Impact of HIPAA on the integrity of healthcare information

Jane Fedorowicz*[†]

Departments of Accountancy and Computer Information Systems,
Bentley College, 175 Forest Street, Waltham, MA 02452 USA
Fax: 781 891 3153 E-mail: jfedorowicz@bentley.edu
*Corresponding author
[†] Authors contributed equally and are listed in alphabetical order

Amy W. Ray[†]

Computer Information Systems Department, Bentley College,
175 Forest Street, Waltham, MA 02452 USA
E-mail: ARAY@bentley.edu

Abstract: Although most patients' interactions with HIPAA end with signing a patient information release form when visiting their doctor, HIPAA is also intended to protect the integrity of that information as it flows among the many healthcare providers, insurers, and clearing houses that will process it. Information integrity is critically and strategically important to healthcare organisations today. Considering information integrity implications of HIPAA requirements can help healthcare administrators identify strengths and weaknesses in their stored information and in the ways in which it is shared with business partners and other healthcare providers. In this article, we describe the impact of HIPAA on information integrity as well as the information integrity challenges that still lie ahead for healthcare organisations. After a brief overview of general information integrity issues related to information sharing across multiple healthcare organisations, we discuss integrity concerns specific to the primary components of the administrative simplification provision of HIPAA, including transaction codes and standards, unique identifier codes, information privacy and information security. The articles closes with a call for additional research to document the true impacts and costs of the legislation, to produce a framework with which practitioners can make informed choices about information integrity issues.

Keywords: data standards; HIPAA; information integrity; privacy; security.

Reference to this paper should be made as follows: Fedorowicz, J. and Ray, A.W. (2004) 'Impact of HIPAA on the integrity of healthcare information', *Int. J. Healthcare Technology and Management*, Vol. 6, No. 2, pp.142–157.

Biographical notes: Jane Fedorowicz, the Rae D. Anderson Chair of Accounting and Information Systems, holds a joint appointment in the accountancy and computer information systems departments at Bentley College. Professor Fedorowicz earned MS and PhD degrees in systems sciences from Carnegie Mellon University and a BS in health systems from the University of Connecticut.

She is Principal Investigator on the Invision Project, studying interorganisational information sharing in a variety of organisational settings. Professor Fedorowicz has published over 60 articles in refereed journals and conference proceedings. The American Accounting Association recognised Professor Fedorowicz with the 1997 Notable Contribution to the Information Systems Literature Award, and she was selected as Bentley College's Scholar of the Year for 2000.

Amy Ray serves as Trustee Chair in computer information systems at Bentley College. Ray's research appears in numerous scholarly journals including the *Journal of Management Information Systems*, *Information and Management*, the *Journal of Information Systems*, and the *Journal of Strategic Information Systems*. She teaches and coordinates courses on electronic business and information security. Ray recently chaired two international information systems conference committees including the Ernst & Young/American Accounting Association e-business Conference committee and the First Annual AAA-Information Systems Section Conference committee. She is frequently invited as a speaker on e-business research and curriculum opportunities at national and regional IS conferences.

1 Introduction

In 1996, US President Clinton signed the Kennedy – Kassenbaum Bill which set forth a broad set of guidelines intended to protect the portability of patients' insurance when they changed employers, without regard to prior illness. As part of this act, additional requirements were mandated to protect the patients' privacy and the security of medical information and to provide for uniform standards for electronic transmission of healthcare data. Commonly known as HIPAA, the Health Insurance Portability and Accountability Act encourages the use of electronic transmission and provides for standardisation of transactions and uniform code sets to be used by healthcare providers and their business associates.

The Department of Health and Human Services (DHHS) has estimated the cost of HIPAA implementation to the healthcare industry will be $18 billion, although this cost should be offset by administrative savings of $30 billion over ten years (Hellerstein, 2001). Costs to healthcare are high because HIPAA requires significant investment in new information systems, organisational policies and partnership agreements. The legislation is far reaching, requiring organisations to reassess and reengineer business processes and policies as well as technology, in order to comply with the law. One key example is the change to healthcare claims processing as a result of HIPAA. The number of healthcare claims filed each year continues to grow. Prior to HIPAA, there were more than 400 different formats alone for filing electronic claims. This heterogeneity slows down inter-organisational information sharing, creates confusion for claims entry personnel, thereby increasing the likelihood of mistakes, and makes validation of claims information more challenging. Ultimately, the existence of 400 different claims formats has a negative impact on information integrity. Thus, the expectation is that HIPAA will have a positive impact on information integrity, while streamlining processes and reducing costs.

