law applies to interstate or foreign transactions only. Efforts to legislate standards for electronic signatures at the state level have followed the general guidelines for the Federal E-Sign Law.[58] However, the approaches have varied significantly enough to make the electronic equivalent of the written device less than fully portable.[59] As seen in subsequent sections, owing to the complexity of methods of electronic identity validation of the signatory, even subtle variations in implementation methodologies, while legally indistinguishable in their respective jurisdictions, nevertheless, can render the signature non-portable across state borders or even systems within a state.

Section 264 is a note to 42 U.S.C.A. § 1320(d)-(2). Also, Section 263 amends the Public Health Service Act, at 42 U.S.C.A. § 242k(k) (West Supp.2002).

[51]Curtis, *supra* note 49.

[52]*See generally* Christian James Helbling, *Electronic Records and Signatures in Healthcare and the Interplay of E-Sign, HIPAA and UETA*, Buchanan Ingersoll (2001), *at* http://library.lp.findlaw.com/articles/file/00323/000777/title/subject/topic/consumer%20law_consumer%20protection/filename/consumerlaw_1_392.

[53]*See supra* Section II.

[54]*See* Peter Brensilver, Note, *E-Formed Consent: Evaluating the Interplay of Interactive Technology and Informed Consent*, 70 GEO WASH. L. REV. 613, 623 (2002).

[55]*Id.* at 630.

[56]*Id.* at 622.

[57]*Id.* at 623.

[58]15 U.S.C. §§ 7001(1), 7001(2).

[59]*See* Brensilver, *supra* note 54, at 630 (citing, as example, two state statutes regarding electronic signatures). But, whereas, LA. REV. STAT. ANN. § 40:2145(B) (West 2000) tasks the Louisiana Department of Health and Hospitals to develop guidelines for permissibility and security requirements such as "the use of codes, fingerprints, or other identifying methods," the functionally similar OHIO REV. CODE. ANN. § 3701.75(B)(2) stipulates that the signatory of the signature must be verified by a "biometric" or "two-level" authentication scheme.

IV. THE REQUIREMENTS OF THE UNIFORM ELECTRONIC SIGNATURE

The goal of this discussion is to propose a uniform electronic signature standard through federal law. We often take for granted this portability as it pertains to a written signature. Seldom do we question whether a signature made on an instrument of financial transaction executed in Ohio will remain a valid instrument after it is mailed to the state of Louisiana. For electronic signatures, the core of this challenge is the portability of the signature. Portability of a signature is indeed a three-fold feature. First, from a forensic standpoint, a written signature is a biometric element that uniquely identifies its signatory through handwriting.[60] Second, and as a result, its authenticity and its integrity are independently verifiable by handwriting experts for the purpose of legal review.[61] The two features – *authentication* of the signatory and *integrity* of the instrument – together guarantee that the transaction validated by a signature will be non-repudiable in a legal dispute.[62] They also establish the intent and consent of the signatory with respect to the transaction.

A. Recent Historical Perspective On The Problem: The Schnorr Patent

The use of an electronic medium to replace a written signature poses the immediate problem of maintaining the integrity of the written device because no longer is the signatory's biometric information inherent in the device. Dr. Claus P. Schnorr, a resident of Frankfurt, Germany, owns the patent for a "Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System."[63] The patent applies to a method for mutual identification of subscribers who are participating in an encrypted data exchange system.[64] The Schnorr patent demonstrates one problem with the transition of the signature to an electronic medium. Whereas the biometric element of the written signature is a human physical characteristic, its technological equivalent here is represented in patented intellectual property that is not freely accessible to others![65]

The proprietary aspect of Schnorr's scheme was the subject of dispute in *Cylink Corp. v. Schnorr* which upheld Schnorr's rights to the patented algorithm.[66] Dr. Schnorr licensed his patent to Public Key Partnership ("PKP"), a partnership formed by Caro-Kann, a wholly-owned subsidiary of Cylink, and RSA Data Security, Inc. ("RSA").[67] Although PKP was eventually dissolved and its license agreement with

---

[60]Alan E. Brill, *The Technologies Of Privacy And Privacy Invasion: An Introduction*, 748 PRAC. L. INST./PAT. 85, 109 (2003).

[61]*See* United States v. Crisp, 324 F.3d 261, 271 (4th Cir. 2003) (finding that "handwriting comparison testimony has a long history of admissibility in the courts of this country").

[62]*See also* Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579 (1993); Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).

[63]U.S. Patent No. 4,995,082 (issued Feb. 19, 1991).

[64]*Id*.

[65]*See* Brill, *supra* note 60.

[66]Cylink Corp. v. Schnorr, 939 F. Supp. 39, 42 (D.D.C. 1996).

[67]*Id.*at 40.

Dr. Schnorr terminated, during the months prior to the dissolution, Cylink and RSA competed for an exclusive licensing agreement with Dr. Schnorr, in which RSA prevailed and was appointed as the exclusive representative to license and enforce the Schnorr patent.[68] Following an RSA press-release Cylink's in-house counsel proposed that Cylink would represent Dr. Schnorr's patent better than RSA but was informed that the agreement with RSA was exclusive and that RSA would enforce the patent.[69] It was suggested that Cylink apply to RSA to obtain a license for the Schnorr patent.[70] Instead, Cylink filed a petition for a judgment declaring that its use of a particular digital signature algorithm did not infringe the patent.[71] Eventually Schnorr's motion to dismiss the petition was granted thereby upholding his patent rights.[72]

The impact of the *Cylink* decision has rippled through the IT community. It has even thwarted the federal government's efforts at creating electronic signatory authentication standards under the Federal Information Processing Standard ("FIPS").[73] The FIPS 186 Digital Signature Standard ("DSS"), was issued in May 1994, under which the Digital Signature Algorithm ("DSA") proposed a standard for authentication, including integrity.[74] However, prior to the adoption of the standard, the U.S. government filed a patent application on DSA in an attempt to exercise exclusive control on the standard and its evolution, avoid variants in the industry, and subsequently license the patent to future implementers of DSA, thereby strengthening the standard itself.[75] The move was successfully opposed by Schnorr who claimed that DSA could not be practiced without infringing his digital signature patent.[76] While the Federal government has continued to make efforts at creating a standard, there has not been any significant legislative backing for implementation of such standards, and even less so in electronic healthcare.[77]

---

[68] *Id*.

[69] *Id.* of 41

[70] *Id*.

[71] *Id.* Cylink was subsequently invited by RSA to either enter negotiations for a license to the Schnorr Patent or cease marketing and selling products that incorporated Schnorr's algorithm.

[72] *Id.* at 42.

[73] *See* Edward J. Radlo, *Legal Issues In Cryptography*, 13 NO. 5 COMPUTER LAW. 1, (1996). In reviewing the evolution of cryptography in digital signatures, the author outlines efforts under FIPS that were challenged by Schnorr. FIPS publications can be found *at* http://www.itl.nist.gov/fipspubs/.

[74] *Id.* at 11

[75] *Id*.

[76] *Id*.

[77] *Id. See also* HIPAA Security Rule, 45 C.F.R. § 164.304, which uses a very non-specific definition of authentication as "the corroboration that a person is the one claimed."

B. Avoiding Risks Associated With Electronic Data: Encryption and Access Control

Aside from portability there remains a continuing need for a standard similar to the FIPS proposals, because the lack of standards introduces significant security risks in electronic data exchange.[78] In practice, this means that signature and transaction data needs protection from improper visibility and unauthorized access. The vulnerability of unprotected data is highlighted in *Cobell v. Norton*.[79] In the April 2001 issue of *The Government Executive* magazine, Dominic Nessi, the Chief Information Officer of the Bureau of Indian Affairs ("BIA") observed that BIA had "no security . . . [and] no infrastructure…[and the] entire network . . . [could] be breached by a high school kid."[80] The plaintiffs had already sought a temporary restraining order ("TRO") aimed at preventing destruction of Indian trust funds and records, which had been granted.[81]

Following Nessi's declaration, Cobell and others brought a second suit against the Secretary of the Department of Interior ("DOI"), seeking among other things, an emergency temporary restraining order to prevent further destruction of data in BIA's systems in violation of the first TRO.[82] A court assigned Special Master began an investigation of the DOI's IT systems and produced a report.[83] The report highlighted that the DOI had breached its duty to ensure the integrity of the data in its care, and had failed to comply with several federal regulations.[84] Furthermore, its failure was evident in the "enormity of the dangers to which this trust information [was] being exposed."[85]

Cobell's issues are applicable to healthcare information and transactions. Elements of electronic signatures such as the signature code, signatory's identity, tokens, and so on, are all pieces of electronic information that are necessarily stored somewhere. If they are openly visible or otherwise retrievable without the signatory's permission or knowledge, then the very identity of the signatory as well

---

[78]*See* Radlo, *supra* note 73.

[79]Cobell v. Norton, 2001 WL 1555296, D.D.C. (Dec 6, 2001).

[80]*Id.* at *1 (citing Katherine McIntire Peters, *Trail of Troubles*, GOVERNMENT EXECUTIVE, April 1, 2001 at 100).

[81]*Id*.

[82]*Id*.

[83]*Id*.

[84]*Id.* at *6 (citing The Paperwork Reduction Act of 1978, 44 U.S.C. § 3501 (making uniform federal information resources management policies and practices as a means to improve the productivity, efficiency, and effectiveness of government programs); The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (criminalizing unauthorized access to electronic communications); The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030 (criminalizing unauthorized access to information stored on government computer systems); The Computer Security Act of 1987 40 U.S.C. § 1441 (requiring the government to promulgate standards for computer security, train relevant employees in computer security and establish plans for the security and privacy of computer information)).

