The Personal Internetworked Notary and Guardian (PING):

The Policy Implications of a Patient-Controlled Electronic Medical Record

Daniar Hussain, Andrew Werner, Neil Desai

Department of Electrical Engineering and Computer Science

Massachusetts Institute of Technology, Cambridge, MA

May 16, 2002

MIT Course 6.805

Prof. Hal Abelson

ABSTRACT

There have been many attempts to create longitudinally-integrated, nation-wide electronic patient record systems ever since information technology has infiltrated the medical profession. This paper compares two recent attempts – a legislative attempt in the Universal Health Identifier (UHID) mandated by the Health Insurance Portability and Accountability Act (HIPAA) and a technical attempt under development at Children's Hospital and MIT called the Personal Internetworked Notary and Guardian (PING). The paper uses these as a case study of two very different approaches to the medical records problem, and examines why UHID failed, and how PING is likely to succeed. PING's technical architecture is examined in depth, and it is compared and contrasted to UHID's stated objectives. Practical market, policy, and legal issues surrounding the national deployment of PING are examined.

TABLE OF CONTENTS

PART I: INTRODUCTION

1.1 Overview

In recent years, medical records have been increasingly kept in electronic form. A computerized patient record keeping system brings with it many advantages; however, the often fragmentary nature of patient records impede the utilization of medical informatics technologies to their fullest extent. A legislative solution emerged in 1996: a national mandate for a scheme that would assign every individual in the United States a unique identifier, so as to facilitate the gathering of health information across organizational boundaries. This met with substantial opposition from privacy organizations and citizens concerned the threat that such a system would pose to the confidence in which their health information would be held.

There exists an alternative solution. Due to the increasing ubiquity of information technology, it is now possible to imagine a patient owned medical record, accessible from many points and to many people, all under the supervision of the entities with the most direct interest in the patients' health information – the patients themselves. The Personalized Internetworked Notary and Guardian, or PING, is a project currently under development as a joint project between the MIT Laboratory for Computer Science (LCS), the Children's Hospital Informatics Program (CHIP), and Harvard Medical School. PING is designed as an adjunct to existing hospital medical record systems, enabling the creation of a lifetime personal medical record, owned by the patient. We contend that PING solves the "medical record problem" better than the unique health identifier or a similar system, as PING effectively leverages technology to enable a solution that is tailored to suit the educated health care consumer's needs.

1.2 The medical record problem

The practice of medicine generates large quantities of information. The enormous complexity of modern health care practice has been accompanied by an increase in the power of the means used to manage medical data. The move to a computerized medical record-keeping system brings with it several substantial advantages.[1] First, increased ease in accessing a patient's medical record can improve the quality of healthcare service received by the patient. Second, medical research programs can benefit from the increased massing of data provided by a unified, electronic database, centered in a hospital or some other locus of health service. Finally, electronic record-keeping lowers administrative costs.

In recent years, substantial progress has been made toward the successful implementation of computerized patient records. However, the full potentialities of a computerized patient record-keeping system have yet to be realized. The modern patient is likely to obtain health care in a variety of geographic locations, from a variety of providers,[2] fragmenting the patient's medical record across geographic and institutional boundaries. For patients with complex medical conditions, moving information essential to the proper administration of health care between a variety of providers can prove to be extraordinarily difficult.[3] The problem lies not only in the movement of electronic information from one organization to another, but also in the management of many legacy records which are still kept on paper.

---

[1] R. Dick et al. The Computer-based Patient Record: An Essential Technology for Health Care. National Academy Press: Washington, D.C., at 53.

[2] Cochran, David, M.D. The coming of age of consumer health informatics. Presentation before the 1999 CPRI Fall Conference, at 8. As Cochran points out, physician loyalty is eroding with the coming of younger healthcare consumers. Source: IFTF and Princeton Survey Research Associates, Consumer Behavior Survey, 1998.

[3] Conversation with Prof. Peter Szolovits, MIT Laboratory for Computer Science, 26 March 2002.

Aware of the administrative obstacles impeding a truly successful implementation of an electronic patient record, Congress passed regulations designed to remove the aforementioned obstacles in 1996, as part of the Health Insurance Privacy and Accountability Act (HIPAA).[4] A major component of this administrative simplification was the establishment of a "standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system."[5] The stated goals of the "standard unique health identifier" include:[6]

- Assurance of continuity of care

- Accurate record keeping

- Prompt payment and detection of fraud, waste, and abuse

These goals will form the central benchmark by which the unique personal health identifier and the PING system are judged in this paper. They constitute a baseline set of goals that policymaking organizations have agreed upon to facilitate the effective sharing of health information. In the first part of this paper, we examine the unique health identifier in detail, discussing its legislative history, the policy goals that motivated its initial enactment into law, and the criticisms that have inhibited its full realization. In the second part, we put forth a detailed architectural examination of the PING system and discuss its applicability to the problem at hand. In the final part, we demonstrate first the adequacy of PING to provide a reasonable means of achieving the main substance of the policy goals that motivated the unique health identifier, and then contend that the architectural features of PING improve quality of care in modes inaccessible to pure

---

[4] Health Insurance Privacy and Accountability Act of 1996 (HIPAA), §1173(a)
[5] Id., §1173(b)(1)
[6] U.S. Department of Health and Human Services, Unique Health Identifier for Individuals: A White Paper

legislation. We conclude with comments on the conception of PING as an instrument of

policy.

PART II: UNIQUE HEALTH IDENTIFIERS

2.1   Introduction and Background to HIPAA

2.1.1   <u>HIPAA Overview</u>

The Health Insurance Portability and Accountability Act of 1996 (The Kassebaum/Kennedy Act) was a Congressional attempt enacted in order to address issues dealing with health care reform. Rooted in the proposals of health care reform in the early 1990s, the main motive behind HIPAA was to better provide access to health insurance, limit fraud[7] and abuse, and reduce administrative costs[8].

HIPAA's legislative motivation was influenced by the increasing use and reliance of electronic means of communication. In HIPAA, Congress asked the Department of Health and Human Services (HHS) to determine certain standards to which health plans, providers, and clearinghouses must abide. These standards dealt with transaction formats and exchange of information which would be necessary because these institutions engage in a great deal of administrative transactions — whether they be financial or logistical.

Congress also directed the HHS to develop regulations to protect the security and integrity of electronic technology and communication after realizing the inherent risks associated with advances in such technology. Additionally, Congress also realized that since there would be an increase in the ease of transmitting electronic information, privacy protection must be increased. Thus, HIPAA required the induction of a privacy statute within three years of the date of enactment. Since Congress had failed to enact any

---

[7] It is estimated that more than $.20 of every healthcare dollar is spent on administrative overhead, with an additional $.11 of every healthcare dollar spent fraudulently. Source: Smed, http://www.smed.com/hipaa/overview-fastfacts.php (accessed 13 May 2002).
[8] When fully implemented, it is conservatively estimated that HIPAA transactions will save providers $9 billion annually. Source: Ibid.

such privacy legislation, the HHS was the authority in setting forth standards to which medical practices must adhere to protect the privacy of health information.[9] A more comprehensive legislative history is outlined below.

2.1.2   Legislative History

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996 (Public Law 104-196). HIPAA required the Secretary of HHS to develop standards for electronic exchange within 18 months of HIPAA's enactment. It also required Congress to enact some privacy legislation within 36 months. The law required all entities to comply within 24 months. The Secretary of HHS met this deadline, announcing the plan for protecting the privacy of individually identifiable health information. However, Congress did not meet their deadline, leaving the responsibility with the HHS.[10]

On May 7, 1998 the HHS began to write legislation regarding privacy of health information. The first two standards were called the National Provider Identifier and Electronic Transactions. The third standard, National Standard Employer Identifier, was written on June 16, 1998. On July 6, 1998, HHS issued a Notice of Intent proposing the Unique Health Identifier (UHID) in a white paper. Quickly, media and public concerns grew and the UHID paper was given a temporary moratorium. A fourth standard, Security and Electronic Security Standards, was released on August 12, 1998. The final rule was written on August 17, 2000. The final rule for Standards for Electronic

---

[9] Dermdex Corp. Privacy. http://www.dermdex.net/salu/privacy/faq.html, (accessed 13 May 2002).
[10] Legislative history sourced by Joint Healthcare Information Technology Alliance, http://www.jhita.org/ (accessed 13 May 2002).

Transactions established standard data content and formats for submitting electronic claims and other administrative health transactions.[11]

2.1.3   Inside HIPAA

HIPAA mandates several changes to the administration of healthcare:

- Health insurance portability provisions that cover: (1) preexisting condition limitations; (2) prior "creditable coverage"; (3) prior coverage certifications; and (4) health status nondiscrimination issues,
- Access provisions that require health plans and employers: (1) to permit enrollment into a plan upon the loss of prior coverage; and (2) to permit enrollment into a plan upon marriage, birth or adoption,
- Changes to the coverage rules applicable to group health plans under the Consolidated Omnibus Budget Reconciliation Act of 1985 ("COBRA"),
- Language that toughens the law related to fraud and abuse in medical billing, and
- A section that deals with simplification and standardization of administrative procedures in healthcare [12]

The last section, called "Administrative Simplification," is most relevant to our discussion, and will be outlined shortly. The "Administrative Simplification" aspect is contained in Title II, Section F and was an addendum to several original insurance reform proposals. This section opens with:[13]

"**SEC. 1173.** (a) STANDARDS TO ENABLE ELECTRONIC EXCHANGE.--

"(1) IN GENERAL.--The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for--

---

[11] Ibid.

[12] Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191). Aug. 21, 1996. Source: http://aspe.hhs.gov/admnsimp/pl104191.htm, (accessed 13 May 2002).

[13] Ibid., §1173(a)

"(A) the financial and administrative transactions described in paragraph (2); and

"(B) other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

The Administrative Simplification aspect of HIPAA required the HHS to develop standards for the transmission of personal health information that identified individual patients. The required health care standards are: transactions and code sets; privacy; security; and identifiers.[14]

The Administrative Simplification part of HIPAA had two goals. The first was to standardize the exchange of electronic data (for administrative and financial issues) in order to improve the effectiveness and efficiency of the current health care systems, including Medicare and Medicaid. The second goal was to protect the security and confidentiality of personal electronic health information, so as to prevent fraud and abuse. All health care organizations that use electronic data as a means of transmission must comply with these standards. A summarized list of standards is formulated below:

- Electronic Data Interchange (EDI) for Claims/Transaction Administration.
- *Unique Health Identifiers.* The standards will facilitate the creation and adoption of the use of a national identification system for health care providers, health plans, and employers.
- Standardized Code Sets.
- Security.
- Electronic Signatures.
- Transfer of Information among Health Plans.
- Privacy.[15]

---

[14] Ibid.
[15] Ibid.

We are primarily concerned with the Unique Health Identifiers, and their implications for security and privacy. HIPAA legislation required the HHS to be responsible for "a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the health care system."[16]

HHS began to write standards in the Federal Register as required by HIPAA. It released two standards – the National Provider Identifier (NPA) and Electronic Transactions. It followed by releasing the National Standard Employer Identifier and the Notice of Intent (NOI) to write a "white paper" on the Unique Health Identifier. The Unique Health Identifier proposal caused an outcry from privacy advocates and the white paper was put on hold. The privacy issues raised will be discussed thoroughly in §2.3.

2.1.4 The White Paper and UHID

The White Paper was the attempt of the Department of Health and Human Services to deal with the administrative simplifications listed in the HIPAA provisions. More specifically, the White Paper attempted to tackle the issues surrounding the implementation of a Unique Health Identifier (UHID). Most of the report explains several of the candidate identifiers, and possible methods and codes for implementation.

The White Paper begins by describing the current problem in the health care industry involving computer-based electronic health information and how this data is traversed across many institutions. While the paper lists several benefits of the UHID (which will be analyzed in the following section), it also takes the opportunity to address the multitude of privacy issues surrounding it. For example, it acknowledges that having

---

[16] Ibid.

health care organizations use the same identifier will cause a great threat to society because it facilitates unauthorized linkages of information about an individual within and across organizations.[17] The paper also emphasizes that several other organizations including the National Committee on Vital and Health Statistics have expressed negative attitudes towards the idea of implementing a UHID. These attitudes will be examined in §2.3.

Before giving a thorough list of the candidate identifiers, there are some criteria that such candidate identifiers must adhere to. The list of criteria is an exhausting 30-item checklist. The writers of the draft, however, believed that the 30 criteria could be sub-organized to fit the following four functions:

1) Positive identification of patients when clinical care is rendered.
2) Automated linkage of various computer-based records identifier in the population of the United States.
3) Provision of a mechanism to support data security for the protection of privileged clinical information.
4) Use of technology for patient records handling to keep health care operating costs at a minimum.[18]

Above all, the creators of the White Paper believed that there are some basic general concepts that a UHID should follow; among these are practicality and cost effectiveness. These are standard goals of new technological development, and many times it is hard to meet both criteria.

HHS considered six candidates for use as unique health identifiers. These candidates are again divided into four classes: 1) UHID not based on Social Security Number, 2)

---

[17] Unique Health Identifier for Individuals: A White Paper. US Department of Health and Human Services.
[18] Ibid.