[85]*Id.* at *6.

as the signature's integrity may be compromised. It is therefore necessary to both secure as well as validate electronic signatures and transaction contents. Technology has answered this challenge with cryptographic techniques of hiding information content, commonly referred to as encryption, which renders data unintelligible by altering it in an ordered fashion.[86] In the healthcare context, the federal government has attempted to respond to such technology by prescribing encryption requirements for healthcare under the HIPAA Security Rule.[87]

The preamble to the rules, in pertinent part, acknowledges the "financial and technical burdens associated with the employment of encryption tools" in the context of "small and rural providers."[88] This degree of hesitance and flexibility in the rule is reflective of the unsettled nature of the law in a rapidly evolving technical field. Arguably, although encryption is an addressable standard, the addressability may be narrowed based on a healthcare facility's size, location, accessibility to resources, and so on.[89] Additionally, the preamble encourages "[healthcare facilities] . . . to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet."[90] Understanding the interplay between electronic signatures as electronic data, and the integrity and security of the transactions they bind to, requires a scrutiny of the interaction of current signature technology, the law, and federal and state technology policy.

V. ELECTRONIC SIGNATURE TECHNOLOGY, CURRENT LAW, AND POLICY

A. Legal Requirements for Electronic Signatures

Any proposed generalized electronic signature scheme should address three principle aspects of the signature - its structure, its signatory, and the integrity of the transaction it binds to.[91] Laws and governmental publications in the past decade lend clues as to the specifications of each of these aspects and we start there.

The structure of the signature is typically found in the definitions of the electronic signature itself. For instance, the Federal E-Sign Law defines electronic signature as "an electronic sound, symbol, or process, attached to or logically

---

[86]Cryptography and encryption are discussed further in *supra* section V.B.

[87]*See, e.g.*, 45 C.F.R. § 164.312(e)(2)(ii) (requiring a covered entity to "[i]mplement a mechanism to encrypt electronic protected health information whenever deemed appropriate."); *See also* § 164.312(a)(2)(iv) (addressable implementation of "a mechanism to encrypt and decrypt electronic protected health information."). "[A]ddressable" and "required" specifications are explained at § 164.306(d)(1).

[88]*See* 68 Fed. Reg. 8334, 8357 (Feb. 20, 2003) (codified at 45 C.F.R. §§ 160, 162, and 164).

[89]*Id.* at 8336 (discussing "addressable" standards as those where a covered entity "will ultimately do one of the following: (a) Implement one or more of the addressable implementation specifications; (b) implement one or more alternative security measures; (c) implement a combination of both; or (d) not implement either an addressable implementation specification or an alternative security measure.")

[90]*Id.* at 8357.

[91]*See* 15 U.S.C. § 7001 (2000).

associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[92] The UETA adopts the identical definition.[93]

In contrast, the Ohio Electronic Signature Systems statute for healthcare defines the electronic signature as:

> [A]ny of the following attached to or associated with an electronic record by an individual to authenticate the record:
>
> (a) A code consisting of a combination of letters, numbers, characters, or symbols that is adopted or executed by an individual as that individual's electronic signature;
>
> (b) A computer-generated signature code created for an individual;
>
> (c) An electronic image of an individual's handwritten signature created by using a pen computer.[94]

Finally, the proposed electronic signature rule under HIPAA ("proposed HIPAA rule") takes a broad and generalized approach.[95] It specifies, in relevant part, that "[a]n electronic signature is the attribute affixed to an electronic document to bind it to a particular entity."[96]

Intuitively, integrity of a signature applies to both the content of a transaction as also to the signatory's consent and intent with respect to that content as she understands it to be at the time of the signing. Abstract expression of consent and intent is inherently difficult to capture in electronic form. Hence, in situations where the law would require a signature in writing, a consumer's understanding and consent must be assured when asked to use an electronic signature instead.[97] In this regard, the Federal E-Sign Law goes farthest by stipulating various assurances that need to be provided to the consumer prior to the expression of their assent to the transaction, when an electronic signature is used for a transaction that would otherwise require a written signature.[98] In contrast, the Ohio signature law requires only that there be "a process to verify that the individual affixing the electronic signature has reviewed the contents of the entry and determined that the entry

---

[92] § 7006(5).

[93] Uniform Electronic Transaction Act § 2(8).

[94] *See* OHIO REV. CODE. ANN. § 3701.75(A)(2) (West 2004).

[95] *See* Security and Electronic Signature Standards, 63 Fed. Reg. 43,241, 43269 (Oct. 12, 1998) (proposed rule to be codified at 45 C.F.R. § 142).

[96] *Id.*

[97] *See* Radlo, *supra* note 73, at 1.

[98] 15 U.S.C.A § 7001(C) specifies a gamut of protected consumer rights. Specifically, § 7001(C)(1) outlines those specific rights that must be guaranteed for an electronic signature to satisfy the requirement of a written signature including intent of the signatory as well has her understanding of the process and the implications of the electronic signature and transaction.

contains what that individual intended."[99] The proposed HIPAA rule requires that there be a "logical manifestation of signature" and that there exist "additional information such as time stamp and signature purpose specific to that user."[100]

While the structure of the signature may be statutorily defined and the intent of the signatory embedded in appropriate language contained in the transaction itself, defining and authenticating the signatory's electronic identity poses a significant technological challenge.[101] Approaches to authentication of the signatory's identity can vary. The proposed HIPAA rule integrates a general authentication requirement of the signatory's identity into the structure by adding to the definition that the signature must "[secure] the user authentication (proof of claimed identity) at the time the signature is generated."[102] The Ohio statute in contrast is highly specific with respect to the technology to be used for authenticating the signatory by requiring that an electronic signature system utilize "either a two-level access control mechanism that assigns a unique identifier to each user or a biometric access control device."[103] Other state statutes take varying approaches.[104]

It should be also noted that identity, authentication, and consent and intent are meaningful only to the extent that their integrity and security are maintained throughout the entire transaction. This might include electronic transmission of the content and the signature. In healthcare, existing privacy and security requirements pertaining to Protected Health Information ("PHI") therefore apply to all transactional content.[105] They would also apply for the entirety of the transmission of such content.[106] The unification of these concepts into the electronic signature structure is at the core of the electronic signature and we turn to it next.

B. Analyzing Portability: Identification, Authentication and Intent - Cryptography and Public Key Encryption

The proposed HIPAA signature rule emphasizes that the signature should "[ensure] the integrity of the signed document to enable transportability of data, interoperability, independent verifiability, and continuity of signature capability."[107] The simplicity of this statutory requirement belies the enormous complexity of the science necessary to address it – cryptography.[108]

---

[99]Ohio Rev. Code Ann. § 3701.75(B)(4).

[100]63 Fed. Reg. at 43,273.

[101]*See generally* SCHNEIER, *supra* note 26.

[102]*Id.*

[103]*See* § 3701.75(B)(2).

[104]*See* statutes listed in *infra* section VI.A and notes therein.

[105]*See* 45 C.F.R. §164.501

[106]*See* 63 Fed. Reg. at 43, 265-69.

[107]*Id.* at 43, 274.

[108]For an exhaustive review, *see* SCHNEIER, *supra* note 26.

Traditional cryptography is a three-step process. First, plaintext transactional content is encoded using: (a) a general mathematical scheme (also known as an *algorithm*), and (b) a signatory-specific key (also known as a *cipher*).[109] The unintelligible, encoded data content (also known as *cipher*text) can be deciphered only by the key-holder; as long as the cipher is sufficiently robust, and the signatory and recipients are the sole proprietors of the keys, the integrity of the transaction is assured.[110] Next, a message authentication code ("MAC"), mathematically derived from attributes of the original message content, is added to the encrypted transaction.[111] The MAC ensures that "the [transaction] came from the person it purports to have come from (authentication), and that the [content] was not altered in transit (integrity)."[112] The last step is to add the digital signature, which itself is a code that is computed from: (a) the encrypted message, and (b) unique information in a signatory's key. [113] The digital signature is then attached to the encrypted transaction to indicate both authorship as well as consent.[114]

To ensure proper functionality, modern digital cryptography uses the Public Key Encryption ("PKE") system.[115] The system uses an asymmetric scheme with a pair of keys per signatory – a public key and a private key.[116] The *public* key is the encryption key and is shared with recipients. It is used by a recipient to *validate* the signatory's digital signature and by a sender to *encrypt* a transaction intended for the key's owner.[117] In contrast, the *private* key is used by the signatory to generate her digital signature for a transaction to a recipient and by a recipient to *decrypt* transactions encrypted with her public key.[118] Public keys are therefore shared by parties to be trusted in a transaction and fraudulent duplication of keys is avoided because a private key cannot be used to generate a public key and vice versa.[119]

Functionally, assume *A* and *B* have exchanged public keys as trusted parties to a transaction. *A* uses *B*'s *public* key plus original transaction content to encrypt the transaction to be sent to *B*.[120] She then uses her *private* key plus elements of the encrypted data to generate her digital signature to be attached to the transaction. She then dispatches the transaction to *B*. *B* uses *A*'s public key to (a) verify the authenticity of *A*'s digital signature and, (b) to encrypt an acknowledgment of receipt

---

[109] *Id.* at 88-89.

[110] *Id*.

[111] *Id*.

[112] SCHNEIER, *supra* note 26, at 92-93.

[113] *Id*.

[114] *Id.* at 97.

[115] *Id.* at 95.

[116] *Id*.

[117] *Id*.

[118] *Id*.

[119] SCHNEIER, *supra* note 26, at 95.

[120] *Id*.

to be sent back to *A*. He then uses his private key to decrypt the transaction received from *A*. It is possible that *C,* who is not a trusted party to the transaction, could receive the transaction in error or by interception. But *C* has neither *A*'s nor *B*'s public or private keys and therefore can neither verify *A*'s signature nor decrypt the content. Also, he cannot duplicate *B*'s signature to create a notification of receipt in *B*'s name, which *A* is expecting.

There are several classes of algorithms that are available for both content encryption and digital signature generation.[121] The algorithms may be proprietary, public, or classified; they could also have different cipher strengths.[122] Furthermore, the complexity of the system poses inherent hurdles, such as determination of the true identity of the signatory and the distribution, compatibility, and reliability of keys.[123] Since the advent of PKE, technology has attempted to create an electronic trust infrastructure to facilitate commerce in electronic form. The most popular and comprehensive of such efforts is the Public Key Infrastructure.

C. Creating an Infrastructure for Electronic Trust: The Public Key Infrastructure

A Public Key Infrastructure ("PKI") is a system of key generation and management that relies on trusted third parties to verify identity of key-owners and signatories.[124] Third-party organizations issue "certificates" to signatories that "list a public key and confirm that the person identified in the certificate holds the corresponding private key."[125] These organizations are known as Certificate Authorities ("CA").[126] They also manage proper pairing of public and private keys, verify the date and time of signatures and transactions, and maintain lists of keys that become compromised, unreliable or otherwise invalid.[127]

Of course, even PKI cannot function for the purpose of standardized transactions in healthcare, or elsewhere, if the keys managed are not themselves standardized. The Internet Engineering Task Force ("IETF") has made the most notable attempt to create a standard for PKI keys.[128] The PKIX Working Group of the IETF was

---

[121] *Id.* at 89-93.

[122] *Id*.

[123] *Id.* at 96. *See also* Reed, *supra* note 22, at 95-97.

[124] *See* Rebecca Porter, *Do Electronic Signatures Mean An End To The Dotted Line?*, 39-SEP TRIAL 52, 56 (2003).

[125] *See* Sun Microsystems, Inc. X.509 Certificates and Certificate Revocation Lists (CRLs) (Sun Microsystems 2001), [*hereinafter X.509 Certificates*], *at* http://java.sun.com/ products/jdk/ 1.2/docs/guide/security/cert3.html (describing a Certificate as a "digitally signed statement from one entity, saying that the public key (and some other information) of another entity has some specific value").

[126] Porter, *supra* note 124.

[127] *Id*.

[128] *See Overview of the IETF*, *at* http://www.ietf.org/overview.html. The website describes IETF as "a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual." It goes on to state that the individual working groups do the technical work. These groups are organized by topic into areas such as

established in 1995 to develop Internet standards to extend the X.509 key-certificate standard to support PKI.[129] The group's proposals created an extensive set of standards for various aspects of X.509 certificate management, distribution, revocation and properties, some of which are based on existing technology.[130] Most significantly, the proposed standard provides the first realistic chance of a functional PKI where key compatibility is not an impediment. Additionally, it also allows special attributes certificates to store biometric templates as a part of the authentication key.[131] Finally, in addition to third party CAs, products from key identity management vendors allow any organization to act as its own CA.[132] Both PKI, as well as these products, represent major industry acceptance of the current version of the X.509 standard.[133]

There is however a gap that remains between the available technology and the acceptability of the standard. Since the X.509 proposal is largely a recommendation, there has been general reluctance to an industry wide adaptation. The lack of a clear legal mandate for a standardization of this important transactional element remains the main contention that continues to thwart portability of electronic signatures.

D. Authenticating the Signatory's Identity: Non-Repudiation

A signatory authentication system could be single factor system such as a password.[134] However, the traditional password-only systems are plagued with security problems that increase the risk of fraud: keystroke monitoring (a *Trojan* program that stealthily monitors keystrokes to collect passwords), social engineering (obtaining passwords using social situational tactics or spying), man-in-the-middle attacks (computers pretending to be the service that a client signatory is trying to reach, accepting the client's password and other identity information, and then using the supplied identity to authenticate on to the real service), network monitoring (sniffing for passwords being transmitted on an entire data network), password

---

routing, transport, and security. An Internet Architecture Board ("IAB") provides architectural oversight and adjudicates appeals on complaints.

[129]*See* IETF, *Public-Key Infrastructure (X.509) (pkix)* (2003), [*hereinafter IETF PKIX*], *at* http://www.ietf.org/html.charters/pkix-charter.html; *see also X.509 Certificates*, *supra* note 125 (*What's Inside an X.509 Certificate?*).

[130]*See* IETF PKIX, *supra* note 129.

[131]*See* Proposed Methods to use X.509 Attribute Certificates to store biometric templates, *hereinafter X.509 Attribute Certificates*, THE BIOMETRIC CONSORTIUM, *at* http://www.biometrics.org/html/x.509.html.

[132]*See e.g.* RSA Keon® Certificate Authority, RSA SECURITY, INC. (2003), *at* http://www.rsasecurity.com/products/keon/certificateauth.html.

[133]*See* RSA Keon® Certificate Authority: Technical Specifications, *Certificate Standards*, RSA SECURITY, INC. (2003), *available at* http://www.rsasecurity.com/node.asp?id=1226.

[134]In any authentication system, the "factor" refers to that quality of the identification process that is unique to the user. In its simplest form, a unique factor would be something that, presumably, only the signatory knows – a secret code or password.

cracking (the "brute force" approach), key-under-the-mat problems (passwords written on Post-It™ notes), and so on.[135]

There are modern, and stronger, single factor systems that use biometric techniques. Biometric authentication automatically recognizes persons based on some physiological or behavioral characteristics that are universal, distinct, permanent, and collectible.[136] These characteristics include fingerprint, face, hand geometry, iris, and voice.[137] However, these techniques suffer from certain drawbacks such as false rejection errors, sensitivity to the environment, user-squeamishness or inconvenience, and cost.[138] Additionally, in healthcare, while biometric methods are used for workforce authentication, they may be unsuitable for patients where a health or physiological condition could itself compromise the efficacy of a chosen biometric characteristic.[139] Biometrics is nevertheless a viable option because characteristics that are inherent to a person are both unique and generally available.[140]

An enhancement to the single-factor system is to use a two-factor system which authenticates a signatory using two distinctive factors – something she has and

---

[135]*See* Rainbow Technologies, Inc., *Two-Factor Authentication – Making Sense of all the Options*, ITSECURITY.COM: THE ENCYCLOPEDIA OF COMPUTER SECURITY (Townsend & Taphouse Feb. 12 (2002), [*hereinafter Rainbow Two-Factor*], *at* http://www.itsecurity.com/papers/rainbow2.htm.

[136]S. Prabhakar et al., *Biometric Recognition: Security & Privacy Concerns*, IEEE SECURITY & PRIVACY MAGAZINE, VOL. 1, NO. 2 33 (Mar.-Apr. 2003), *also available at* http://biometrics.cse.msu.edu/j2033.pdf.

[137]*Id.* at 36.

[138]*Id.* at 35-36.

[139]For instance, an iris-scan on a patient with an eye-infection. *See Ultra-Scan's Livescan Ultrasonic Identification System Achieves Extremely High Results in Independent Lab Tests*, FINDBIOMETRICS.COM (published by TopickZ Inc.), Jan. 23, 2003, at ¶7, *at* http://www.findbiometrics.com/Pages/news_releases/news295.html, [*hereinafter Ultra-Scan*] (stating that conventional optical finger printing technology can "fail to read and enroll significant portions of the population, for example, older people, people with dry skin, people with petite fingers or fine ridge structures, often Asian women and children, and some people with dark skin"). *See also* Vance C. Bjorn, *An Introduction To Privacy And Security Considerations of Biometrics Technology*, 701 PRAC. L. INST./PAT. 105, 107 (2002) (stating that biometrics have "long been used in law enforcement and government applications," and enumerating applications in access control). *But see also* David A. Petti, *An Argument for the Implementation of a Biometric Authentication System ("BAS")*, 80 J. PAT. & TRADEMARK OFF. SOC'Y 703, 703 (1998) (indicating that "widespread regulation of biometrics remains uncharted territory in the legal framework of the United States").

[140]*See* discussion in *supra* section IV.A (comparing the biometric qualities of a handwritten signature which is unique to the signatory and generally available, with algorithmic techniques such as the Schnorr method, which is patented and not generally available). *See also* Edward P. Richards, *Phenotype v. Genotype: Why Identical Twins Have Different Fingerprints*, *in* Identification Evidence at ¶1 (Forensic-Evidence.com 2004), *available at* http://www.forensic-evidence.com/site/ID/ID_Twins.html (illustrating why fingerprints may be key evidentiary distinction between identical twins who are genetically virtually indistinguishable).

something she knows - thereby reducing the risk of fraud.[141] The second factor continues to be the same as single-factor systems; for example, it can be a code or password. The first factor is typically a physical possession such as a key, a card, a token, and so on. The reduced risk of fraud reduces the need for a biometric factor and avoids the associated problems.[142] Two-factor systems themselves come in several flavors including code generation tokens, smart cards, and smart tokens.[143] These devices have varying degrees of reliability and security, but they are susceptible to loss, destruction and malfunction.[144]

VI. REGULATORY EFFORTS AND INITIATIVES TOWARDS STANDARDIZATION

Section V.A introduced some statutory and regulatory schemes for electronic signatures. It also pointed out that these constructions were not specific with regards to the technology behind the signature. One might draw an analogy with the United States Postal Services and other carrier systems such as UPS and FedEx. We rarely wonder why in spite of these being different carrier systems the general delivery of letters, parcels, etc. does not run into the types of problems encountered by electronic transactions. More specifically, while a pathology specimen gets efficiently delivered from a clinic to a laboratory by the local courier who obtains a delivery signature on paper, the electronic transaction involved in sending the pathology report digitally from the laboratory to the clinic runs amuck with difficulties of identification, authentication, privacy, and electronic signatures. It would seem that regulatory schemes that impose electronic transaction standards without delineating any technology can complicate rather than facilitate the portability of transactions.