UHID based on Social Security Number, 3) Proposals that do not require a UHID, and 4)

hybrid proposals. The six candidates are:

1) Social Security Numbers: popular yet controversial candidate.
2) Biometric identifiers: DNA analysis or voice recognition.
3) Directory service: matching common data elements (birthday, SSN, name, sex) and retrieving data from search.
4) Personal immutable properties: ID number scheme based on birthday, geography, etc.
5) Patient identification system based on existing medical record number and practitioner prefixes: how some hospital currently identify patients.
6) Public Key / Private Key cryptography method: take an existing number (SSN for example) and simply encrypt it.[19]

The Social Security Number (SSN) is currently the best candidate because it matches the criteria for a UHID very well – including the cost effectiveness and practicality. Many healthcare providers currently use SSN to identify patients as it is a very simple method of identification. The HHS believes that only the correct legislation (privacy and confidentiality protections) provided in HIPAA will ease the linkage of health information with institutional databases.

The positive aspects of using the Social Security Number identification are several. Most of these attributes evolve around the fact that this number is already in use and many American citizens know their SSN numbers. This tackles the issue of cost, because there are little infrastructure-based changes involved; i.e. no creation of a new identifier number is needed. Additionally, the ease of implementation can be especially

---

[19] Ibid.

seen in the healthcare industry: these institutions currently use SSN as ways of identifying their users.

Despite the seemingly flawless attributes of the SSN based UHID, the negative aspects of implementation are far lengthier. First, SSNs do not have a "check digital" feature – i.e., there is no process of applying an algorithm to the SSN making it indecipherable.[20] Secondly, many people are not currently eligible for the SSN and it would impose cost and more technology to find these people and identify them. Also, since several people have multiple SSNs – for legitimate and illegitimate uses – issues of double counting arise. Authentication is an important issue and one that is non-trivial to privacy advocates. Since SSNs are so widely used, it would be rather easy for someone to steal someone else's SSN and ultimately steal his or her identity. Finally, there is no current law requiring citizens to provide their SSN for any purpose. Implementing a UHID based on SSN would require some complex additional legislation requiring citizens to hand-over their SSNs to the government.

The White Paper continues to describe all of the candidate identifiers in detail and expresses the positive and negative aspects of each, which go beyond the scope of this research. A brief generalization of the positive and negative aspects of the candidate identifiers will be provided now.

The identifiers that rely on SSN, but not directly, use some algorithm to convert the SSN into another number. This method resolves the authentication issues, but is extremely costly, and since it depends on the SSN, some of the same negative attributes listed above carry over. The UHID proposals that do not use SSN deal with identification

---

[20] Ibid.

by creating a different 16- or 19-bit number for each individual.[21] These proposals are definitely valid because they comply with the HIPAA administrative simplification scheme, but the down side is cost. Creating a new identifying digit, one that is larger than a SSN, will introduce huge infrastructure and implementation costs. These proposals use longer digits to allow for diffraction; i.e., allowing the first 6 digits to be some geographical representation, the next 10 digits to be the actually ID number, and the last 3 digits to be some form of encryption key. These intricate proposals introduce a burden on the heath care industry and some opponents believe it may not be worth the cost of implementation.

One of the proposals, the biometric identifier, may seem too advanced for our time, but trials have already been run in Europe. Smart Cards are personal credit-card sized identifiers that hold a significant amount of personal identifiable information. They can store such personal information as DNA analysis or fingerprints. Researchers in the Netherlands have already tested a system to facilitate passport checking: the passenger puts his finger up to a glass plate, and a camera scans the fingerprinted image; a remote computer compares the retrieved image with a stored image on the smart card.[22] This method of authentication raises several social and legal issues and must be deliberated thoroughly before some type of legislation is enacted.

Clearly, the public has to be in agreement with any candidate identifier that is enacted. The public will need to determine two things: (1) whether the proposed Unique Health Identifier will truly protect electronic medical records and health information; and (2) how invasive would the UHID be to individual privacy.

---

[21] Ibid.

[22] Fancer, Carol. Smart Cards. Scientific American. http://www.sciam.com/0896issue/0896fancher.html (accessed 13 May 2002).

2.2   Proponents of UHID

2.2.1   Overview

Over the past three decades, the healthcare industry, along with the federal government, have tried several ways to handle the outstanding increases in healthcare costs. Strategies have included group insurance plans, subsidized plans, managed care, self-insured funds, wellness programs, and preventative patient education.[23]

Unfortunately, progress has not been made in standardizing the elements of the industry-wide movement towards healthcare transactions automation.[24] Today, health care providers find themselves compounded with several different identifier codes assigned by several different health plans. Sometimes even one health plan may have different identifiers for one individual. Alternatively, the same health identifier may be issued over multiple healthcare platforms.

A Unique Health Identifier for individuals could solve this problem at several levels. One could be to increase the quality of health care services by creating an accurate and rapid identification and compilation of an individual's health records. Health information can be difficult to identify, especially because each organization has its own method of identifying individuals. Similarly, although many of these systems use similar articles to capture identification (e.g. name, sex, SSN), the information is not necessarily recorded in identical ways. UHID would standardize the collection of a patient's

---

[23] Scheur Management Group. http://www.scheur.com/scheur.nsf/smg/newsletterVol2C1.htm (accessed 12 May 2002)
[24] HIPPAdvisory. National Identifier. http://www.hipaadvisory.com/regs/natident.htm (accessed 11 May 2002)

18

identifiable information and would simplify the health care industry's databases, ultimately reducing costs.

Unique Health Identifiers for individuals would also be used to facilitate the synthesis of health information among various health care providers. Having multiple accesses to an individual's historical and other relevant health information can be an important component of quality health care. Therefore, for example, UHIDs may help to better integrate the information on drug allergies and other medications (through historial analysis) and use this new integrated information to help coordinate the medication of patients. This data retrieval would take a matter of seconds, as opposed to lengthy patient queries.

There are additional aspects of health care that could benefit from the use of a UHID for individuals including: 1) fast and reliable payment for aide, 2) longevity of care, 3) prevention and detection of fraud and abuse, and 4) accurate record keeping and data storage.[25] Having several different identifiers for the same person across several organizations stifles quick access to necessary and immediate information. Unique identifiers could facilitate in reporting test results by allowing lab results to be quickly referenced to the right individual. Once a lab test is in the central system, chart updating and maintenance and retrieval of medical records are easily completed.

2.2.2   Computer-based Patient Record Institute

The Computer-based Patient Record Institute (CPRI), established in 1992, is a nonprofit organization whose goals are centered on improving the quality and costs of

---

[25] Gelman, Jon. The Compelling Need for Privacy of Medical Records in the Workplace http://www.gelmans.com/Articles/Privacy11.html. (accessed 10 May 2002).

health care with the use of current information technology. CPRI is a neutral forum that combines the many interest of health care entities in order to form consensus.

The means of developing solutions to benefit computerized health records is through the use of the unique identifier. In 1993, the CPRI published a paper advocating the use of the SSN (with modifications) as a "universal patient identifier".[26] In a paper, the CPRI outlined some possible considerations for adopting the SSN as a potential UHID. The five considerations are confidentiality and security, trusted authority, uniqueness, cost/benefit, and education.

The first consideration involves one of the more important issues circling UHIDs: confidentiality and security. CPRI believes that the only way to deal with this issue is through the use of legislation. Implied in these words is the need for some "privacy protection law, anti-discrimination law, and security authentication procedures to prevent unauthorized access to confidential data".[27]

The second issue deals with the creation of a "trusted authority" to administer the unique health identifier system. Any such group must have the public's trust; similarly, it must consider both private and public interests. The CPRI leveraged their ideas of using the SSN to promote the Social Security Administration (SSA) as the trusted authority. There must be some change in the methods of issuing SSNs, which the SSA will have to determine. Also, the SSA will have to deal with other issues, including possibly having alphabetic characters used in addition to numbers if the SSNs were to grow to capacity.[28] Also, the SSA will have to handle all the problems of SSNs as listed in §2.1.4.

---

[26] CPRI-Host Organization. http://www.cpri-host.org/resource/summit/uhi.html (accessed 13 May 2002)
[27] Ibid.
[28] Ibid.

Uniqueness and costs/benefits are the next two considerations for the CPRI to implement a UHID using social security numbers. These are simple considerations and their issues are similar to the ones established above. The final consideration is education. The CPRI referred to a survey that showed that American citizens have strong support for the use of SSN as a UHID.[29] Although the survey results incline towards using SSN as a unique identifier, CPRI still recommends educating the public on issues about UHID so that they may better understand the protection of personal health information.

2.3   Opponents of UHID

2.3.1   Privacy Concerns

In addition to establishing unique identifiers for patients, HIPAA also required the Secretary of HHS to create a list of recommendations concerning standards with respect to privacy of personal health data. In September 1997, the Secretary announced her recommendations to Congress concerning privacy issues. Since Congress failed to enact any privacy legislation by August 21, 1999, the Secretary became responsible to submit final legislation to protect the privacy of personal health information. The Secretary's recommendations concern the necessity of privacy regulations to be enacted whenever the UHID for individuals is implemented.

Currently, there exists very little federal legislation for the protection of privacy of health information. Generally, these issues are protected under state law, with each state setting its own set of standards. As noted in the Secretary's recommendation to

---

[29] A strong majority of leaders (72%) and the public (67%) favors using the SSN as their health care identification card. Source: Ibid.

Congress[30], state laws greatly vary in their scope and meaning. Thus, those laws cannot be generalized to fit with privacy laws across all states. As a result, the confidentiality and privacy of individual identity may be jeopardized by interstate movement. It is because of this flow of health data that many privacy advocates believe there is a strong need for a uniform national privacy standard.

The National Committee on Vital Health and Statistics (NCVHS), an advisory committee to help the HHS develop health policy, has recommended that using a UHID for health data without proper health privacy legislation to ensure the privacy of personal health information will be a poor decision and will lead to great concerns amongst the public. The NCVHS's conclusions were as follows:

- The selection of a unique health identifier for individuals will become the focus of tremendous public attention and interest, far beyond that afforded to other health privacy decisions. No choice should be made without more public notice, hearings and comment.
- Until new Federal privacy law adequately protects health record privacy, it is not possible to make a sufficiently informed choice about an identification number or procedure. The degree of formal legal protection in such a law will have a major influence on both the decision itself and the public acceptance of that decision. Passage of a comprehensive health privacy law may make the choice of an identifier easier and less threatening to privacy.
- A unique health identifier for individuals could not be protected from misuses under current law, notwithstanding the criminal penalties enacted in HIPAA.[31]

---

[30] Privacy Standards: Issues in HHS Proposed Rule on Confidentiality of Personal Health Information. Department of Health and Human Services. April 26, 2000.
[31] Unique Health Identifier for Individuals: A White Paper. US Department of Health and Human Services.

There has been additional concern about giving the government a great deal of strength by allowing it to issue out UHIDs. There is uncertainty of what may happen when the government has such a power over individuals. History has shown that federal attempts to preserve the confidentiality and privacy of information are not effective at shielding its citizens from the prying eyes of government entities. There have been many cases of IRS abuse and misuse of FBI files. Moreover, there was a case of a Medicaid worker who had access to a health database on the computer and had sold patient information to an HMO.[32] How can such fraud be prevented? This indicates that the only way to protect privacy may be to prohibit the government from issuing UHIDs.

Patient and physicians have shared a common relationship, one that has developed over many years and has privacy as one of its main foundations. One negative effect of the implementation of a unique identifier to individuals is the break of the patient-physician relationship. In a case in the US Supreme Court, Jafee V. Redmond, the Court noted that: "Reason tells us that psychotherapists and patients share a unique relationship, in which the ability to communicate freely without the fear of public disclosure is the key to successful treatment".[33] The Court further noted that no patient should be required to agree to the release of any personal health information protected by the therapist, either as a condition for receiving such treatment or as a precondition to insurance coverage of treatment that falls within the privilege[34]. The problem with UHID in this scenario is that there exists no current prohibitions that allow a doctor from giving a patient's UHID to another institution, whether it be an HMOs or a research institute. This is a major source

[32] Statement of Rep. Ron Paul (R-Texas). http://www.house.gov/paul/privacy/statementprivpro.htm (accessed 14 May 2002)
[33] Jaffee v. Redmond (95-266), 518 U.S. 1 (1996)
[34] *American Psychoanalytic Association*, September 7, 1999.

of concern, and patients may find it difficult to trust their physicians. A 1994 American Civil Liberties Union poll found that nearly 70% of patients are concerned a "great deal" about health insurance companies getting more information about them than is needed from their doctors.[35] The UHID proposal will not do anything to calm this fear that health information will be shared across unwanted boundaries. A UHID may be shared from one doctor to another, and thus private information may ultimately exist in several locations, many of which are undesirable to the patient. *Privacy is the right of the patient*. When an individual's right to privacy is in conflict with external needs, such as research institutions or other administrative issues, the scenario must be carefully analyzed in order to strike a fair balance between social and individual needs. This is very important because patients have a right to know who has access to their identity. The next section will discuss another federal attempt at creating a national identifier database.