A. Electronic Signatures in State Statutes

Most states have enacted the UETA.[145] Additionally a few states have enacted electronic signature laws specifically for healthcare.[146] There are two categories of

---

[141]*See Rainbow Two-Factor*, *supra* note 135. The author illustrates a common example of an automated teller machine (ATM) card and a personal identification number (PIN). Together, they represent a form of two-factor authentication. Individually each is useless to a prospective identity thief. Only when used together can an identity be confirmed and access granted.

[142]*Id*.

[143]*Id*.

[144]*Id*.

[145]*See, e.g.*, CAL. CIV. CODE ANN. § 1633.2 (West 2003); COL. REV. STAT. ANN. § 24-71.3-102 (West 2003); CONN. GEN. STAT. ANN. § 1-267 (West 2003); DEL. CODE ANN. tit. 6 § 12A-102 (2001); D.C. CODE ANN. § 28-4901 (2001); FLA. STAT. ANN. § 668.002 (West 2003); ILL. COMP. STAT. ANN. 175/5-130 (West 2003); MD. CODE ANN., COMMERCIAL LAW, § 21-101 (West 2003); MICH. COMP. LAWS ANN. § 450.832 (West 2003); N.J. STAT. ANN. § 12A:12-2 (West 2003); OHIO REV. CODE ANN. § 1306.01 (West 2004); TEX. BUS. & COMM. CODE ANN. § 43.001 (Vernon 2004).

[146]*See* CAL. HEALTH & SAFETY CODE § 123149 (West 2003); CONN. GEN. STAT. ANN. § 19a-25a (West 2003); LA. REV. STAT. ANN. § 40:2144 (West 2003); MISS. CODE ANN. § 41-9-64 (West 2003); N.D. CENT. CODE § 31-08-01.2 (2003); OHIO REV. CODE ANN. § 3701.75 (West 2004).

problems that persist in such statutory schemes. First, the UETA, although consistent in terminology, is not sufficiently specific in requirements.[147] Neither is it clear on methods of implementation to be followed. For instance, section 9 of the UETA states:

> (a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any *security procedure* applied to determine the person to which the electronic record or electronic signature was attributable.
>
> (b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and *surrounding circumstances* at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law. [148] (emphasis added)

Particularly in the area of requirements, this definition creates an obstacle for the enacted law to be useful as a standard. "Surrounding circumstances" is not defined. Nor is there specification of what elements of the circumstances can be considered as representing "agreement."[149] The UETA's definition of "security procedure" also poses similar problems:

> [A] procedure employed for the purpose of verifying that an electronic signature, record, or performance *is that of a specific person* or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures. [150] (emphasis added)

Here, the phrase "is that of a specific person" in itself embodies a wide range of methods to authenticate persons.[151]

To further complicate matters, healthcare-specific electronic signature statutes vary in both specificity and consistency.[152] They also suffer from lack of clarity. For example, the term "two-level access control" under the Ohio law is ambiguous under industry terminology.[153] It could mean a two-factor system described previously.[154]

---

[147] *See, e.g.*, UETA §§ 2(8), 2(10), 2(14), 2(16), at 4-5.

[148] § 9(b).

[149] *Id.*

[150] § 2(14).

[151] *See supra* section V.D.

[152] *Compare* CAL. HEALTH & SAFETY CODE § 123149(g) (requiring signatory authentication by "electronic signature keys") *with* OHIO REV. CODE ANN. § 3701.75(B)(2) (requiring authentication by a "biometric or two-level access control").

[153] *See* § 3701.75(B)(2).

[154] *See supra* section V.D.

But it could also refer to two sets of credentials in a credential hierarchy system.[155] In such a system, the signatory's access to the electronic signature system itself would be conditioned on her credentials existing at two different logical levels in a multi-level hierarchy.[156] However, the focus of the latter approach has more to do with managing *access control* (what systems and functions a person has access to), rather than *authentication* (whether the person indeed is who she is claiming to be). It is relevant to note that while authentication is a prerequisite for access control, the driving factor behind authentication in this discussion is the establishment of the signatory's identity.

In healthcare, such inconsistencies in specifications and implementation would prevent an electronic transaction from crossing a state border with predictable legal effect. The PKI used in one state might incorporate keys that are not recognizable by the PKI used in another state. There may be inconsistent distribution mechanisms of keys. The authentication technique used or implemented in one state may not be the same and hence not verifiable in another state. Finally, even if the information were logically portable, the inconsistency in legal effect would throw valid consent in one state into jeopardy in another.

B. State Agencies: The Ohio State Pharmacy Board & "Positive Identification"

In Ohio, the State Pharmacy Board ("OSPB") is responsible for administering and enforcing laws governing the legal distribution of drugs.[157] The enforcement role in the administration of dangerous drugs has inevitably lead OSPB to address issues surrounding modern electronic methods of drug dispensation and recordkeeping. OPSB's recent rules under the Ohio Administrative Code specify minimum requirements that must be met before a computerized alternative to the traditional paper systems can be used for pharmacy purposes, including data content, refill history, validation, print capabilities, and association of each prescription with relevant patient profiles.[158] Specifically, OSPB's rules focus on three inter-related areas of electronic transactions that are functionally analogous to an electronic signature – authentication, standardization and integrity.[159]

First, with respect to authentication, the rules mandate the requirement of "positive identification" ("PID") of individuals in all electronic pharmacy systems.[160] PID is defined as:

---

[155]*See* Elisa Bertino, *Maχ: An Access Control System for Digital Libraries and the Web*, PROC. OF THE 26TH INT'L COMP. SOFTWARE AND APPLICATIONS CONF. 945, 947 (IEEE 2002), *at* http://semioweb.msh-paris.fr/euforbia/download/max.pdf.

[156]*Id.*

[157]*See* OHIO REV. CODE ANN. §§ 4729.25, 4729.26 (West 2004); *see generally* OHIO ADMIN. CODE § 4729 (2003).

[158]*See* OHIO ADMIN. CODE § 4729-5-28 (2004).

[159]General information about OSPB can be found *at* http://pharmacy.ohio.gov/.

[160]OHIO ADMIN. CODE § 4729-5-01(N).

> [A] method of identifying an individual who prescribes, administers, or dispenses a dangerous drug. Such method must include a physical means of identification such as, but not limited to, the following:
>
> (1) A manual signature on a hard-copy record;
>
> (2) A magnetic card reader;
>
> (3) A bar code reader;
>
> (4) A thumbprint reader or other biometric method; or
>
> (5) A daily printout of every transaction that is verified and manually signed within twenty-four hours by the individual who prescribed, administered, or dispensed the dangerous drug. The printout must be maintained for three years and made available on request to those individuals authorized by law to review such records.
>
> A magnetic card reader or a bar code reader system of identification must also include a private personal identifier, such as a password, for entry into a mechanical or automated system.[161]

The definition incorporates both technical and procedural specifications for an authentication mechanism applicable to electronic signatures. For the purpose of this discussion PID appears to be a fairly comprehensive definition for a number of reasons. It statutorily incorporates the transition between the written and electronic signatures.[162] It also incorporates an enumerated version of the authentication provisions of the Ohio Revised Code §3701.75(B)(2), discussed in section V.A.[163] Finally, it addresses the security concerns of electronic systems, discussed in section IV.B, by incorporating procedural controls for record of authorization of transactions in each 24-hour period, and maintenance of these records for review.[164]

Second, in the area of standardization OSPB acknowledges the variety of methods available for transmission of electronic prescriptions – "[s]ome of the systems are office-based, some are web-based, and some use a switching station to route the prescription to the pharmacy directly from [a prescriber's] computer to a pharmacy computer or facsimile machine."[165] To ensure compliance, OSPB requires

---

[161] *Id*.

[162] *Id.* at (1).

[163] The provision of "two-level access control" under §3701.75(B)(2) is incorporated by combining § 5-01(N)(2) or § 5-01(N)(3) at ¶1, with ¶2.

[164] § 4729-5-01(N)(5).

[165] *See Electronic Prescription Transmission Systems*, [*hereinafter EPTS*], State Board of Pharmacy (Feb. 4, 2004), *at* http://pharmacy.ohio.gov/ElectronicRx-040204.htm (describing electronic prescription systems as those that allow prescriptions to be sent electronically from a prescriber to a pharmacy).

that electronic prescription systems intended for use in Ohio must obtain prior approval from OSPB.[166] The approval includes a review of each system to ensure that "true [PID] of the prescriber sending the prescription" has been achieved under the statute.[167]

Finally, with respect to integrity of the PID, OSPB notes that a mere pictographic representation of a signature visible on a printed version of the transmission does not meet PID requirements.[168] Instead the procedural verification requirement, aimed at non-repudiation of the transaction signatory, uses a written signature on a daily printout of signed actions.[169] However, this unfortunate reliance on printed output in the standard hinders portability for the purpose of electronic signatures. The validation is only available to the sender and not the recipient of the transaction. The result yields a transaction of reduced trust because a key assurance with respect to the trust – the authentication and integrity of the signature – does not electronically travel with the transaction. Indeed, the lack of portability and, the concomitant lack of trust in the transaction, are evident in certain aspects of OSPB's use of electronic prescription systems.[170]

Two further observations can be made about the PID approach in the context of electronic signatures. First, the approach is novel as compared to existing electronic signature systems. Not only does it explicitly disavow pictographic representations of signatures standing alone, but it also obviates the requirement for a *structural definition* of an electronic signature altogether.[171] Instead PID puts its emphasis on the *signatory* rather than the *signature* by requiring that PID be demonstrated at each point where a signatory performs an act of professional responsibility in various pharmacy transactions.[172] In doing so, the definition incorporates the signatory's identity, authentication, consent, and intent into each transaction that requires some accountability.

This implementation has the benefit of being usable in a complex, multi-user environment where a single computer terminal may be used by multiple people in a short time frame. This is the closest and most realistic electronic analogy to a paper

---

[166]*Id.* at ¶2.

[167]*Id*.

[168]*See id.* at ¶3. Item (4) of the paragraph states:

> [An observer], may or may not, see a signature on a prescription sent to a pharmacy by a prescriber using an electronic prescription transmission system. Electronic signatures are not recognized as a means of 'positive identification' and therefore are not required. If a signature is present, the prescription must indicate that the signature was computer-generated.

[169]*See* § 4729-5-01(N)(5).

[170]*See EPTS*, *supra* note 165. Item 1 under ¶3 states prohibits the use of electronic prescriptions for Schedule II controlled substances. Also, only a few systems have been approved under this process, as listed in ¶4.

[171]*Compare* OHIO ADMIN. CODE § 4729-5-01(N) *with* OHIO REV. CODE ANN. § 3701.75(A)(2) discussed in *supra* section V.A.

[172]*See* § 4729-5-28(A)(9), § 4729-5-28(B)(5), § 4729-5-28(C)(1), § 4729-5-28(E)(3), § 4729-5-28(I)(10).

signature, where a signatory can affix her signature or initials where and when necessary, on a single document regardless of its physical custodian. Likewise here, each signatory, whose PID contains the four essential elements of an electronic signature discussed in section V, can electronically sign at various points within a computer session, independent of the owner logged on to the terminal.

Second, the novelty of the approach is ironically its own barrier to portability as compared to PKI. Notably, Ohio is the only state where a state agency has promulgated such a standard.[173] Electronic pharmacy transactions from all other states will therefore not meet the requirements of this law and will have to revert to traditional paper processes. Even if the implementation is adopted by other states, there remains the technical challenge of integrating this scheme with more conventional electronic signature approach in current systems which uses separate logical points for authentication (at the beginning of a session, logon, and so on) and the signature (at the time of action by a signatory, the click of a mouse, a key, and so on). This latter approach fundamentally relies on some a method to identify the signatory (authentication), and separate, logical and structured information to attach to the transaction (electronic signature).

The conventional approach which has been varyingly embraced is neither easy nor efficient to discard. However, for compliance with OSPB's provisions, existing systems may need only minor modifications to introduce the element of authentication at various action points. It can therefore be argued that a structural definition of an electronic signature, although not required, is nonetheless not prohibited by OSPB. It can be further argued that the act of placing a signature on a transaction can be documented by the use of a structurally defined signature, since the latter can be *attached* to the transaction itself. It would therefore supplement the need for using the paper recording of all PIDs used for validation in the OSPB approach.[174] Ultimately, to ensure use of electronic signatures across the conventional systems, while accommodating OPSB's PID requirements, a definition of a structural electronic signature should be retained in any proposed standard.

C. Federal Regulations, Federal Information Policy, & Federal Agency Efforts

At the federal level, in addition to the Federal E-Sign Law, there are other instances of regulation and agency practice that have attempted to create electronic signature standards. While these are somewhat fragmented, they nevertheless shed some light on current thoughts on future national technology policy with respect to electronic signatures in healthcare and other areas of commerce.

The Federal Paperwork Reduction Act was enacted in 1995.[175] The Federal Information Policy was accordingly revised to include aspects of electronic data

---

[173]*See, e.g.*, *Analysis of State Pharmacy Regulations Regarding ADS, Attachment 1: State-by-State Overview of Automated Dispensing* at 23, AMERICAN SOCIETY OF CONSULTANT PHARMACISTS (2001), *at* http://www.ascp.com/public/ga/2001/pdfs/st_auto.pdf. The authors compile lists of states with respect to Automated Dispensing System (ADS) laws. Ohio is the only state that requires PID.

[174]*See* § 4729-5-01(N)(5).

[175]*See* Paperwork Reduction Act, 44 U.S.C.A § 101 (West 2004).

management.[176] Indirectly the act favors PKI as the standard for electronic signatures by stipulating appropriation of necessary funding to the General Services Administration office to "ensure the development and operation of a Federal bridge *certification authority* for digital signature compatibility, and for other activities consistent with this section . . . ."[177] (emphasis added)

Similar trends are also evident in the policies of the department of Food and Drug Administration ("FDA").[178] Following the Federal E-Sign Law stipulations, the FDA defines the electronic signature generally as "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature."[179] This regulation also goes into significant details of implementation: it inherently favors biometric methods of authentication, and explicitly allows two-factor systems in the alternative;[180] it requires that components include identity, consent, and intent;[181] it also requires use of encryption and signature standards to ensure the integrity and security of the signature in both open and closed systems.[182]

The National Institute of Standards and Technology ("NIST") has also been involved in the standardization efforts for electronic signatures.[183] Recently the NIST claims to have taken "a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key-enabled security services" by "coordinating with industry and technical groups developing PKI technology to foster interoperability of PKI products and projects" through the NIST Computer Security Resource Center ("CSRC").[184] Specifically, CSRC has created a Digital Signature Guidance document for a PKI for use by federal agencies.[185] Strongly emphasizing broad use of PKI, the guidance indicates that "the same PKI over time will serve increasingly large numbers of customers, with capabilities such as encryption. Consequently, up-front development costs of the PKI may be evaluated as something to be incurred over time (like maintenance costs) and in the context of a total service delivery program."[186]

---

[176]*See* Purposes, 44 U.S.C.A § 3501.

[177]§ 3501.203(d).

[178]*See* Electronic Records; Electronic Signatures, 21 C.F.R § 11 (West 2004).

[179]§ 11.3(b)(7).

[180]§ 11.200(a).

[181]§ 11.50(b).

[182]§§ 11.10, 11.30.

[183]*See NIST's Role in Electronic Commerce*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2000), *at* http://www.nist.gov/public_affairs/factsheet/ecommerce.htm.

[184]*See NIST PKI Program*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CSRC (2001), *at* http://csrc.nist.gov/pki/.

[185]Kathy Lyons-Burke, NIST Special Publication 800-25: *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CSRC (2001).

[186]*Id.* at 22.

Other departments of the United States government have also released similar documents following the NIST guidelines.[187] But whereas the NIST initiative has significantly aided broad use of electronic signature standards in the federal agencies, its scope is limited to those agencies that have adopted such operational practices. They do not extend to the operations of non-federal entities and certainly do not enter state jurisdictions. Neither do they apply to the context of healthcare which can comprise of both governmental and private entities.

VII. NON-REGULATORY EFFORTS AND INITIATIVES TOWARDS STANDARDIZATION

Aside from federal and state policy goals, there are other significant non-regulatory reasons why electronic signatures in healthcare need standardization. Outside the area of rules and regulations there have been other initiatives both in healthcare and elsewhere, that at their core depend on the portability of authorized transactions. These activities range from national efforts by federal agencies and committees, state health oversight boards, and the private sector.[188] Without a portable standard for electronic signatures these activities and initiatives continue to face an uncertain legal future.

A. The US Dept. of Health And Human Services: The National Health Information Infrastructure (NHII) Initiative

According to HHS, NHII is "the set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health."[189] It is therefore:

- an initiative set forth to improve the effectiveness, efficiency and overall quality of health and health care in the United States
- a comprehensive knowledge-based network of interoperable systems of clinical, public health, and personal health information that would improve decision-making by making health information available when and where it is needed
- the set of technologies, standards, applications, systems, values, and laws that support all facets of individual health, health care, and public health
- voluntary

---

[187] *See NIST PKI Program*, *supra* note 184 (citing similar documents from The National Archives and Records Administration, the Department of Treasury and the Department of Justice).

[188] This note will focus on federal efforts to highlight healthcare transactions that cross state boundaries, which is where the portability of signature standards becomes particularly relevant.

[189] *See FAQs about NHII: What is NHII?*, U.S. DEPT. OF HEALTH & HUMAN SVCS., (2001), *at* http://aspe.hhs.gov/sp/nhii/FAQ.html#What.

> • NOT a centralized database of medical records or a government regulation.[190]

More specifically, it cites lack of standards as one of four barriers to the infrastructure.[191] HHS also acknowledges the importance of its role in national effort "in helping to adopt standards for communication and interoperability between systems."[192]

In an interim report, the NHII workgroup of the National Committee on Vital and Health Statistics ("NCVHS") emphasized the importance of standards and interoperability as follows:

> If information in multiple locations is to be searched, shared, and synthesized when needed, we will need agreed-upon . . . gate-keeping systems…. We will also need reliable and valid data collection methods; common vocabularies for personal, clinical and public health information; *compatible systems to manage, transmit and protect the confidentiality of information; and standards for interoperability*.[193] (emphasis added)

Of course, for the reasons discussed in section III, interoperability and transmission of confidential and individually identifiable health information will be obstructed if the consents and authorizations to such use, and the attendant disclosures, are not standardized and understood by the various systems involved in the transaction.