2.3.2   Case Study of a National Identifier

The implementation of UHID is not the first time that the government has tried to create some form of a national identifier database. In the fall of 1996, President Clinton signed the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIR) of 1996. The law is designed to prevent illegal immigrants from obtaining employment. It requires the Justice Department to create three pilot programs to control illegal immigration using the following two steps: 1) the federal government must make a list of authorized to workers in the United States, and 2) it must somehow prevent anyone who is not on that list from being employed in the United States.[36]

---

[35] American Civil Liberties Union. "Live and Let Live," 1994.
[36] Sutherland, Daniel. Big Brother Flunks a Test: Monitoring the National ID Program. September 1997.

In "basic pilot programs" the government observed several problems when creating a list. They did not account for the fact that some cultures, Chinese for example, use the surname first then followed by the personal name. This causes the database to not recognize an individual simply because their name was reversed. Most of the time, officials who entered in their employee data, had made typographical errors. If an employee name does not turn out on the list, that employee can contest a non-confirmation. This has often been the case in pilot test and it is found that an error is detected 25% of the time.

Two other pilot programs were created, but the third program is what mostly resembles a National ID. The third pilot program is called the "machine-readable-document pilot program." The program forces all new employees to present ID cards that contain their Social Security Number and can be swiped into an electronic card-reader. In a test run, the Social Security Administration's database of wage reports was flooded with mistakes and an attempt to correct these errors resulted in 100,000 corrections in one year out of a possible 200 million unmatched wage repots.[37] The problems with these databases were related to the issues presented above.

Lack of security in computer systems is another issue that was raised in response to a national ID database. In April 1997, Congress forced the SSA to end its new on-line system, reporting that an intruder would only need to know a person's name, SSN, birthday, and mother's maiden name in order to get through the system. These entities are easily available from other sources and it created a major privacy issue for the government. The SSA had admitted that its security infrastructure may not withstand hacking from intruders.

---

[37] Ibid.

Proponents of the IIRIR argued that the government already collects a multitude of individual personal information. However, this new database would be strikingly unique in many respects. First, the program needs to link two large government databases: an unprecedented move. It will link the INS database (for immigrant authorization) and SSA database (for social security purposes). Now, for the first time, there is a large linked database including everyone who has permission to be in this country.

Another way the collected information is unique is that it must create a new database. The SSA will simply need to collect more data, and it must also include certain people who are not included in SSA's database (including some farmworkers, ministers, student nurses or delivery boys, for example). The SSA will also have to delete data – it was noted that "about 210 million [Social Security] numbers are considered active, according to SSA, and at least 75 percent were issued without proof of the individual's identity or citizenship."[38] A federal commission in the 1970s warned, "The real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[39]

Sponsors of the IIRIR, Sen. Alan Simpson (R-Wyo., ret.) and Rep. Lamar Smith (R-Texas), assured politicians that the end result of the law would not create a "national ID card." However, throughout several sections of the law, it is noted that the IIRIR demands the creation of some type of ID card. Terms like "development of prototype of counterfeit-resistant Social Security card" (section 657), "improvement in border crossing

---

[38] General Accounting Office, Immigration Reform: A New Role for the Social Security Card. 1988.
[39] Privacy Protection Study Commission, Personal Privacy in an Information Society, 1977. Quoted in the Tarnished Golden Door: Civil Rights Issues in Immigration, A Report of the United States Commission on Civil Rights, 1980.

identification card . . . biometric card . . . machine-readable" (section 104), and "improvements in identification-related documents" (section 656) which mandates driver's licenses to be machine-readable and contain a SSN. The vision is clear: to create a new electronic database, so that all employees will have an ID number that is fraud-proof through the means of biometrics identifiers (as explained in the White Paper).

It is clear that whenever the government is in access of important information, abuses are inevitable. As Robert Holland, a columnist with the Richmond Times-Dispatch notes, "Information is power – the power to harass, snoop, embarrass, fabricate, bully, even jail for political reasons. It is dangerous to put such all-inclusive informational power in the hands of government – no matter how much more 'efficient' immigration or other policy might become."[40] It is because of all the reasons mentioned above that the IIRIR's mandates for a national database were repealed in 1999.

The repealed IIRIR proposal draws parallels to the unique health identifier, in that both ultimately require the creation of some national database. The UHID would create a database linking patients to ID numbers – possibly through the use of SSNs. This large database will be unique in the similar manner as IIRIR's proposed database – and thus many of the problems involving the IIRIR's database will be inevitable.

---

[40] Holland, Robert, "Government Tracking Imperils Liberty," <u>Richmond Times Dispatch</u>, Aug. 23, 1995.

Confidentiality is the cornerstone of quality health care. All the legal and moral issues, developed in order to establish this confidentiality, are the burden of the health care providers themselves, to promote absolute disclosure from the patient. The basis for this burden is based on the notion that an individual patient, who believes that all communication will be held to confidence, will be willing to ask for treatment and completely disclose all necessary health information, so as to allow that health care provider to more accurately and effectively diagnose and care for the patient. Without complete disclose of all the relevant vital information, health care quality is harmed.

As society moves into a time of electronic ingenuity, privacy and confidentiality must not be sacrificed. It is apparent that serious problems existed with the unique health identifier causing the pause in legislation. The current train of thought in legislation is to create some type of national identifier to link a great deal of data on citizens. This is not the solution to the problem of medical records because it is placing individual privacy at risk. Unique Health Identifiers cause a great deal of controversy and privacy groups will not consent until a better solution is found.

PART III: THE PERSONAL INTERNETWORKED NOTARY AND GUARDIAN

The Personal Internetworked Notary and Guardian (PING) aims to be a next-generation software package to manage medical record data. It is being developed at Children's Hospital Informatics Program[41] under a grant from the National Library of Medicine[42] and with support from the Clinical Decision Group of MIT's Laboratory for Computer Science.[43]

3.1 Design objectives and obstacles

The main goal of PING is to create a patient-controlled electronic medical record. This is an inversion of the traditional medical record, which is in the current system controlled and administered by health-care institutions. Even though legally patients currently own their own medical record, it is often very difficult for patients to retrieve their records in a timely and consistent manner. In the PING paradigm, the patient controls her own record, and grants access privileges to other parties, such as physicians, health-care institutions, or government agencies. PING should allow seamless access to nomadic users, yet maintain the privacy of medical data and security of the over-all system.[44]

Medical records are unique from many other forms of records, because they are potentially important for a person's entire lifetime. Thus, any medical records system needs to guarantee the longevity and durability of medical records for several decades, if

---

[41] Children's Hospital Informatics Program, http://www.chip.org/, accessed 15 May 2002.

[42] Next Generation Internet Initiative, Phase II. Contract N01-LM-9-3536

[43] There is not much published literature on PING, since it is a system in development, so much of the information contained here comes from personal communication with the research team working on PING: Eric Pan, Alberto Riva, and Isaac Kohane.

[44] Mandl KD, Szolovits P, Kohane IS. Public standards and patient control: how to keep electronic medical records accessible but private. BMJ 322 (2001): 283-7.

not longer. Furthermore, the system needs to be flexible enough to adapt to the technological changes that will come about with the passage of time, to allow retrieval of medical records many years from now. The system should also be highly scalable because almost everyone in the developed world will need to store their electronic medical records in the near future.

PING should be built to public standards and be open source. This accomplishes several goals: it increases the likelihood of the longevity of the medical record, encourages the interoperability of different record systems, and increases over-all patient confidence in the system. PING is not designed to compete with existing institutional medical information and record-keeping systems. Hospitals and physicians will continue to keep their own records, if only for their own legal protection. Rather, the objective of PING is to serve as a patient-controlled horizontal integration of medical records across different institutions. Thus, a key design hurdle is the integration and communication between PING and the co-existing institutional record system. This is facilitated by conforming to existing public standards on data communication and exchange.

3.2 System architecture – a bird's eye view

The basic architecture of PING consists of *databases* that store the PING record, a *server* that controls access to the record, and various *agents* that manipulate the record through the PING server. This interaction is diagrammed schematically in Figure 1.
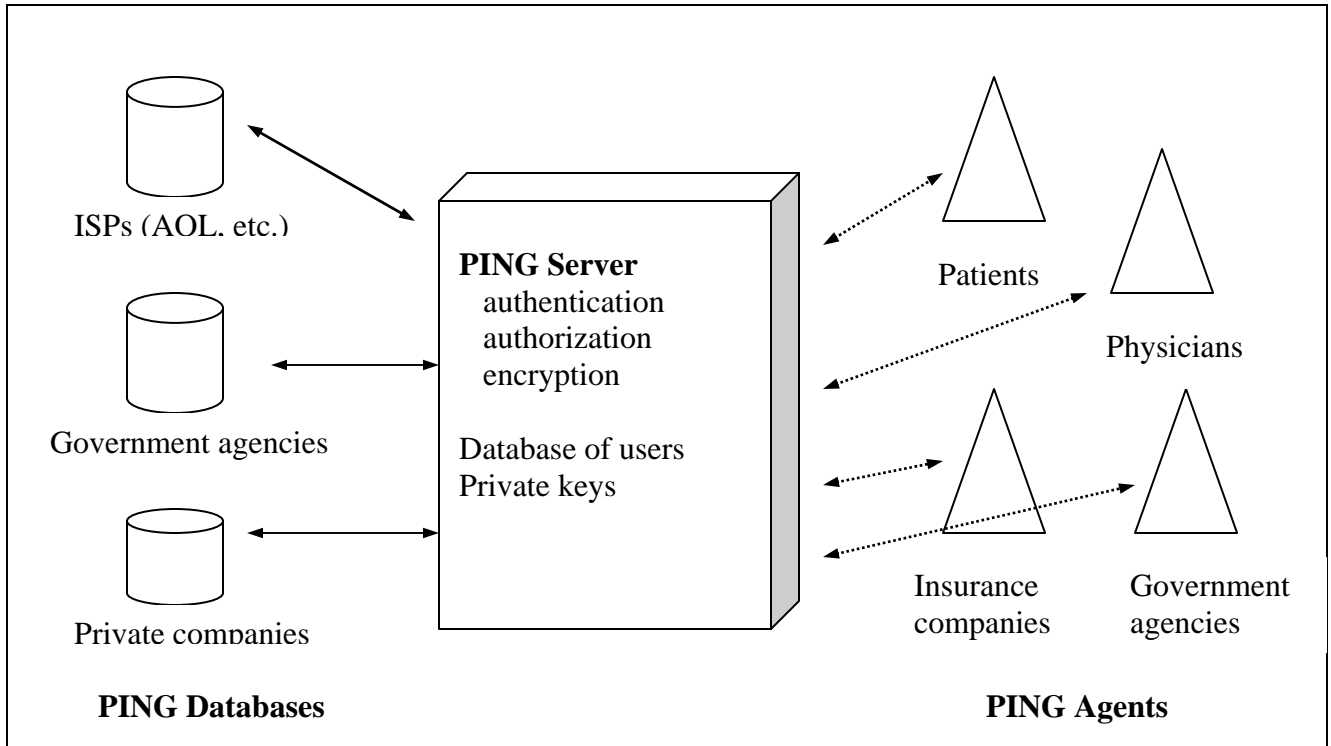
Figure 3.1 PING Architecture

The key feature to observe is that the databases where the data is actually stored can be any number of data providers, including traditional ISPs. There is no assumption about the capabilities or security of these databases. In fact, the databases are accessible to all, and the communication links between them and the PING server are not secure. The only requirement on the PING database is that they support the HTTP protocol, and the HTTP `put` command. This means that any existing web-server can function as a PING database. Thus, users have a choice among many existing web services to hold their medical record, and can easily migrate or mirror their records on multiple servers.

The PING server is responsible for encrypting the PING record using an internal secret key before placing it in the PING database. It is also responsible for authorizing and authenticating the agents that desire access to the record. The communications

31

channels between the server and the agents are secure and authenticated using public key certificates. Thus, all security vulnerabilities are concentrated in the PING server, making the system easier to defend against attacks.

The function of the agents is to manipulate the data contained in the PING record through the server. An agent can be autonomous, or it may represent a human user. In many scenarios, the agents would be software applications tailored to specific tasks or contexts. The agents authenticate themselves with the server before access privileges are given, and their privileges are constrained by the task or context they are designed for. For example, an application used to display laboratory results would only have read privileges to the laboratory section of a person's PING record.

The PING server provides five atomic operations to manipulate the record: Create, Delete, Read, Modify, and Annotate. It is the task of the agent applications to combine these primitive operations into more elaborate tasks.

The current implementation of the PING server is written in the JAVA programming language, and all communication occurs over the internet's pre-existing HTTP protocol. This means that the server code can run on any machine that supports Sun's JAVA virtual machine, which is now supported by almost all computer vendors. In addition, the only requirement on the client machines is that they support JAVA-enabled web browsers, which frees the users from special-purpose client software.