The gateway systems referred to in the report would be unable to process interstate healthcare transactions as envisioned by the NHII.[194] Assume that a patient who ordinarily lives and receives health care in Atlanta, Georgia and who is diagnosed with cardiac myopathy is flown in to Cleveland, Ohio, for a heart-transplant. Further assume that the patient has electronically signed appropriate informed consent and waiver documents. Finally, assume also that the donor is a deceased patient from Louisville, Kentucky, whose family or estate has provided similar consent to his primary care provider in accordance with provisions of his will. Both sets of consents, along with pertinent clinical and medical history of both patient and donor would have to electronically arrive at Cleveland prior to the surgery, and distributed to all the relevant hospital staff and only the relevant staff.[195]

---

[190] *Id*.

[191] *Id. at* http://aspe.hhs.gov/sp/nhii/FAQ.html#Barriers.

[192] *Id. at* http://aspe.hhs.gov/sp/nhii/FAQ.html#HHS. *See generally* A Strategy For Building The National Health Information Infrastructure, Report and Recommendations From the National Committee on Vital and Health Statistics Washington, D.C. (November 15, 2001), [*hereinafter NHII Strategy*], *at* http://www.ncvhs.hhs.gov/reptrecs.htm.

[193] *See* Interim Report: Toward a National Health Information Infrastructure § 2, NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, at http://www.ncvhs.hhs.gov/NHII2kReport.htm. (2000).

[194] *See id.* § 5, *at* http://www.ncvhs.hhs.gov/NHII2kReport.htm#infrastructure.

[195] *See* 45 C.F.R. §§ 164.502(b), 164.514(d) (stipulating minimum necessary disclosure of protected health information).

The availability of the transactions involved here are not the technological challenge. However, the transactions could not be meaningfully utilized if they were not transmitted with reliable and interoperable indications of the patient's identity, intent, and consent.[196] Additionally, there would have to be utmost assurance that (a) the transacting hospital entities were indeed who they are, and (b) that the information whose accuracy is critical to the life of the patient, had not been tampered with or altered, either inadvertently or intentionally, during transit. Finally, the technology implemented for such assurances of authentication and integration would have to be understood by the disparate systems at the various facilities in three states. This is only possible if the systems followed a single standard.

B. Recommendations of the NCVHS: The Need for a Federally Mandated Electronic Signature Standard in National Healthcare

In its report, the NCVHS also lists the perceived obstacles between the current state of affairs and the desired future.[197] They include consumer and industry attitudes and practices in healthcare:

> Health care professionals will need to reach consensus on and accept the contribution of practice guidelines and other knowledge management tools. *Public health will need to include in its toolkit integrated data systems*; high-quality community-level data; tools to identify significant health trends in real-time data streams; and geographic information systems. Consumers and patients must have confidence the NHII will deliver real benefits. They will need to feel comfortable that an appropriate balance is being struck between their desire to *safeguard personal health information and health professionals' need for de-personalized information to protect public health, conduct medical research, and improve health care quality*.[198] (emphasis added)

The "toolkits" can only be developed if the efforts are based on a standard in which the public can have some confidence. This, perhaps more than any other element of healthcare practice, supports the need for a federally regulated and mandated standard as proposed here.

There are a few lessons to be learned from the promulgation of the Administrative Simplification provisions of HIPAA.[199] A study in the 1980s on costs in healthcare found that a staggering proportion of federal dollars spent on healthcare was expended in *recovering the cost* of healthcare itself.[200] It was estimated that "almost one-fourth of total health care spending [in 1987]" was

---

[196]*See id.* § 2, *at* http://www.ncvhs.hhs.gov/NHII2kReport.htm#stands.

[197]*Id.*

[198]*See id.* § Attitudes and Practices.

[199]45 C.F.R §§ 160, 162 (West 2004).

[200]*See* Goodman, John C. and Musgrave, Gerald L., *Patient Power* (Cato Institute, Washington, D.C. 1992), excerpt *at* http://www.ncpa.org/w/w53.html.

expended in administrative costs.[201] The study attributed this cost to hospitals spending an enormous amount of time on paperwork for both financial exchange and determination of proper and necessary care.[202] In November 1991, Secretary of HHS, Dr. Louis Sullivan, convened a forum of national health care leaders to discuss the challenges of reducing administrative costs; the forum subsequently formed a voluntary, public-private task force called the Workgroup for Electronic Data Interchange ("WEDI").[203]

The findings of WEDI were less than flattering. According to WEDI, improvement to healthcare costs could be realized only if the healthcare industry adopted the X12 EDI transactions.[204] It also recommended that the requirements be federally mandated.[205] Based on their recommendations the original EDI provisions of HIPAA Administrative Simplification were drafted. Although the final rules include privacy and security provisions for health information,[206] the very existence of these recommendations and ensuing regulations reflect, and even suggest, the health industry's reticence to technical self-regulation or standardization.[207]

C. The Private Sector: Federated Identity Management

Previous sections have highlighted access control and signatory authentication for electronic signatures.[208] The absence of consistent standards for authentication has led to certain private sector initiatives, the most recent (and perhaps the most prominent) of which is federated identity ("FID") management.[209] David F. Carr describes FID as a form personal of identification; individuals can use the same FID to sign on to different systems belonging to multiple enterprises to conduct transactions.[210] Although similar to PKI certificates, FIDs are unique because they use a cooperative system of trust where partners offer FIDs to their clients and customers, "depend on *each other* to authenticate their respective users," and "vouch for their access to services."[211] (emphasis added) This would allow a physician with

---

[201] *Id*.

[202] *Id*.

[203] *See Executive Summary*, The 1993 WEDI Report § *i* (October 1993). WEDI is located at http://www.wedi.org. The full report, [*hereinafter WEDI Report*], is located at http://www.wedi.org/public/articles/full1993report.doc.

[204] *Id*.

[205] *Id*. at 1-1. *Appendix 1: Standards Implementation and Uniform Data Content* at ¶1 makes the following recommendation: "Mandate, by federal law, that all health care participants use ASC X12 standards."

[206] *See* 45 C.F.R. §§ 160, 164 (West 2004).

[207] *See WEDI Report*, *supra* note 203 at § ii (Executive Summary).

[208] *See supra* sections IV.B, at 11; V.D, at 18.

[209] *See* David F. Carr, *Primer: Federated Identity Management*, BASELINE, November 3, 2003, *at* http://www.baselinemag.com/article2/0,3959,1373941,00.asp.

[210] *Id*.

[211] *Id*.

a FID from her own facility, who refers a patient to another facility, to update an internal record of on the latter facility's data network, while using her own facility issued FID. To enable this, the two facilities would have to be trusted and cooperative partners in a FID agreement.

Companies internally use various protocols to recognize their users' identities. Maintaining the identities of all employees of all partners in the various systems would be a prohibitively cumbersome task. To overcome this, FIDs utilize communications protocols such as the Security Assertion Markup Language ("SAML") to share information contained in FIDs, across computerized applications and systems. Hence, a company keeps only its own directories and FIDs; it securely exchanges FID information from it with those of its partners and vice versa without needing to adopt the same technologies for the disparate authentication services of its partners.[212] The principle proponents of the emerging SAML standard are the Organization for the Advancement of Structured Information Standards ("OASIS") and the Liberty Alliance Project ("Liberty").[213] Liberty, an industry group formed under the Institute of Electrical and Electronics Engineers ("IEEE") to promote FID standards, adopted SAML version 1.1 as part of its application framework.[214] Early adopters of FID include American Express, Boeing, General Motors and Nokia.[215] FID management is an attractive alternative to managed PKI, but the case studies of the early adopters highlight the challenges that would face healthcare were it to become an adopter to the standard.[216] These challenges are both logistic as well as legal.

Logistically, a single healthcare system can provide multiple types of specialized care at multiple locations.[217] In a 2001 article, Nicholas P. Terry notes that "a patient's [health information] likely will be spread across many systems and various [computerized patient records ("CPRs")]." Referring to CPRs as the location for maintaining longitudinal health records to improve healthcare quality, Terry notes that "some of a patient's medical records will be in discrete *unregulated* systems," so that his discussion uses the "somewhat inaccurate singular form for CPR, including

---

[212]*Id.*

[213]OASIS is located at http://www.oasis-open.org/home/index.php; Liberty is located *at* http://www.projectliberty.org/.

[214]*See* David F. Carr, *supra* note 209. For a layout of Liberty's proposed specifications using this standard, *see* Liberty Alliance Project Phase 2 Specifications (The Liberty Alliance 2003), *at* http://www.projectliberty.org/specs/index.html.

[215]*Id.*

[216]For an excellent overview of case studies of the early adopters of FID *see* Dan Blum, *Federated Identity: Early Adopters Case Studies and Lessons Learned* at 10 (The Burton Group, September 2, 2003), *at* http://www.burtongroup.com/guests/content/report/liberty alliance1.asp (website requires free registration to access this complementary content; also on file with the Journal of Law & Health).

[217]*See, e.g.*, The MetroHealth System located at http://www.metrohealth.org. The system directory page, located *at* http://www.metrohealth.org/general/directory/directory.asp, lists various types of services provided.

within that concept multiple, but interoperable and interlinked CPRs."[218] (emphasis added) The challenge exists because realization of the goals of FID would initially require standardizing authentication and access control in various systems *within* a healthcare organization in compliance with the HIPAA Security Rule.[219] Even beyond this, maintenance of uniform longitudinal health records in disparate systems would be difficult at best if such maintenance were dependant on cooperative technology efforts and resources of diverse participants ranging from single practitioner offices to a large multi-site healthcare systems and insurance companies. HIPAA itself acknowledges these variations in both statutory definitions as well as comments in the preamble.[220]

Legally, FID's requirement of trusted partners may raise concerns of liability and indemnity. Analyst Carol Coye Benson points out that the liability has to do with the *quality* of the identity itself.[221] In essence, because one healthcare organization would have to trust FIDs provided by another, the liability would arise from doubts regarding the integrity of and the ability to repudiate the identity information. This trust is relevant in the context of our discussion of signatory authentication in section V.D.[222] Assume that hospital *A* grants its employees FIDs and each FID contains the birth date and social security number for verification. This practice may be unacceptable to insurance company *B* whose FIDs additionally record the signatory's telephone number, mother's maiden name, and city of birth. *B* might argue that its practice yields higher *quality* FIDs (i.e. less susceptible to fraudulent use). *B* may well require *A*, to either implement stronger FIDs or indemnify *B* from any harm resulting from fraudulent use of *A*'s FIDs. Although Benson's ultimate conclusion that "large-scale identity federations will all operate with explicit disavowals of liability" is perhaps somewhat unrealistic, it nevertheless identifies the problem.[223] It would appear that there is no legal standard or precedent addressing the quality of the FID. Furthermore, in a cooperative environment the formulation of a standard would be extremely difficult given the individual investments made by various healthcare institutions in their diverse authentication systems.