3.3 File system and data representation

A PING record consists of a virtual directory tree of PING objects. A PING object may contain data or represent a directory. All PING objects are encoded in plain
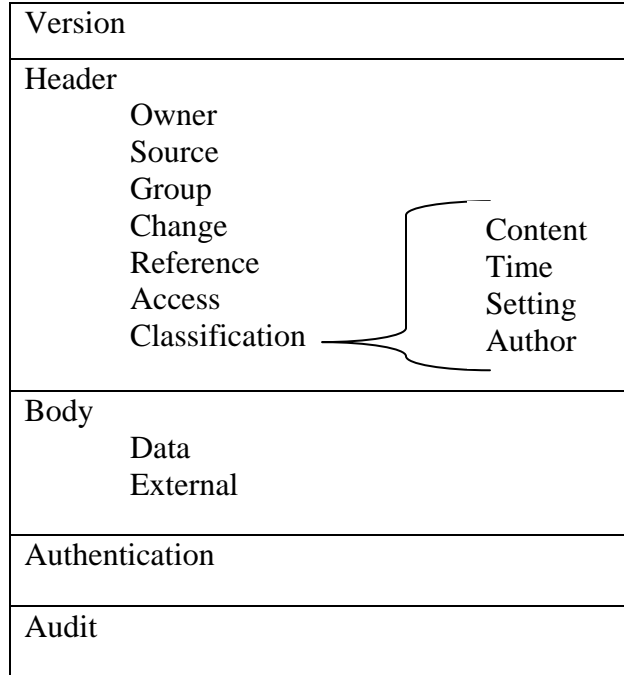
ASCII, XML structured text. This has several advantages because XML is a public standard for representing structured text. There are a large number of versatile, open-source XML parsers available free of charge, and "they are generally fast and reliable, and produce as output a tree-like data structure that lends itself well to subsequent automatic processing."[45] Furthermore, all browsers now support the XML file format, and support is likely to evolve over time, ensuring the longevity of the records. Finally, XML files are human-readable, which has two main advantages. In the event of PING server failure, the files themselves may be read by a human being. Though this process would be very tedious, it does mean that the data would still be accessible. And the fast-paced evolution of information technologies will very likely support XML, and in the even they do not, the files can be read by a human many years from now.

The clinical document data model is shown in Figure 3.2. Notice how every PING object has an authentication section that signs the legitimacy of the document, and proves that the document was not tampered with. The author's digital signature provides for the integrity and non-repudiation of the record. In addition, every PING object has an audit trail that records when the record was accessed, what modifications if any where made, and by whom. This is a crucial aspect of the PING system, and it will be discussed in more detail below.

---

[45] Mandl KD, Riva A, Kohane IS. A distributed, secure file system for personal medical records. Proceedings AMIA Symposium 2000, pg. 1075.

```
┌─────────────────────────────────────────┐
│ Version                                 │
├─────────────────────────────────────────┤
│ Header                                  │
│         Owner                           │
│         Source                          │
│         Group                           │
│         Change            Content       │
│         Reference         Time          │
│         Access            Setting       │
│         Classification    Author        │
├─────────────────────────────────────────┤
│ Body                                    │
│         Data                            │
│         External                        │
├─────────────────────────────────────────┤
│ Authentication                          │
├─────────────────────────────────────────┤
│ Audit                                   │
└─────────────────────────────────────────┘
```

Figure 3.2 Clinical document data model.[46]

An example of a PING object is shown in Figure 3.3. Every PING object contains a header and a body part. The header contains the most important indexing information, such as author, access and modification history, and access rights. The body contains either text data or else a pointer to binary data, such as a radiology image or an ECG. Since the header and body form two separate parts of the XML file, they may be separated during processing for more efficient search, sorting, and management. Thus, for example, the PING server does not need to download the whole PING body in order to determine whether a given agent can access the file, since that information is contained in the header. Furthermore, this allows the ability to easily create redundant mirrors of the record by simply including multiple pointers to the data.

---

[46] Eric Pan, personal communication, 30 April 2002.

```
<Ping-object name="Example">
  <Header>
    <Author alias="agent1" />
    <Creation-date time="944003712498" />
    <Privileges>
      <Privilege role="owner" read="t" annotate="t" delete="f" />
      <Privilege role="author" read="t" modify="t" />
      <Privilege role="other" read="t" />
    </Privileges>
  </Header>
  <Data type="text/xml" url="data1.xml">
  </Data>
</Ping-object>
```

Figure 3.3 A sample PING object representation in XML[47]

PING objects are encrypted, and stored in the PING databases. The directory structure in the database has no correlation to the virtual directory structure of the PING record. The database directory structure is either completely flat, or else to improve storage and search efficiency, is a randomly generated tree with random directory names. This is important because the virtual tree structure itself may contain sensitive information. An example would be a directory entitled "psychiatric records," or "STD test results."

It is important to note that the *owner* and *author* of a given PING object may be different people, and may not have the same access privileges. For example, the owner of a record (the patient) may not have the right to modify or delete it if another author (the physician) created it. (The patient may have the right to annotate the record only – that is, to add her own comments.) This is an important feature for medical records for both medical integrity and legal liability.

---

[47] A. Riva, et.al., The Personal Internetworked Notary and Guardian. Int. J. Med. Inform. 62 (2001): 27-40.

3.4 Privacy and security

The role of the PING server is to provide for privacy and security of the PING record, while simultaneously granting access privileges to authorized parties. Since the system does not rely on any security features of the databases, it is the server's job to authorize and authenticate agents, and to manage the encryption and decryption of the record for storage in the databases.

3.4.1 <u>Encryption</u>

The PING server maintains a database of all users of the PING system. This database includes basic contact information about the user, such as name, address, electronic mail, and phone number. It also contains the username and password for the user, as well as the secret key used to encrypt the data. "The encryption algorithm is not fixed – it can be specified in the server configuration file. Currently, the systems uses a symmetric-key encryption algorithm called RC4 (RC4/CFB/PKCS#7), but it can be anything that can be passed to the Cipher.getInstance() method in the java.security package. The key is generated by the KeyGenerator class using the same algorithm used for encryption. The default key length is 128 bits, but it can be set anywhere up to 1024."[48] The key never has to leave the PING server because all encryption and decryption takes place inside the server. This architecture allows the system to periodically re-encrypt the entire PING record with a new, longer key whenever the passage of time brings with it better encryption technologies.

Because the PING system does not rely on any security measures of the database computers, the entire security of PING rests on the encryption protocol. Since this is a

---

[48] Alberto Riva, personal communication, 15 May 2002.

crucial possible security threat, it is worth expounding on this at some length. There are several issues that can be raised here, but there exist a satisfactory technical solutions to all of them. Firstly, a potential attacker has access to the source code of the server, since the project is open-source, and furthermore she has total knowledge about the precise document type definition of the PING object. All PING objects have a very precise structure since they must conform to XML standards and to the PING object standards. For example, all PING objects begin with the text "<Ping-object> <Header>" (see Figure 2). Therefore, an adversary would have a lot of knowledge with which to mount a "known plain-text attack." Secondly, a single key is used to encrypt all of the files for a given user. This means that the adversary has access to many different encrypted files, all of which are based on a common template. This means that an adversary can use the known plain-text header information of many different files to crack the secret private key of the server. She could then use this key to decrypt all of the PING files that belong to that user. Using a different key for each file is impractical, because of the key management problems this would raise, and scrambling the order of the lines in the file before encryption would not solve the problem because the lines themselves would still follow the same template.

Fortunately, there exist several well-known encryption techniques for precisely this scenario of encrypting multiple files with similar structure with the same key. One common method used is called "cipher-block chain mode," and it provides a solution to this security issue in PING[49], so it worth describing here. Examples of cipher-block encryption algorithms include RC5 and AES (Advanced Encryption Standard). They

---

[49] Personal conversation with Ronald Rivest, MIT Prof. of Electrical Engineering and Computer Science, 13 May 2002.

contrast with stream ciphers, like RC4, in that an entire block of the message is encrypted at a time.[50] "No block cipher is ideally suited for all applications, even one offering a high level of security. This is a result of inevitable tradeoffs required in practical applications, including those arising from, for example, speed requirements and memory limitations, constrains imposed by implementation platforms, and differing tolerances of applications to properties of various modes of operation."[51] However, NIST and the Commerce Department have recently approved AES as the encryption standard for all government agencies, and it is believed to be secure for 20-30 years[52]. Furthermore, the JAVA 2 SDK v1.4 provides support for the AES standard as part of the JAVA Cryptography Extension (JCE).[53] From among the popular encryption technologies, AES is the most appropriate to use in this context.

A cipher-block, chain-mode encryption algorithm works as follows. Let the key length be 128-bits, and break up the message M into 128-bit blocks M_i. First, generate a random 128-bit string, and call it M_0. Let C_i be the encrypted version of M_i, then $C_0 = f(M_0, key)$, and $C_i = f(C_{i-1} \textbf{ xor } M_i, key)$, where $f(x, key)$ is an encryption function, such as DES3 or AES. That is, to encrypt the ith block, first xor the ith message block with the i-1st encrypted block, and then encrypt the result. Since M_0 is randomly chosen, even two identical messages encrypted with this technique will look totally different. This technique solves the problem of allowing multiple files with the same general structure,

---

[50] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of applied cryptography, 5 ed. Waterloo: CRC Press, 2001. Available at http://www.cacr.math.uwaterloo.ca/hac/ (accessed 15 May 2002).
[51] Ibid., p. 223
[52] The National Institute of Standards and Technology (NIST) approved the Federal Information Processing Standard (FIPS) for the Advanced Encryption Standard, FIPS-197, in October 2000, to be effective starting May 26, 2002. Source: Federal Register, vol. 66: 235 (December 6, 2001), pp. 63,369-71. See http://csrc.nist.gov/encryption/aes/ for information about the standard (accessed 15 May 2002).
[53] See JAVA 2 SDK, Standard Edition Documentation, available at http://java.sun.com/j2se/1.4/docs/ (accessed 16 May 2002).

and encrypted with the same key, being accessible to the adversary. In this context, a key length of 128-bits using this method is essentially unbreakable using current technology.[54]

3.4.2 Authentication

The first task of the PING server upon receiving a request from an agent is authentication – "determining the identity of the agent with the highest degree of certainty"[55]. There are many widely used solutions to this problem. In the current implementation, PING uses a straight-forward username/password scheme, which was easy to implement, but offers very limited security. In future iterations, possible authentication schemes include "cryptographic identifiers, hardware tokens, or biometric devices, such as fingerprint readers."[56]

PING is flexible in allowing multiple forms of authentication to be used. Depending on the level of security provided by a certain authentication protocol, PING may grant more or less privileges to the agent. As technology progresses, and more sophisticated and secure authentication schemes come into common use, PING will be able to seamlessly integrate it into the architecture.

3.4.3 Authorization

The goal of authorization is to determine whether a requested operation by a given agent is allowed by the patient. The authorization procedure is described by Mandl, et. al. as follows:

---

[54] Ron Rivest, personal communication, 15 May 2002.
[55] Mandl, et.al., supra note 44
[56] Ibid.

An agent A sends to the PING server a request to perform the operation C on an object O, along with the credentials necessary to prove its identity. After verifying the credentials, the PING server determines the set R_A of roles that are associated with agent A. It then reads the privilege information contained in the header of O and determines the set R_O of roles for which operation C is allowed. The authorization to perform C is granted if R_O contains *Other*, or if the intersection between R_A and R_O is not empty.[57]

This role-based authorization procedure is flexible because it allows multiple people to fill a given role, and it allows a single person to hold multiple different roles. For example, the role of "primary-care physician" may be fulfilled by Dr. Adam, but when the patient moves to another city, it may be fulfilled by Dr. Bill. The only change required would be removing Dr. Adam from the list of people who fulfill the "physician" role, and adding Dr. Bill. In another context, a group of people that share a common role may have access to a patient's record. For example, the role of "emergency room personnel" may be fulfilled by any number of nurses, doctors, etc. when a patient is admitted into an emergency room. This also allows for the over-ridding of general patient privacy in an emergency situation.

3.4.4 Audit

Audit trails are an important part of the medical record. In traditional paper records, changes or deletions from the medical record are generally not allowed. Instead, only additions are allowed. Changes must be recorded as additions, as this clearly marks the time of change and who made it. PING implements a similar audit trail with each

---

[57] Ibid.

PING object. Thus, as a default setting, PING objects can not be deleted (the *delete* tag in the header is marked *f* by default). Whenever a PING object is changed, the previous version of the object is saved onto a stack that represents the audit trail of that object. Thus, as seen in Figure 3.2, every PING object has an audit appended to it.

The audit is important both for medical and legal reasons. Medically, it is important for physicians to know when lab results changed, for example, and what the old lab result was. Legally, it is important to know accurately the information that was available to a given physician at a given time, in suits of negligence or malpractice.