Ultimately, the establishment of any standard to ensure quality authentication is likely to fall on third party professional identity providers such as CAs.[224] Many CAs currently provide some assumptions of liability with regards to the use of their

---

[218]Nicolas P. Terry, *An EHealth Diptych: The Impact Of Privacy Regulation On Medical Error And Malpractice Litigation*, 27 AM. J.L. & MED. 361, 370 (2001) (emphasis added).

[219]45 C.F.R. §§ 164.312(a)(2)(i), 164.312(a)(2)(iv); *see also supra* section IV.B.

[220]*See*, *e.g.*, 68 Fed. Reg. 8334, 8357 (February 20, 2003) (referring to "small rural providers" in preamble); *See also* §160.103 (defining "small health plan").

[221]*See* Carol Coye Benson, *Liability and Federal Identity: Much Ado About Nothing?*, DIGITAL ID WORLD, Nov./Dec. 2003, at 70-71, *at* http://magazine.digitalidworld.com/Nov03/Page70.pdf.

[222]*See supra* section V.D.

[223]*See* Benson, *supra* note 221, at 70.

[224]*Id.* at 72.

PKI certificates.[225] In healthcare, under the HIPAA Security Rule, liability protection and indemnification language may be considered a statutory requirement in agreements with business associates.[226] Based on these considerations, FIDs may not provide legally reliable and predictable signatory authentication for the purpose of electronic signatures as compared to PKI.

VIII. THE IRONY: THE REAL SCENARIO OF PORTABLE HEALTHCARE

In light of current circumstances, my imaginary encounter at UAMC system would likely be less than the utopian picture painted in section I. Instead, I would have to enter the hospital as an emergency department ("ED") patient, rather than a referral patient, since this would be the most expedient way to get care without an appointment. Much waiting and signing of several pieces of paper would be followed by more waiting before contact with a PSR. After all, in a trauma facility, my influenza or even suspected pneumonia would be less critical than gunshot wounds.

It would be almost two hours later that the PSR would have finally obtained my relevant pharmaceutical history by interviewing me (although this information already exists in my electronic record in Cleveland). It would be 10:00 PM before the attending physician would finally receive a faxed copy of my records from Cleveland, because the first transmission of my authorization would be lost in transit, sent to a fax number incorrectly entered by an orderly in the frenzy of ED activities. The physician would then formalize his decision to admit me for observation, with his staff faxing off a Notice of Admission to MMO. The facility would then go about the laborious process of preauthorizing my treatment and observation stay through a combination of phone calls and fax transmissions. I would have signed several more paper authorizations and disclaimers. In the flurry of papers, my copy of the NPP would be lost.

I would finally be in my assigned bed for the night. I would be immersed in a pamphlet with instructions about resolving billing and insurance processes awaiting my return to Cleveland. With dawn only a few hours away, I would be oblivious to the snow falling outside. *Blow Fly* would have to wait.

IX. PROPOSAL: FINAL HIPAA ELECTRONIC SIGNATURE RULES - A HEALTHCARE PKI

One observation that can be made from the preceding sections is that availability technology is not the barrier for portability of electronic signatures. If anything, there are too many choices of technology. Neither is availability of model standards the problem. Indeed, the main problem is the lack of a *single adopted* technology standard.

A second observation is that a reasonable scheme already exists in the proposed HIPAA electronic signature rule.[227] The scheme addresses the basic requirements of

---

[225] *See, e.g.*, Secure Payments: Buyer Authentication (VeriSign, Inc. ©1995-2004), *at* http://www.verisign.com/products/payflow/fraud/protection/buyerauth.html (describing integrated liability protection from Visa® and MasterCard®).

[226] *See* 45 C.F.R. §§ 164.308(b)(1), 164.314(a)(1).

[227] *See* 63 Fed. Reg. 43,241 (1998).

identity, authentication, consent, integrity and security as they uniquely apply to healthcare providers, payers and clearinghouses.[228] Improving on the existing proposed rule can thus create a workable proposal, and is arguably the most logical approach to a national electronic signature standard for healthcare.

A. A Final Electronic Signature Rule Under HIPAA – Modifications to the Proposed Rule

The central thrust of this proposal is to set up a trust infrastructure for E-health under the proposed electronic signature rule of HIPAA.[229] It is also recommended that all technical specifications and standards under the rule be developed or adopted jointly by NIST and ANSI and maintained by them as the designated standards maintenance organizations ("DSMO").[230] To this end, the following refinements to the existing proposed rule are added:

1. Identity

The Federal E-Sign Law is testimony to the realization that the only feasible solution for identity management in e-commerce is a PKI. The HIPAA provisions should accordingly incorporate this requirement in the form of a healthcare PKI. The key or certificate management standard should follow the NIST recommended X.509 version 3 public and private keys, further adapted to include identity roles in healthcare transactions.[231] The specifications should be adopted and maintained by HHS as formal regulatory standards.[232] Finally, a division of HHS should become the designated CA, either directly, or through delegation to another DSMO, for all PKI certificates assigned for healthcare operations.[233]

2. Authentication

Typical biometric systems used for authentication for the purpose of access control may not be the most efficient technology for authentication of a signatory's identity for reasons identified earlier.[234] For the typical healthcare consumer, this

---

[228] *Id*.

[229] *Id*.

[230] *See* Health Insurance Reform: Announcement of Designated Standard Maintenance Organizations, 65 FED. REG. 50373 (August 17, 2000), [*hereinafter HIPAA DSMOs*], where pursuant to 45 C.F.R. § 162.910, the Secretary of HHS has designated the following organizations as DSMOs: Accredited Standards Committee X12; Dental Content Committee of the American Dental Association; Health Level Seven; National Council for Prescription Drug Programs; National Uniform Billing Committee; National Uniform Claim Committee.

[231] One acting as a provider signing on a healthcare document in one transaction could herself be a patient providing consent in a different transaction or care setting. An identity management solution would have to accommodate these distinct roles of a single signatory in the healthcare setting.

[232] *See* HIPAA DSMOs, *supra* note 230.

[233] *See supra* section V.C (discussing PKI and CAs).

[234] *See supra* section V.D.

could represent unacceptable delays in healthcare should such systems malfunction. It is useful to note that more sophisticated biometric systems are available that can virtually eliminate false rejections.[235] However commercial application of such systems in healthcare has two drawbacks: (a) they are usually not cost-effective solutions, and (b) they often use proprietary or patented techniques, with the associated problems discussed in section IV.A. Accordingly, digital signature capture solutions that capture signature metrics are favored over biometric solutions in this proposal.[236] This technique offers the benefits of biometrics while retaining a pictographic symbol familiar in printed output. The standard should specify the minimum metrics to be captured in digital signature capture systems to ensure portability of authentication. Appropriate metrics templates should be incorporated into the modified X.509 key standard for signatures thus captured.[237]

Two-factor authentication can also be used as an alternative method, with a digital signature code unique to the user to be attached to each transaction.[238] It is noted that when sufficiently developed, the emerging SSL/UA standard can be incorporated into this standard with its attendant benefits of easy distribution and low cost.[239] It is useful to reiterate that authentication here is narrowly tailored for use in electronic signatures.[240] For the purpose of general workforce access control, either conventional biometrics or two-factor authentication remain the principal choice. Specifically, where a member of the workforce is also a patient, the use of both methods is not precluded in the scheme proposed here.

3. Intent And Consent

Standard consent language fields should become a part of the transaction content for all healthcare transactions. Logical manifestation indicating intent and understanding of the transaction content is more complex, and should be formalized

---

[235] *See, e.g.*, Ultra-Scan® Corporation, located *at* http://www.ultra-scan.com/. Ultra-Scan offers high-accuracy ultrasonic fingerprint identification technology based on patented processes. One such patent listed among others is U.S. Patent No. 6,296,610 (issued Oct. 2, 2001). This patent, titled *Ultrasonic Biometric Imaging And Identity Verification System*, is for an ultrasound imaging method for human tissue surface, where "[t]he quality of the images obtained using ultrasound technology is superior as compared to those obtained using optical technology since the ultrasonic images are less dependent on the surface condition of the finger." *See also Ultra-Scan*, *supra* note 139.

[236] *See* Benjamin Wright, *Eggs In Baskets: Distributing The Risks Of Electronic Signatures*, 15 J. MARSHALL J. COMP. & INFO. L. 189, 195 (§ 5 describes a pen biometrics technology that captures signatures made on a digital pad, and measures "size, shape, and relative positioning of the curves, loops, lines, dots, and crosses, as well as the relative speed at which each feature is imparted." *See generally* Larry Donovan, *Secret Identities*, FIN. TIMES, Feb. 6, 1996, at Technology 11 (discussing possible mechanisms to secure e-commerce transactions).