3.4.5 Dealing with system attacks

Attacks on a system may take many different forms, depending on the motivation, resources, initial access, and technical capability of the attacker. Attacks on a system can range from a malicious employer snooping at her neighbor's medical record to organized crime attempting to blackmail a powerful individual. Clayton et. al.[58] provide a taxonomy of possible system attacks, organized by levels one through five, representing increasing levels of sophistication:

1) Insiders who make innocent mistakes and cause accidental disclosures
2) Insiders who abuse their record access privileges
3) Insiders who knowingly access information for spite or for profit
4) The unauthorized physical intruder
5) Outsiders who mount attacks to access unauthorized information, damage systems, and disrupt operations

---

[58] Clayton PD, Boebert WE, and Defriese GH, et al., eds. Computer Science and Telecommunications Board, National Research Council. For the record: Protecting electronic health information. Washington, DC: National Academy Press, 1997, pp. 54-65.

Clearly, the fourth and fifth class of attacks are the most difficult to organize, but they are also potentially the most devastating. However, good technical measures can be implemented to make these classes of attacks more challenging. The architecture of PING concentrates all of the security vulnerabilities in the PING server, which means that all of the energy to protect PING can be concentrated in a single locale. Thus, a bank may chose to operate a PING server as part of their package of financial services. In addition to providing a vault for their client's money, a bank can put the PING server into a highly secure physical vault, thus making the burden to a physical intruder (attack class four) extremely high. This type of security is not possible with traditional medical records that are stored in hospital information systems, since it is not practical for a hospital to maintain that level of security.

Good encryption standards are essential to defend against an attack of class five. Section 3.4.1 describes how a cipher-block chain-mode encryption scheme based on the new Advanced Encryption Standard is believed to be secure for the next 20 to 30 years. Furthermore, it is relatively easy to re-encrypt the entire PING record with a new algorithm or standard in the future, as encryption technologies progress.

Dealing with insider attacks that fall into classes one, two, and three are more challenging, and require organization, in addition to technical, approaches. Threat one can be the most difficult to prevent, but good education programs on information security and privacy policies to new users of technologies can go a long way. This threat is endemic to all information technologies, and is in no way unique to PING. "Threat one can best be countered by organizational mechanisms that detect and defer abuses. Simple procedural measures appear to be most appropriate – for example, reminders about

behavioral codes, confirmation of actions that might route or access information erroneously, or screen savers and automatic log-outs to prevent access to unattended displays."[59]

The best way to protect against threat two is deterrence: "appeals to ethics, education about what constitutes fair practice, and the imposition of sanctions after an incident occurs. Technology can also play a role in controlling inappropriate access to patient information. Strong user authentication, based on cryptographic techniques, can effectively control the extent that system users protect their identifying data and make appropriate use of the information they are authorized to access. The use of encryption can place significant obstacles in the way of potential abusers, requiring them to obtain special data (keys) to make patient information legible. Properly analyzed audit records of accesses are another powerful tool to deter abuse."[60] PING has all of these mechanisms in place, as discussed in §3.4.1 (encryption), §3.4.2 (authentication), and §3.4.4 (audit).

Finally, "a combination of obstacles and deterrence is necessary to counter threat three. These include reasonable obstacles to prevent unauthorized access without interfering with authorized use and the deterrence steps used against threat two. Audit trails are particularly effective at deterring this type of threat."[61] As this section demonstrates, PING successfully implements each of these deterrence measures.

---

[59] Clayton, et.al., supra note 57, p. 62
[60] Ibid.
[61] Ibid.

3.5 Integration and interface with existing health-care systems

It is important to observe that PING does not compete with existing institutional record systems. Rather, it is meant to serve as a patient-controlled, horizontally-integrated record complement to existing record systems. In particular, this means that hospitals, physicians, insurance companies, and other parties will continue to keep the records that they need to run their enterprises smoothly. These organizations will maintain their own records, rather than rely entirely on PING, both for medical safety and legal liability.

PING will act as a "sponge" to soak up records collected by health-care institutions. This requires a communications interface between the hospital record system and PING. This is facilitated by the fact that PING uses public communications protocols (HTTP), and conforms to widely used data standards (XML). PING is designed to work with ISO's Health Level 7 (HL7) and X12 standards. HL7 "provides a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports the clinical practice and the management, delivery, and evaluation of health services."[62] There exists an XML DTD for HL7, which means that the XML parsers can readily check PING objects for validity. Furthermore, compliance with the "HL7 DTD guarantees compatibility with future HL7-enabled systems, as well as with many legacy systems."[63]

In order for PING to successfully interface with existing informatics systems, the hospitals must clearly provide access to their systems to PING. A PING agent must become a trusted part of the hospital record system, access the desired patient record, and

---

[62] Health Level 7, http://www.hl7.org/, accessed 7 April 2002.
[63] Mandl, et.al., supra note 44

send it to the PING server for storage. This is the job of the PING *Puller* agent, and its operation within the PING system is diagramed in figure 3.4.
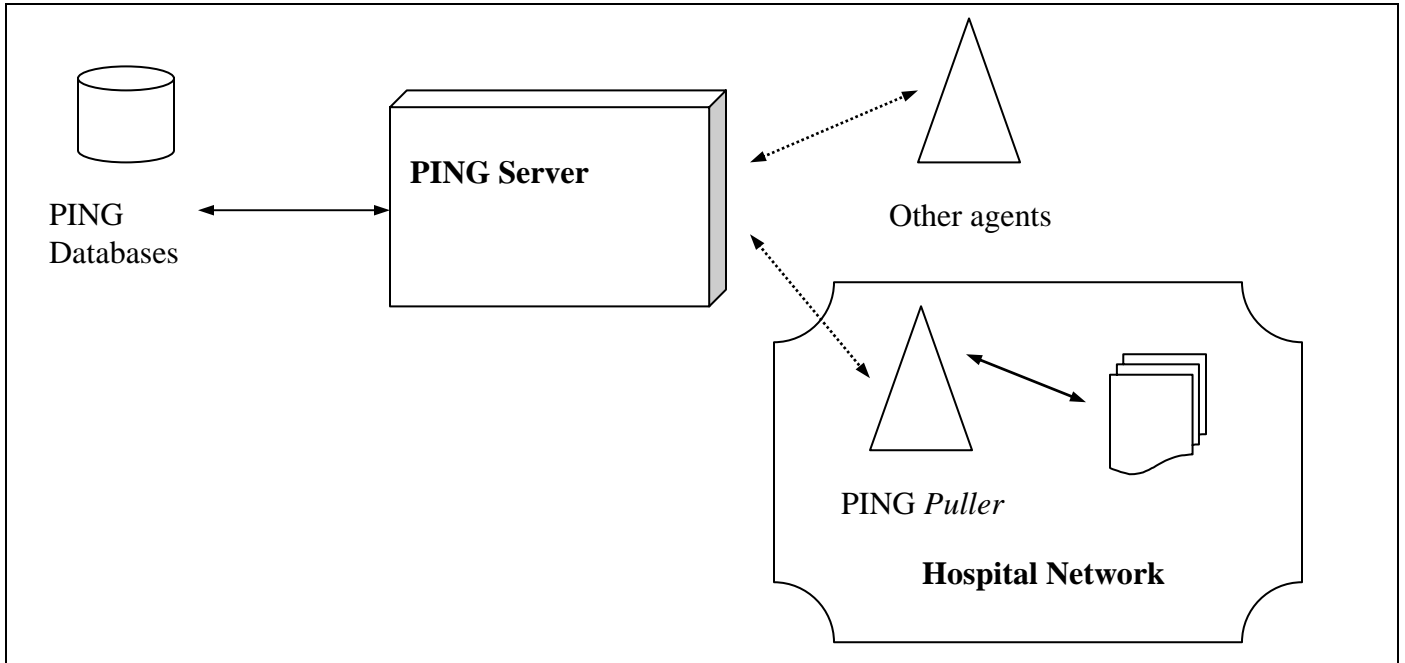
Figure 3.4 PING *Puller* Agent

Currently, there are a few administrative hurdles towards the implementation of the architecture diagramed in figure 3.4, since it requires the collaboration and consent of the hospital. Although a patient is the legal "owner" of his record, the hospital – as the guardian of the patient's record – has many legal responsibilities related to the data. These responsibilities include maintaining the record for a minimum number of years, preventing unauthorized access, and allowing the patient to retrieve his records. However, the current system is not setup to make patient retrieval of their own record easy or fast. Most hospitals as a matter of policy will not provide an electronic copy of a patient's record, even if it is available. Usually what the patient receives is a very high

mountain of papers that represent his paper record.[64] It would be a big challenge to enter this data into PING.

Until the PING system becomes ubiquitous enough for hospitals to trust the PING Puller agents in their networks, or else legislation forces hospitals to provide electronic records to patients, another solution to the problem of integration is available. The task of the PING *Fax* application is to translate the analogue paper record into a digital PING record. This is accomplished by scanning the paper record and storing the digital images in TIFF format, together with indexing and audit information.[65] The task of automatically recognizing and parsing the paper record intelligently by machine is too complicated to have a solution even on the horizon. This is far from the ideal solution to the integration problem, but it provides a workable resolution until the administrative hurdles are surmounted.

3.6 Medical and public health research

Sometimes, the interests of society must outweigh the privacy concerns of individuals. Such cases are common in medical and public health research, where access to patient records is crucial for research that has many long-term social benefits. Thus it is crucial that PING provide for secure mechanisms by which such research can be conducted. The PING architecture provides for this scenario, by providing access to authorized researchers, while simultaneously protecting the anonymity of patients. In fact, under the PING system, researchers would have access to a richer, more integrated patient record, and would have simpler access to many more patients than under the

---

[64] Personal conversation with Eric Pan, 30 April 2002.
[65] Eric Pan, personal communication, 16 May 2002.

current system. "The PING *Poller* agent is able to access the PING records of a group of patients, and to create a relational view of a subset of their data, possibly in anonymized form." [66]

The PING Poller broadcasts a series of queries to a specified population of PING records. "The PING Poller then dynamically builds a relational database using the results returned by the PING Server. Each user can specify those queries to which they will respond, and the subset of their data they want to make visible."[67]

The PING system allows for greater and finer patient control and input in how their medical data is used for research purposes. For example, a cancer patient may specify that his data can be used by the National Cancer Foundation for research funded by the government, but that his record can not be used by research done by pharmaceutical companies. Or he may specify that only those parts of the medical record related to his cancer may be released to researchers, while maintaining the privacy of other parts of his record. This is a much finer level of control than is possible under the current system, and will likely make both privacy-conscious citizens and medical researchers happy.

3.7 Current prototypes

There are two major prototypes currently installed testing the operation of PING. The information learned from these prototypes will guide improvements to the next version of the PING server. The first prototype is an application to report to parents their children's strep throat test results after being admitted to Children's Hospital Emergency

---

[66] Mandl, et.al., supra note 44
[67] Riva, et.al., supra note 46

Department for soar throat. This test requires a laboratory analysis, and usually requires 48-72 hours; traditionally, the test results are telephoned to the parents by a nurse. In this PING implementation, the parents are given a brochure that instructs them how to retrieve their child's strep throat results online; their child's patient number is the username, and a password is given in the brochure. The parents can check their child's results online, learn about what needs to be done given the test outcomes, as well as request an electronic prescription for antibiotics if their test result is positive. The physician and nurse can examine their patients test results in a single screen, as well as if the parents have checked their results; the nurse will call the parents by phone if they have not checked their own results within 24 hours.

All patient interaction with PING was logged: "every login attempt, and every linkage in the throat application is logged with the user-id and time" of access. Eric Pan[68] reports that "there is a lot of interest from patients. [But] we are finding our paper and human instructions need to improve. For example, patients had not been fully aware that results are not available until 48-72 hours after their ER [emergency room] visit. So a few patients grew so frustrated by not having the results available when they check the system the day after their visit. They would check every hour, hoping for something different, then give up after 4-5 tries." Thus, patients are generally interested in using new information technology to access their medical information, but may become frustrated and give-up if the system does not work according to their expectations. There are two things that can be done to address this problem: educating the patient population about proper use of the information system, and designing user-interfaces that more closely correlate with user expectations and experiences with other

---

[68] Personal conversation, 16 May 2002.

software tools. This means that a careful use-case study of the user-interface of PING's various applications is essential to practical acceptance of the system by real-world patients.

The second prototype is a state-wide immunization registry in Vermont, which is being done in collaboration with the American College of Pediatrics, the Vermont State Department of Public Health, and the University of Vermont, Burlington. Regional immunization registries are important because they enable the epidemiological study of diseases across geographic areas. The PING system allows for the creation of a national immunization registry, yet one that does not threaten the privacy of individual citizens. In traditional registry projects, someone other than the patient owns and controls the information, and it is often difficult, if not impossible, for the patient to look at her own record. PING addresses this problem by placing control of the immunization information in the patient's own hands.

The current prototypes demonstrate that PING is a working and reliable system. This section has analyzed the architecture of PING, and has shown it to be a secure and reliable trusted third party for medical records. The next section compares PING with the UHID standard discussed in section 2, and discusses real-world issues in the deployment of PING.

PART IV: ADVANTAGES OF THE PING SYSTEM

4.1 Goals met by PING

The Department of Health and Human Services (HHS) identified a series of objectives that would be easier met with the presence of a unique personal health identifier. We now turn our attention to addressing the problem of how well PING satisfies the major goals outlined in the HHS white paper on the unique personal identifier.

In the following, the issue of universality of access and usage is not discussed. Instead, an environment in which PING is ubiquitous is assumed. Potential market dynamics and other issues concerning the actual adoption of the PING system will be discussed in a later section.

4.1.1   The role of PING in a medical information system

PING does not replace the existing systems of record-keeping that hospitals must employ. PING functions as an aid to healthcare consumers: it is a record that is owned by the patient, randomly accessible by the patient, and monitored by the patient.

HIPAA imposes affirmative obligations on hospitals and other healthcare providers to maintain records of their medical transactions;[69] states generally do the same.[70] Additionally, healthcare providers themselves have incentives to maintain their

---

[69] See 64 Fed. Reg. 59994.

[70] See, for example, 055 Pa. Code §1101.51 (d) and (e).

own records (i.e. for use in the event of malpractice claims) and furthermore, have the right to maintain them.[71]

4.1.2   Continuity of Care

For the purposes of evaluating PING's efficacy at assuring uniform continuity and quality of care across organizations, two major factors are of concern. First of all, the effectiveness of PING depends largely on its interoperability with legacy medical informatics systems. Second of all, continuity depends largely on the delicate balance between the availability of points of access and the overriding need for system security. If a patient's PING record is not readily available at many loci of care, then PING carries with it no intrinsic advantage insofar as continuity is concerned. If a patient's PING record sacrifices availability for security and flexibility in patient management, then PING could potentially create a privacy problem that does not exist now.

Fortunately, neither of these eventualities appears to be the case. First, a PING record is designed to contain many types of electronic data. The type of data handled by the PING server is of no concern to the server's operation, as described above. The challenge then lies in ensuring that the data itself, routed through the PING server, can be read by a variety of participants in the healthcare process, regardless of their organizational affiliation. This is not a problem unique to PING; indeed, any attempt at unifying medical records across boundaries will encounter this same problem.[72] As we

---

[71] Conversation with Eric Pan, 8 April 2002.

[72] See for example, W. Grimson, et. al. Federated Healthcare Server—The Synapses Paradigm, International Journal of Medical Informatics, 52 (1998) 3-27. This paper describes a means of using a form of intermediation to ensure compatibility between different organizations' healthcare records. For successful implementation, however, data must be converted to be understandable in the terms of the Synapses server, a problem similar to what could be experienced with PING.

have discussed, PING is engineered specifically to accept a wide variety of data into the records that it manages (*cf.* the "sponge" metaphor). And as consensus emerges in record standards (HL7, X12, etc.), the PING record should become increasingly universal. Longevity is also aided by the use of XML, as discussed in §3.3.

Next, the issues of balancing security and access have figured prominently in PING's design. Access points are easily accessible to those with permissions — they are located on the World Wide Web. The control over assigning permissions rests with the patient and other entities in which the patient places his or her trust. Additionally, our analysis of the threat model indicates that PING can be trusted to run securely for a long span of time. Moreover, the inherently decentralized nature of PING key distribution provides a less obvious target for those who deign to gain unauthorized access to PING records. Finally, by remaining separate from hospital record systems, PING avoids adding infrastructure to existing systems that could potentially have unintentional, compromising effects on internal hospital records. Given a reasonable assessment of security risks, and taking into account the inherent flexibility of the system, it appears that PING allows many modes of use while not compromising its most essential aspect — security.

4.1.3   Accurate record keeping

Whether or not PING can actually meaningfully improve the accuracy of records kept of someone's medical record is not immediately clear. The unique personal health identifier would have plausibly improved the accuracy of the computerized patient record. Checks for consistency of data become easier given a single element that may be

used to `JOIN` multiple databases to form a coherent personal record. Additionally, questions of mistaken identity would be effectively eliminated through use of the identifier, if the security of such a system were not to be breached. In contrast, the PING system may seem to do the opposite: control over patient information is distributed among a wider variety of actors, and moreover, the administration of internal hospital records is not changed in any material way by the presence of the PING adjunct.

In response to this claim, several things may be said. First, data entered in the PING system is accurately stored, auditable and verifiable. Second, the same actors who handle record-keeping in the status quo will retain their power in responsibility in a system with PING. Third, patients regard their medical information with a great deal of importance and are likely to be reliable monitors of and contributors to their medical record. Finally, with all of this, PING could also provide a measure of error correcting functionality above what is currently possible with existing medical record systems.

4.1.3.1 Data in the PING record

The data in the PING record is, by its nature, very sensitive. As a result, care needs to be taken to ensure that a data stream transmitted to a PING server arrive intact and with substantial identifying information. The design parameters of PING hold these as central goals. Existing implementations have used robust digital signature technology to verify the content and author of a message incorporated in the PING record.

4.1.3.2 Access control and the record

Equally important to the effectiveness of the PING record is flexibility in the allocation of rights to information. Rights to information are managed by logging of the *author* of content in the record as well as the *owner*. This allows for different parties to share different privileges with regard to the same data. Creation of data, for example, can bestow the right to delete the data upon the creator only, as the application dictates.

4.1.3.3 Patients as masters of their own record

Much hinges on the question of whether or not patients can be trusted to report accurately to their patient record if necessary. While the audit trails in the PING record are thorough, the patient could conceivably have the power to obfuscate, if not corrupt, the record. Whether this would be through a conscious desire to conceal potentially embarrassing information, or through incompetent use of the PING system, the end result is the same. Misuse of the PING system has the potential to confuse, rather than clarify.

A priori, limitations can and should be placed on the patient's power to modify his or her own medical record. First, there does not seem to be too much of a need for restrictions on adding information to the record. A patient could add annotations and commentary to his or her satisfaction and never risk being confused with a doctor or healthcare administrator. This is guaranteed by the authentication and signing process that occurs whenever an item is added to the PING record; it would be almost impossible for the patient to convincingly imitate a qualified doctor.

Moreover, patients have been shown to be reliable reporters of their own information when called upon to do so. A 1992 study by the Center for Health Research

took a survey of 380 patients and asked each in some detail about various aspects of their medical history. Patients' responses, when compared to medical records, showed sensitivity across all areas of query, by and large, and a good degree of specificity for a somewhat smaller subset of the tests.[73] A more recent study concluded that given sufficiently specific instructions and frequent regimens of self-testing, over 90% of hypertensive patients studied were able to report their blood pressure with a high degree of accuracy (less than ±3-4 mm Hg uncertainty).[74]

A study at Children's Hospital in Boston compared parents' reporting of their children's past medical history to a computer terminal with face-to-face interviews with a doctor. The validity of the information supplied was high, 94 to 99 percent for the information regarding past medical history. The study concluded that parents could be relied upon to contribute accurately to their children's electronic medical record.[75]

These studies suggest that patients, on the whole, operate in good faith when dealing with medical record systems, supplying reliable and helpful information. These studies indicate that the value of the PING record could only be increased by the presence of patients' input to the record keeping process, so long as their remarks remained properly attributed.

The picture changes somewhat when the subject of deletion from the PING record is concerned. First, it is important to recall that nothing can be truly "deleted" from the PING record — only relegated to a less recent "edition" of the record. However, a

[73] Brown, J.B., Adams M.E. Patients as reliable reporters of medical care process. Recall of ambulatory encounter events. Med Care 1992 May; 30 (5): 400-11.

[74] Ciree A. et al. Influence du protocole sur la qualite de l'automesure tensionnelle. Arch Mal Coeur Vaiss 2001 Aug; 94 (8): 893-6.

[75] Porter, S.C. et al. Parents as direct contributors to the medical record: validation of their electronic input. Ann Emerg Med 2000 Apr; 35(4): 346-52.

"deletion" from the record has the potential to substantially alter the "surface" appearance of the PING record in ways that are not helpful to the overall medical records picture. It follows that a qualified medical practitioner, trusted by the patient owning the PING record, should hold the power of iteration-by-deletion, and not the patient. In the event that some dispute should arise over the validity of an entry in the medical record, the patient's capability to access and audit his or her own medical record vis-à-vis the easy access and extensive audit trails built into the PING architecture provides a necessary framework for a transparent adversary process. PING allows for a secure and trusted forum in which to resolve record disputes between interested parties. Giving patients the right to delete elements from their record carries no real advantage, and introduces a significant measure of risk.

In sum, there is little reason to fear that patients adding dada to their own records would compromise a PING record. However, a responsible implementation of PING should carefully restrict the files that patients are able to delete.

4.1.3.4 Riding piggyback: PING as a redundant record

The question now arises: Can PING contribute to the verification of information in legacy electronic medical record systems? The answer is a qualified yes. Existing methods of verifying medical records are automated, relying on bulk statistical analysis of an entire hospital's record.[76] Restrictions of access to the PING record preclude such a comprehensive search of a wide range of patients. However, in the case of a confusion localized to a small group of patients, obtaining access to the group of PING records may

---

[76] One such method is described in Hassey et al., A survey of validity and utility of electronic patient records in a general practice. BMJ 2001 Jun 9; 322 (7299): 1401-5. The response to the article, BMJ 2001 Nov 17; 323 (7322): 1184; discussion 1184, alludes to several more such methods.

be possible. In this case, PING can function as a "redundant record," allowing a practitioner to compare two potentially differing records. The auditing functionality of PING again can be useful in this situation.

Clearly, a PING system does not markedly assist healthcare providers in verifying accuracy of records across administrative boundaries in as much volume as a unique individual health identifier would. However, in some cases, PING has the potential to serve as a useful and rich source of information that can be helpful in ensuring the accuracy of a hospital's medical record.

4.1.4 Collections

PING would have limited use in the collection of payments. First, while billing information could certainly be stored in a PING record, PING is also, by its nature, not compatible with the innards of a hospital billing and payment system. The usefulness of PING as an instrument of simplification in the financial realm is thus limited.

4.1.5 Fraud and law enforcement

Insofar as fraud is concerned, a medical record is useful insofar as it may be used by law enforcement. HIPAA regulations discuss this type of use of the healthcare record. The rule making mainly treats disclosures of information by a "covered entity," defined as a health plan[77], healthcare clearinghouse[78], or a healthcare provider[79] who transmits electronic health information pursuant to the activities covered by the rule.[80]

---

[77] HIPAA, supra note 4, §1171(5)
[78] Id., §1171(2). The definition reads: "The term 'healthcare clearinghouse' means a public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements." Here standard refers to data transfer conforming to the rulemaking in sections 1172-1174

Availability of medical records held by covered entities follows well-prescribed legal patterns for disclosure. Covered entities may disclose information to health oversight agencies without notice or consent from patients involved or a warrant from a magistrate, so long as the information is not used in direct connection with an investigation of a patient.[81] In judicial proceedings or for needs of law enforcement, a court order, or (under certain circumstances) a subpoena, is sufficient for the discovery of personally identifiable health information by law enforcement agencies.[82]

None of these powers or means of discovery would be directly abridged by the existence of the PING system; as discussed, the PING system does not replace existing hospital record systems. Moreover, it appears unlikely that any organization providing PING services would be considered a covered entity under the current language of HIPAA[83] — hence the aforementioned privacy rules dealing with oversight and law enforcement would not specifically apply to the PING record. Most importantly, a PING record differs from a conventional record in that the patient is the owner of his or her own PING record. Putting these facts together, it is clear that the PING record exists in a different privacy framework than conventional medical records.

Though a market structure that might govern PING has yet to be realized, architectural concerns indicate that the present day role of Internet Service Provider (ISP)

---

of the HIPAA of 1996. PING, operating independently of legacy healthcare systems, and being not specifically designed to operate in conjunction with or in conformation to the provisions of the aforementioned code, would probably not be considered a "healthcare clearinghouse" after subjection to legal scrutiny.

[79] Id., §1171(3)

[80] Final Standards for Privacy of Individually Identifiable Health Information, §160.102

[81] Id., §164.512(d)

[82] Id., §164.512(e), §164.512(f)

[83] Conversation with Dr. Isaac Kohane, 23 April 2002. See also HIPAA, supra note 77.

might serve as an appropriate analogy for the sort of role that the operator of the PING server/content warehouse might play under PING.

The first level of privacy that a user can expect to receive is governed by the ISP's Terms of Service. Experience with the UHID, as well as opinion surveys (see §4.3.1), indicate that consumers value their health privacy very highly and would be unlikely to entrust any service with that information without clear and strong provisions for the protection of information routed through or stored on the ISP's servers. The market could reasonably be expected to provide for strict contractual provisions for privacy.

Use of electronically communicated and stored information for law enforcement and other governmental purposes is controlled by the Electronic Communications and Privacy Act of 1986 (ECPA). The pertinent disclosure provisions, insofar as medical records are concerned, dictate that a warrant is required for a governmental agency to obtain the information without notice to the owner of the record, and that a subpoena may be used to obtain the information if notice is given to the owner.[84] Though this is far from a complete discussion of privacy issues facing ISPs, a comparison of the HIPAA privacy rule and the applicable disclosure provisions of the ECPA indicate that the ECPA establishes a higher standard for disclosure of medical records held by an individual; specifically, the HIPAA privacy rule contains alternative provisions for disclosure, without a warrant or notice, when the records desired are not used in the prosecution of the person in question.[85]

---

[84] 18 USC §2703
[85] Final Standards for Privacy, supra note 80

It is then difficult to regard PING as an effective instrument of law enforcement. The number of actors introduced into the data storage and transmittal picture is potentially large, and the protections given to individuals' electronic data are strong.