[237] *See* X.509 Attribute Certificates, *supra* note 131.

[238] *See* SCHNEIER, *supra* note 26.

[239] *See Rainbow Two-Factor*, *supra* note 135, at The Next Wave of User Authentication – SSL User Authentication.

[240] *See supra* section V.D.

in the standard as a mechanism of recording a series of actions such as key-strokes (e.g. the Page Down key) indicating that the signatory has viewed all the appropriate screens by paging through them before signing.

4. Integrity And Security

PKI ensures the integrity and security of transactions because it allows the incorporation of encryption and integrity check schemes into the various stages of the transaction creation, transmission, receipt, and acknowledgment sequence.[241] The only remaining stipulation required here is the use of a standard encryption scheme. Owing to the rapid development and improvement in encryption ciphers and their relative strengths, this area of the standard could be stipulated as a set of minimum requirements. However, in the interest of ensuring portability, a better proposition would have requirements specified and adopted by the DSMOs as part of the PKI, to be updated as needed by proposed HHS rule-making from time to time. This will further ensure that the technical maturity of the standard remains flexible to the underlying legislative processes.

B. Benefits of Electronic Signature Regulations Under HIPAA: The Role of the Federal Government in Healthcare as a National Enterprise

The benefits of the proposed standard are numerous. First, the proposal calls for a modification of *existing* proposed rules under HIPAA. New congressional lawmaking will not be required; instead refinement and furtherance of existing agency regulations will suffice. Legislative and judicial challenges of new congressional lawmaking thus will be avoided. Additionally, HHS will have the benefit of experience gained from the ongoing implementation of the Transactions and Code Sets rules of HIPAA in the area of patient financial transactions.[242]

Second, HIPAA includes a broad grant of authority from Congress to HHS as to the regulation of medical information:

> If legislation governing standards with respect to the privacy of individually identifiable health information transmitted in connection with the transactions described in section 1173(a) of the Social Security Act (as added by Section 262) is not enacted by [August 21, 1999], the Secretary of Health and Human Services shall promulgate final regulations containing such standards. . . . [243]

HIPAA also includes provisions that address the issue of non-preemption of state laws by clarifying that "[a] regulation promulgated under [the rule] shall not supercede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation."[244] Since the UETA is modeled after the Federal E-Sign Law, and this

---

[241] *See supra* section V.C

[242] 45 C.F.R. §§ 160, 162.

[243] *See* 110 STAT. 1936, 2033 § 264(c)(1).

[244] § 264(c)(2).

proposal draws on the latter, non-preemption should not be a problem in states that have only enacted the UETA. However for those states where disparate electronic signature statutes exist specifically for healthcare, the proposed standard should prevail; more stringent state technical standards may nevertheless be incompatible with this standard in the realm of portability. Therefore, minimally the preemption clause should apply to invalidate any state statute whose implementation would be *contrary* to the technical standards developed under this proposal.

Third, Congress's legislative authority under HIPAA has successfully passed judicial scrutiny. In *South Carolina Med. Ass'n v. Thompson*, the appellants challenged HIPAA on grounds of impermissible Congressional authority and sought to have several provisions of the HIPAA declared unconstitutional.[245] The fourth circuit rejected the argument because "Congress laid out an intelligible principle in HIPAA to guide agency action . . . ."[246] The court found the promulgation of the regulations to be "a necessary cooperation between coordinate branches" rather than a constitutionally impermissible delegation of legislative authority.[247] In particular the court pointed out that the regulations focused on "enabling electronic *portability*, not simply on regulating purely electronic activity."[248] (emphasis added)

Similarly, in *Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dept. Of Health and Human Services*, the petitioners challenged the authority of HHS under HIPAA claiming that it violated the Tenth Amendment to the United States Constitution.[249] However, that court also rejected the complaint because "HIPAA regulates interstate economic activity" and "[h]ealth care providers transmitting health information in electronic form in connection with health claims, referral authorizations, and health care payments, also engage in interstate commerce."[250] It thus concluded that HIPAA fell within Congress's authority under the Commerce power.[251]

Finally, in the NHII reality healthcare effectively ceases to be a local or state owned process. Instead it becomes a national industry that facilitates the delivery of healthcare seamlessly and uniformly across state borders. In this context, conflicting standards that impede the flow of healthcare transactions across state borders would be contrary to national healthcare policy. Indeed, one could go so far as to argue that if NHII becomes the *de facto* standard for electronic healthcare, any state electronic signature law for healthcare that contradicts the infrastructure's intended portability also effectively "burdens interstate migration and thus violates the [signatory's constitutional] right to travel."[252]

---

[245]South Carolina Med. Ass'n v. Thompson, 327 F.3d. 346, 348 (4th Cir. 2003).

[246]*Id*.

[247]*Id.* at 350.

[248]*Id.* at 353.

[249]Ass'n of Am. Physicians & Surgeons, Inc. v. U.S. Dept. of Health and Human Servs. 224 F. Supp. 2d 1115, 1125 (S.D.Tex 2002).

[250]*Id.* at 1126.

[251]*Id*. (citing U.S. v Gregg, 226 F. 3d 253 (3d Cir 2000)).

[252]*See* Anderson v. Green, 513 U.S. 557, 558 (1995) (citing Shapiro v. Thompson, 394 U.S. 618 (1969)).

C. Implementation, Non-Compliance, and Sanctions: Some Final Thoughts

It would be prudent to note that NCVHS's final report on the NHII[253] is followed closely in time by its formal recommendations for the Patient Medical Records Information ("PMRI") standards.[254] Specifically, *PMRI Recommendation*, made pursuant to a provision in HIPAA,[255] stipulates Health Level Seven as the current standard for clinical transactions such as order entry, scheduling, medical record/image management, patient administration, observation reporting, financial management, and patient care.[256] This is the last significant piece of the electronic healthcare puzzle. While the standard transaction provisions under HIPAA address the financial and billing transactions for healthcare, *PMRI Recommendations* would cover clinical transactions.[257] This is arguably the best opportunity the health industry has had to effectuate true portability of a standardized healthcare transaction – an effort that at its forefront must include the electronic signature issues for reasons previously discussed.

One might also note that state signature statutes rarely contain explicit sanctions for violations; as seen earlier, disputes involving non-compliance have had to resort to the common law.[258] In contrast, HIPAA stipulates civil and monetary penalties for violations of the HHS rules.[259] Additionally, HHS can bring to bear the enormous financial weight of the federal Medicare and Medicaid programs as healthcare payers in order to encourage compliance. The sanction provisions, combined with this financial clout, would make a modified final HIPAA electronic signature statute, under the authority of HHS, the ideal approach to achieving the vision of NHII.

X. CONCLUSIONS

NHII's vision of an integrated health information infrastructure can provide a truly seemless healthcare environment for today's patient. Information can freely flow between entities across state borders. The vision is fundamentally dependant on various functions of the traditional signature in the healthcare context. Such functions are a product of both the common law as well as legislative efforts at state and federal levels. To bring healthcare into the electronic information age, one must migrate healthcare information management from paper processes to electronic records. An integral and vital part of this migration is the formulation of an

---

[253]*See* NHII Strategy, *supra* note 192.

[254]*See* John Lumpkin (Chair NCVHS), *Letter to the Secretary, U.S. Department of Health and Human Services* (February 27, 2002), [*hereinafter PMRI Recommendation*], *at* http://www.ncvhs.hhs.gov/020227lt.htm. For a timeline, *see* the NCVHS Reports and Recommendations website, *available at* http://www.ncvhs.hhs.gov/reptrecs.htm.

[255]*See* 110 Stat 1936, § 263, codified at 42 U.S.C.A § 242k(k).

[256]*See PMRI Recommendations*, *supra* note 254. Health Level Seven is *available at* http://www.hl7.org.

[257]*Compare* 45 C.F.R. § 160, 162.1101 *et. seq. with PMRI Recommendations*, *supra* note 254.

[258]*See supra* section II and cases therein.

[259]*See* 42 U.S.C. § 1320d-6.

electronic signature that is uniform and portable. Portability will assure that the legal requirements of signatures – identity, authentication, consent and intent, and integrity and security – become a part of each healthcare transaction.

The ultimate realization of NHII will necessitate creating a healthcare PKI. A PKI will inherently provide non-repudiated authentication of the signatory's identity, consent, and intent. It will also ensure integrity and security of the transaction content through encryption. Current regulatory efforts at standardization through state statutes, federal regulations, federal information policy, and federal and state agency rules have produced inconsistent results. But these efforts point to the need for a healthcare PKI. This position is also supported by non-regulatory efforts and initiatives both at the federal level as well as in the private sector. The absence of a uniform standard destroys the utopia of the NHII with the frustrations of non-portability.

Accordingly, a federally mandated uniform statutory scheme would be ideal under a final modified version of the pending HIPAA electronic signature rule. It would create a national healthcare PKI, and address all aspects of electronic signatures - identity, authentication, consent and intent, and integrity and security. Such a rule would benefit from the federal government's role in national healthcare and its prior experience with implementation of other HIPAA provisions. The federal government's authority to create such rules through HHS has already been endorsed by the judiciary. Finally, the civil and monetary penalties of non-compliance under HIPAA, as well as HHS's financial weight as a payer in the healthcare industry, would ensure satisfactory compliance with the rule's standards. NHII could indeed be the reality of future national healthcare.

ASHOKE S. TALUKDAR[260]

[260]Ashoke Talukdar is Manager, Information Security & Compliance for The MetroHealth System located in Cleveland, Ohio where he has held this and other technology positions since 1995. Mr. Talukdar is a J.D. candidate for December 2005 at Cleveland State University, Cleveland-Marshall College of Law.