4.1.6   PING and the UHID

PING compares favorably to a UHID scheme in the regards of continuity of care, and can plausibly improve the accuracy of medical records. However, the individualized PING record is less easily accessed by law enforcement and other regulatory bodies than is bulk health information contained in hospitals. Strictly speaking, PING would be less useful for law enforcement than the UHID. The question now is one of balance. Many groups were opposed to the UHID on the grounds that it too easily enabled governmental aggregation of information. As an instrument of policy, should PING be faulted for preventing what has already impeded the implementation of one scheme for achieving a more comprehensive national health infrastructure? Perhaps it should not — the UHID debate has shown that even in the face of approval from a variety of industry groups,[86] individuals' privacy concerns can have a substantial voice in the dictation of policy. It is to those individuals, and their related concerns in the new realm of electronic healthcare, that our discussion now turns.

4.2 Impacts: What PING can offer

To provide a truly compelling policy option, the PING system must offer advantages that transcend adequacy at meeting the goals that motivated the proposition of the unique personal health identifier. We contend that PING does offer benefits, both

---

[86] HHS White Paper on UHID, supra note 17

short- and long-term, that are impossible without the incorporation of its particular architecture into the nation's health infrastructure.

4.2.1 The proactive patient

Patients are nominal owners of their medical records, but that ownership does not translate to control over the way their data is handled, nor to detailed knowledge of the detail contained therein.[87] PING takes a first, giant step towards redressing the problem by providing a tool by which patients may increase their knowledge of, and participation in, activities involving their medical records.

Batami Sadan has pointed out a case for what she calls "patient co-ownership of medical records." While her concept is legally redundant, it has a functional aspect that is revolutionary. Her advocacy of co-ownership turns on three major points. First, involving patients in the information management process can lead to improved privacy practices. Second, communicating data directly to patients via a record-keeping system provides an objective way of communicating treatment options that is currently unavailable. Finally, involving patients in the data recording process adds to the richness and usefulness of the medical record. Patient involvement, she concludes, not only improves privacy practice but also has the potential to better handle the subjective aspects of clinical treatment.[88]

---

[87] Riva et.al., supra note 46

[88] B. Sadan. Patient data confidentiality and patient rights. Int. J. Med. Inform. 62 (2001) 41-49. Sadan makes specific mention of the inherent subjectivity of the clinical decision making process, and notes that the patient-doctor relationship is marked by an inherent asymmetry of information. While much of this asymmetry is unavoidable (not every patient can reasonably be expected to hold an M.D.), enabling easier flows of information between the patient's electronic record and all interested parties could improve the situation substantially.

Sadan's claim is a powerful one, and highlights a major deficiency in existing medical information systems: the patient's interests in their own medical information are not necessarily considered in the design of such a system. Moreover, her analysis is emblematic of an emerging trend in medical informatics: the appearance of interactive health communication (IHC) technology as a supplement to existing patient-doctor relationships. Emergence of new technologies has created new kinds of consumers for healthcare products – consumers who are increasingly interested in taking proactive roles in their personal health management.[89] A trustworthy system like PING, used in conjunction with trusted doctors and administrators, could prove an exceptionally valuable tool in the new consumer health landscape.

To better understand the dynamics of the situation, we first give a brief overview of interactive health communication and its applications and risks. We then evaluate the ability of the PING architecture to provide value-added IHC services as part of its information management capabilities.

4.2.2   Interactive Health Communication defined

The realm of interactive health communication is crowded, and a taxonomy of viable IHC models is well beyond the scope of this paper. In a broad sense, IHC may be defined as "the interaction of an individual – consumer, patient, caregiver, or professional – with or through an electronic device or communication technology to access or transmit health information, or to receive or provide guidance and support on a health-related

[89] See Cochran, supra note 2. Cochran used the term "21st Century Health Consumer" to refer to this trend in his talk before the 1999 CPRI fall conference.

issue."[90] Interactive Health Communication functions generally include: (1) *relaying*

information, which means to provide general or personalized health information on

demand; (2) *enabling informed decision making,* which can involve active computerized

assistance with selecting healthcare options, or facilitating communicating with a

physician or other expert party; (3) *promoting healthy behaviors*; (4) *promoting peer*

informational exchange and emotional support; (5) *promoting self-care,* which may

involve disseminating information and encouraging users to use said information to

manage their own health; and (6) *managing demand for health services*.[91]

4.2.3   The modern health consumer

Evidence indicates that the proliferation of information technology is affecting

consumer expectations and habits. Consumers are both aware of the availability of

information and interested in obtaining it.[92] Moreover, as the Internet establishes itself

ever more firmly in the mainstream, the class of users interested in having access to

health information is expanding, from the technically savvy to the neophyte.[93]

As consumers are learning more, they are becoming increasingly interested in

contributing proactively to their healthcare. A 1998 survey revealed that upwards of

eighty percent of all patients are likely to seek information about treatment options

---

[90] Robinson TN, Patrick K, Eng TR, Gustafson D, for the Science Panel on Interactive Communication and Health. An evidence-based approach to interactive health communication: a challenge to medicine in the Information Age. *JAMA*. 1998; 280:1264-1269.

[91] Science Panel on Interactive Communication and Health. Wired for Health and Well-Being: the Emergence of Interactive Health Communication. Eng TR, Gustafson DH, editors. Washington, DC: US Department of Health and Human Services, U.S. Government Printing Office, April 1999, at 13.

[92] Id., at 7. One example was cited of searching patterns on the National Library of Medicine's MEDLINE database in the year after the database became freely available on the Web. The number of searches increased tenfold, and thirty percent of the users were members of the general public.

[93] White Paper: The Find a Health Site Report: Enhancing the Quality of Interactive Health Communication. Tanner TB, Principal Investigator. Report presented to National Cancer Institute, 9 February 2001.

themselves, and of these, more than half are likely to make a decision themselves based on this information.[94] Moreover, according to the same survey, eighty percent of consumers want to play a "major role" in treatment of major ailments and in prevention. Sixty percent want to play a "major role" in the treatment of common illness.[95]

The convergence of these two trends puts healthcare service providers in a unique situation: they increasingly have to provide care in an environment of ubiquitous information. In some cases, this proliferation of advice and counsel external to the primary physician-patient relationship has been perceived to undermine the physician's status as a source of reliable and trusted information, in some cases even leading patients to "challenge" their doctors' recommendations.[96] Though this is not necessarily true in all cases, it does provide primary care providers with a new challenge: how to maintain their role as a trusted practitioner in the information age.

In this environment, consumers also have emerging needs. The first is to be able to reliably choose trusted sources of electronic health information.[97] As a youthful technology, no "canonical" IHC service has yet emerged from the clutter of existing IHC services. For example, a survey of Internet users who search the web for health information revealed that the highest-recommended health information site (DrKoop.com) could claim only 19% of users as loyal adherents to the site; five other sites could claim response rates of ten percent or more as the "best source for Internet health information."[98]

---

[94] Cochran, supra note 2, at 9.
[95] Id., at 10.
[96] Eng et al., supra note 90, at 21.
[97] Id., at 76.
[98] Tanner et al., supra note 88, at 19. The survey was web-based and given to visitors of www.health-center.com.

Moreover, a similar survey indicates healthcare professionals have not even reached a consensus as to the usefulness of Internet-based health information. Roughly equal amounts of respondents replied that their physicians considered using the Internet for health "dangerous, poor idea" and "very helpful, tremendous."[99] In the absence of consistent advice from health professionals, patients have to rely on their own, inexpert intuition to guide themselves toward helpful information.[100] While interest remains high, IHC technology is clearly a technology which has yet to mature.

4.2.4   Risks of IHC

Studies have identified a few risks of IHC. They include (1) *inappropriate treatment or delays in care*, potentially caused by inaccurate information given to the patient; (2) *damage to the patient-provider relationship*, as discussed previously; (3) *violations of privacy and confidentiality*; (4) *wasted resources and delayed innovation*; (5) *unintended errors*; and (6) *widening the technology and health gap*; or the risk of widening the "digital divide" as regards health information and service.[101]

4.2.5   PING as Interactive Health Communication

Under the definitions agreed upon in the literature, PING certainly qualifies as a form of interactive health communication. It is first and foremost a method of relaying personalized medical information between different parties; information stored in the PING system is available in real-time to a variety of actors concerned with the patient's healthcare. This is very appealing feature in itself; as discussed in §3.7, consumers have

---

[99] Id., at 19. The numbers were 32% and 29%, respectively.
[100] Eng et al. contains an interesting hypothetical case study this effect. Supra note 90, at 77.
[101] Id., at 20.

reacted very favorably to PING. Behavior patterns in the trial discussed indicated that consumers could, quite literally, not get information quickly enough.

What is less obvious is that PING has the ability to enable informed decision making, not only on the part of the patient but the doctor as well. Sadan[102] notes in her paper several ways in which the sharing of information between physician and patient is characterized by an inherent subjectivity. Patient and physician may share different perspectives on the same medical position because of the simple difference in roles between the person experiencing the illness (and the concomitant "loss of wholeness," as she puts it) and the doctor making a clinical decision with the patient. The physician may have a difficult time reasonably conveying the amount of risk associated with a given course of treatment. Most significantly, the physician has the power to use his or her superior knowledge of the subject matter at hand to implicitly recommend one course of treatment over another.

While all of these are unavoidable consequences of the inherently different roles taken by patient and doctor, tools can still be developed to help manage and minimize the deleterious effects of such difficulties in communication. PING is emblematic of this technology at its best. The PING architecture enables the medical record to come to life, becoming an important and personalized source of shared information between physician and patient. The PING record could very plausibly become a source for increased interaction, both face to face and electronically, between physician and patient.[103] Given a common record and set of information to work with, a patient is able to ask their

---

[102] Sadan, supra note 87.
[103] See Borowitz S.M., Wyatt J.C. The Origin, Content, and Workload of Email Consultations. JAMA. 1998; 280: 1321-1324 for an example of how electronic interaction can improve quality of care.

physician better questions and, if necessary, be able to seek outside help with the confidence that their clinical data can be reported as accurately as they wish it to.

In addition to making information available to as many parties as the patient wishes to authorize, PING can itself become a mode for more information exchange than has previously been possible in the realm of the personal medical record. As noted in section 4.1.3.3, patients would be able to make their own contributions to their personal medical record. A given treatment plan could be documented by the doctor in the PING record and annotated by the patient. This record could then be called up years later by another, perhaps different, doctor and the patient's annotations and comments on the treatment used as an important tool in both generating a dialogue between doctor and patient and in enabling a more informed clinical decision. Sadan specifically advocates this in her paper, noting that co-documentation, as she calls it, could allow a patient to feel more a participant in the decision-making process.[104] By incorporating input from all sources and evening the distribution of trusted information between parties, PING is able to better deal with the inherent subjectivity of the treatment process, open new channels and forums for discussion, and to satisfy the proactive mindset of modern health consumers.

As an additional benchmark for evaluating an IHC system, Eng et al.[105] have identified six criteria that they believe to be key to the evaluation of any IHC application. We comment briefly on each of these criteria.

(1) *Accuracy of content.* As discussed previously, the PING system contains

safeguards, audit trails, and other related functionality that provide excellent

---

[104] Sadan, supra note 87, at 46.
[105] Eng et al., supra note 90, at 55.

assurance of the accuracy of the record. Being a patient's personal medical record, rooted in fact, the PING content is likely to be one of the most pertinent sources of content that a patient will be able to choose from.

(2) *Appropriateness of content.* Here, while the content of a PING record is clearly applicable to its owner, the level of expertise assumed in the expression of the content may be too high for the layman. However, that does not preclude the patient from using the content as a basis for discussion and consultation, as well as annotating his or her own record.

(3) *Usability.* This is one component of PING that is very much in flux. Demonstration versions of the software, as discussed, have intuitive web interfaces; however, one man's intuitive is another's arcane. Only wider release and testing of the actual PING interface will indicate how usable the system is.

(4) *Maintainability.* As discussed before, PING is designed to run for a long time and main compatibility with an indeterminate number of file formats. As long as a file means something to somebody, it will mean something to PING.

(5) *Bias.* This characteristic is almost non-applicable for the PING system. It is worth mentioning that if anything, the PING record benefits from the presence of authenticated and attributed biased statements, as these statements form an important part of the dialogue that may be engendered by the system.

(6) *Efficacy and Effectiveness.* Currently, no evidence exists of the real-world implications of a widely adopted PING system. We will discuss the real-life dynamics of PING in the next section.

Though not realized yet as a consumer product, the architecture of PING is inherently well suited to meet the criteria that effective interactive health communication systems must satisfy.

4.3 PING and the real world

We now relax our assumption of universal acceptance and use of the PING system, and indeed of electronic medical records in general, and turn to the evaluation of PING as a real-world policy option. It is unrealistic to expect adoption and use of such a far-reaching system as PING to be ideal in all respects. As a result, we consider in turn the consumer and provider perspective, and discuss potential problems and their impact on the goals of a PING system.

4.3.1 <u>PING and the Consumer</u>

One of the risks associated with the adoption of an interactive health communication scheme is that access is not equal across demographic lines. The so-called "digital divide" could acquire new significance were it to become synonymous with stratification in the quality of healthcare delivered to different people, based on their access to information technology.[106]

The first issue is accessibility. Since PING uses the world wide web as the locus of access, access to PING is contingent upon the availability of an Internet connection. Studies confirm a "digital divide" in this regard. Overall, 51 percent of Americans have a computer; 42 percent have access to the Internet. Predictably, this is not the case across all levels of income; those making between \$50K and \$75K annually enjoy overall

---

[106] Eng et al., supra note 90

Internet access rates in excess of 60 percent, and those making above $75K approach 80 percent access rates. However, as annual income falls, the percentage of people having Internet access drops precipitously.[107]

None of this information is particularly surprising. However it raises a question about how universal the PING system may be expected to be. Without a doubt, different classes of users will emerge in a widespread implementation of PING. According to Dr. Isaac Kohane, Principal Investigator for the PING project, the classes of use will be defined by the patient's ability to access and effectively use information technology. However, the barriers to access are not absolute, and the main barriers can be expected to be educational or conceptual.[108]

The existence of use classes, it should be noted, is not bad in and of itself. In many cases, it may reflect the interest of the patient in the subject matter at hand. It may not be conceptually necessary for every patient to store their PING record on the server of their own choosing, even though that option is available. There must, however, be a baseline level of competence that all users must share, or some would be unable to use the PING record effectively.

The PING record may well be described as "quasi-static." Over the time frame of months and years, the record evolves as health concerns emerge, but routine daily maintenance of the PING record is not likely to be necessary. Consequently, linking home-based Internet access with the ability to effectively manage one's PING record is fallacious. For the types of occasional, directed access that are necessary, any variety of forums may suffice. Since connections to the PING server are secure regardless of the

---

[107] Statistical Abstract of the U.S.: 2001. US Census Bureau, 2002, at 720.
[108] Conversation with Dr. Kohane, supra note 82

point of access, a public library suffices for occasional maintenance of one's PING record. Moreover, it is not inconceivable to see the emergence of dedicated computer kiosks in loci of care.[109] Consequently, the issue of physical access need not be particularly significant in determining how effectively one can utilize the PING functionality to achieve their personal health management goals.

The educational/conceptual barrier may prove more difficult to surmount. Current trials of PING include information pamphlets designed to guide users of the system through the process of managing their personal medical record.[110] Existing trials have shown that users are unfamiliar with the pace at which medical data is processed;[111] what other technical gaps in knowledge exist should become clearer over the ensuing months.

Accompanying the issue of education is that of a "social engineering" attack towards users designed to obtain their personal information through some means of deception. This can include commercial offers promising some free good in exchange for access to an individual's PING record. The question arises: does a large, less educated class of users of healthcare information have the ability to effectively distinguish between appropriate and inappropriate uses of one's own record?

While such a circumstance has yet to occur, existing evidence indicates that consumers are likely to be wary of such inducements. A 1994 poll indicated that 75 percent of respondents are concerned about insurance companies' misappropriation of

---

[109] Porter et al., supra note 74 provides one possible scenario.
[110] Conversation with Eric Pan, 16 May 2002.
[111] Id. See §3.7.

electronic medical data.[112] In a 1993 poll, 96 percent of respondents expressed the sentiment that medical information should be classified by the government as "sensitive" and be protected by stiff penalties for unauthorized disclosure.[113] Moreover, a recent poll had 87 percent of respondents apply in the affirmative when asked whether they had ever refused to give a business personal information on the grounds that it was unnecessary or too intrusive.[114] With medical privacy so highly valued by consumers, and an uneasiness about the ability of corporations to responsibly handle sensitive data,[115] such barefaced ploys to obtain medical data as those hinted at appear unlikely to enjoy more than a small measure of success.

In short, there exist asymmetries of access and education in the consumer marketplace that may make a successful implementation of PING more difficult, but such difficulties may be dealt with a combination of architectural evolution (i.e., increased public access to the Internet, wired hospitals) and consumer education.

4.3.2   Institutional Barriers to Adoption

It is tautological that PING must be widely used to be of any use as a policy instrument.   A natural question then arises: What are the issues affecting the implementation of a system like PING?

---

[112] Electronic Privacy Information Center, http://www.epic.org/privacy/medical/polls.html , accessed 13 May 2002.
[113] Id.
[114] Electronic Privacy Information Center, http://www.epic.org/privacy/survey/default.html, accessed 13 May 2002. Source: Harris Interactive, 19 Feb 2002.
[115] Id.

4.3.2.1 Electronic Medical Records – Issues in practice

A first step towards an answer lies in the use of electronic medical record (EMR) systems. The impact of easier electronic transfer of medical records is directly proportional to the prevalence of EMR in common practice. The implementation of an EMR system, especially on a large scale, is an enormous task; so despite the many advantages of such systems, adoption has been slower than one might hope.[116]

Evidence in ambulatory care practice indicates resistance to full acceptance of electronic medical records. A survey of practitioners based in Hong Kong revealed that the computer, while recognized as a necessity in modern practice, is not perceived as a benefit. EMR systems were perceived as time consuming, both in terms of the time taken to learn to use the system and the actual use of the system during consultations. Moreover, physicians surveyed seemed unconvinced that EMR systems could substantially benefit their patients.[117]

Hospital practice appears to face similar challenges. A survey revealed that 53 out of the 72 hospitals in Norway had taken concrete steps to implement an EMR system as of January 2001.[118] Physicians practicing at hospitals implementing EMR systems were queried regarding the ways in which they used the medical record systems that their hospitals had already implemented them. The doctors surveyed were, as a whole, computer literate and had easy access to computers. Irregardless of these facts,

---

[116] Iakovidis, I. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe. Int. J. Med. Inform. 52 (1998) 105-115

[117] Johnston, J. Physicians' attitudes towards the computerization of clinical practice in Hong Kong: a population study. Int. J. Med. Inform. 65 (2001) 41-49

[118] Laerum et al. Doctors' use of electronic medical records in hospitals: cross-sectional survey. BMJ 2001; 323:1344-1348

physicians' responses indicated the medical records systems being used at a capacity significantly below their functionality; user satisfaction was, as a whole, "moderate."

It should be noted, however, that electronic medical record systems are not doomed to fail simply because support for EMR is not universal among the population of physicians. What is indicated is that the process of adoption needs to be a gradual one, and the effect of computerization on the patient-doctor relationship needs to be stressed.[119]

From an administrative perspective, the business case behind any EMR system is paramount. The director of information systems of a chain of hospitals noted the usual suite of motivating factors for an EMR system – customer satisfaction, the need to reduce errors in hospital operations, and access to a continuum of information over a wide area – but with the qualification that all of these goals must eventually translate into the eventual goal of more business for the healthcare provider.[120]

4.3.3.2   Implications for PING

In a sense, PING is independent from many of these concerns, as it in no way purports to serve the functions of a hospital EMR system. What is at stake is not necessarily hospitals' hardware implementation of a PING server and the accompanying software; more important is the general issue of PING advocacy and compliance. Healthcare providers need to believe in the potential for PING to achieve positive ends to the extent that they support and advocate its use. Then if PING is to eventually serve as

---

[119] Hood, B. et al. An Incremental Approach to a Web-Based Computerized Medical Record. J. Healthc. Inf. Manag. 2001; 15 (3): 199-205
[120] Conversation with Patricia Malloy, Director of Information Services for Ministry Healthcare, 14 May 2002.

an effective bridge between organizations, and if PING is ever to reach its potential of assuring continuity of care and all of its other assorted advantages, it must respect the concerns that have inhibited full utilization of EMR capability to date.

The first of these concerns to address is the physician. Here, PING's potential to enhance the doctor-patient relationship can prove key to dispelling the belief that computers dehumanize practice. Existing EMR systems can carry the stigma of being simply tools for administrative simplification, and not necessarily for improving the quality of care delivered to patients or the doctor-patient relationship.[121] Moreover, PING needs to be a timesaver. Time is one of the physician's scarcest resources; saving time assists the physician in providing high quality care, and increases his or her satisfaction.[122]

The issues from an administrative standpoint are in a way less tractable. First of all, the act of making available a PING data stream via a secure connection, even on a moderate to large scale, should not prove prohibitively expensive for healthcare organizations.[123] Expenses are likely to be incurred through education – both of the employees of the hospital and of the patients who use PING for their medical records. Moreover, as an architecture, PING need not initially impose any additional demands on a medical records implementation other than the act of sending the secure data stream; hospital EMR implementation timetables need not be disrupted through the adoption of the PING system.

A major difficulty lies in an inherent collective action problem that exists for the interconnection of hospital information systems. Each healthcare organization looks for a

---

[121] Johnston et al., supra note 116
[122] Conversation with Malloy, supra note 119.
[123] Id.

competitive advantage in its information system, and a system like PING that enables effortless flows of information between organizations could be perceived as undermining a hospital's business interests by easing a patient's transition between institutions.[124] Consequently, industry-wide acceptance of PING as a viable architectural model is unlikely to come from purely business-related motivations. This means that higher-level uses of PING functionality (the PING Puller application, etc.), which require larger degrees of integration with hospital information systems, may be difficult to implement. Administrators are unlikely to grant PING a substantial amount of privilege on their internal information systems without a compelling business case for such an operation.

The collective action problem may prove significant enough to effectively preclude the widespread adoption of PING or PING-like systems for the foreseeable future. In this case, it is possible that legislation may be required that mandates the establishment of PING as a government-sanctioned record-keeping system that also enables hospital interoperability and intercommunication.

---

[124] Id.

PART V: CONCLUSION

The policy issues surrounding the medical records problem are subtle. An initially obvious and efficient solution – the unique personal health identifier – languished because its aims were fundamentally irreconcilable with the privacy concerns of the vast majority of American health consumers. Americans, time and time again, have shown themselves to be wary of attempts to mass their personal data in any sort of centralized framework.[125] The progress on the unique personal health identifier has now stalled – no concrete action is currently scheduled for the foreseeable future on this initiative.

Rather than leave the problem unresolved, we propose PING, an architectural solution to a policy goal. Rather than a simple mandate, PING is a technological innovation that allows a fundamental change in the locus of control of a patient's record. By and large, PING can accomplish the same policy goals as the UHID. It can do this while empowering the patient, instead of making patients feel as though they are losing control of their information to healthcare conglomerates and insurance companies. Moreover, PING respects the evolution of the computer in a way that the UHID proposal did not – PING leverages the ubiquity of information technology in such a way as to allow patients to become contributors to, rather than observers of, their own personal medical history. This is a fundamental change in the conception of a "record." Before the information age, it was impossible to imagine the countless charts, prescription slips, and other records held in immense filing cabinets transforming into a dynamic, evolving personal medical record-cum-decision making forum-cum-personal medical diary. All of this capability is an inherent outgrowth of the flexibility of the PING architecture.

---

[125] See section 2.3.1.

The functionality inherent in PING corresponds deeply to Jonathan Zittrain's concept of "granularity of rights." Zittrain explains: [126]

> Second, privication architectures might help meet the daunting challenge of *defining fair information practices*, since the increased granularity of rights afforded by a technological system makes room for entirely new rights constructs. The expression of rights through a trusted system may allow for "baby-splitting" among interests that is not feasible in more traditional regimes. For example, in place of the stalemate over who should "own" a record, a *well-defined self-enforcing rights architecture* could allow information sharing without having to ultimately resolve matters in as coarse a way as "owner" or "non-owner." A patient might wish the right to delete her record, while medical researchers would object to the non-random loss of possibly important medical data. The system could enable deletion for "most intents and purposes"; one could imagine a deleted record no longer appearing on a hospital computer display, and no longer being available for marketing purposes, while still being included in scans of records by medical researchers.

PING has the ability to securely assess the identity of its users and dynamically assign rights according to the record owner's preferences. This is the crystallization of Zittrain's vision: using technology to enable automated privilege negotiation between parties with different stakes in the same information. PING, then, succeeds as a forum for individuals to establish their own policy over a master copy of their life's medical record and to have their wishes acted on by a system they trust.

The HIPAA experience has shown, and continues to show, that complicated and contentious areas of concern resist sledgehammer solutions — like the UHID. The UHID, and all of its benefits, were effectively voided by its own inability to respect the

---

[126] Zittrain, J. "What the publisher can teach the patient: intellectual property and privacy in an era of trusted privication." Public Law and Legal Theory Working paper series, Working paper No. 007, February 24, 2000 at 64.

privacy concerns that patients have for their personal health information. The nuance possible with the PING system transcends the area of policymaking available to simple rulemaking in and of itself. The opportunities for synergy between law and technology exist. Society can only gain from using them to their fullest.

Acknowledgements