While HIPAA legislation addresses issues beyond administrative simplification, the focus of this paper is the analysis of actual and expected impacts of the administrative simplification sections of the HIPAA legislature on information integrity. The administrative simplification portion of HIPAA enables movement of more healthcare transactions online. The integrity of healthcare information is critically important as we move into an era where information is seamlessly shared at the speed of light across multiple organisations. An error in one healthcare transaction can affect multiple systems. Considering the information integrity implications of HIPAA requirements can help healthcare administrators identify strengths and weaknesses in their stored information and in the ways in which it is shared with business partners and other healthcare providers.

2 Elements of the legislation

Essentially, there are four primary components to the administrative simplification provision of HIPAA, including transaction codes and standards for electronic healthcare transactions, unique identifier codes, information privacy, and information security.

Transaction codes and standards (TCS) regulate the exchange of administrative and financial healthcare transactions. Each electronic transmission must adopt the same standards for transmitting information. Specifically, HIPAA regulators adapted a version of the well-known Electronic Data Interchange (EDI) format as the standard for transmission, as well as a common numbering scheme and set of data elements. Code sets also include allowable values for the data elements.

Unique identifier codes are national employer identification standards that must be used by health plans, healthcare clearing houses and healthcare providers. The information privacy component regulates policies and procedures around a defined set of protected health information (PHI). It governs confidentiality of PHI within an organisation and in transactions with the organisation's business partners.

The information security standards were the last to be finalised. These standards mandate how PHI is electronically captured, stored and transmitted. They apply not only to the privacy of health information, but also to its integrity and availability. The regulation also includes a provision for backing up data (Brewin, 2002).

The TCS standards work in conjunction with the unique identifier codes to simplify data input, manipulation, and retrieval. Similarly, the privacy and security components of the legislation are both designated as necessary for the protection of data.

One primary concern in the establishing of new systems, policies and procedures necessary to meet HIPAA requirements is the integrity of information that is stored and transmitted. In the remaining sections of this paper, we describe the impact of HIPAA on information integrity as well as the information integrity challenges that still lie ahead for healthcare organisations. We begin with an overview of general information integrity issues. The next section covers concerns related to data processing simplification, specifically focusing on some strengths and weaknesses of the TCS and unique identifier components of HIPAA. After that, we discuss some information integrity strengths and weaknesses of the final two components of HIPAA designed to protect data, the privacy and security sections.

2.1 HIPAA and general information integrity issues

Information integrity refers to the state of data as whole, complete and uncorrupted (Whitman and Mattord, 2003). Information integrity is potentially affected every time data is manipulated in one way or another, including all of the following (Gelinas and Sutton, 2002):

- methods used for presentation of data to users
- methods used by database administrators that can affect the consistency and form of record structures when databases are initialised
- information systems and networks that affect the timeliness of information delivery at points of data entry and manipulation
- controls and systems checks that affect record completeness at the point of initial data entry and subsequent manipulation
- controls and checks that affect the accuracy of record content at the point of data entry or data modification.

HIPAA directly addresses *presentation* of data and *structure* of the records in the transaction code sets portion of the legislation, by defining specific standards for transmission of common forms used in inter-organisational information sharing.

HIPAA mandates that healthcare organisations use specific electronic data transfer standards for all of the following types of healthcare transactions:

- coordination of benefits
- healthcare claims status request and responses
- health plan premium payments and fund transfers
- health plan eligibility, coverage, and benefits
- submission of healthcare claims.

The section of HIPAA related to data transfer standards also has an indirect, positive affect on the *timeliness* of data, because it encourages electronic transmission of transactions. This should reduce the time that it takes to move data from point to point, reduce data entry time and eliminate any errors introduced by retyping data. As healthcare organisations become more accustomed to electronic transmission methods, further improvements in timeliness of data should result because data input and management processes should become more systematic.

One new challenge to information integrity in a more electronic environment will be ensuring availability of health information. As healthcare organisations rely more on technology for inter-organisational communication, it will be critically important to always ensure electronic and manual back up mechanisms in case of information system or general power failures.

The information integrity characteristics of *completeness* and *accuracy* of information are not directly affected by HIPAA legislation, so it is up to implementing organisations to consider these issues independently. If records are formatted into a particular structure, the completeness of an individual record should be relatively easy to assess when inspected manually. For example, if a field such as patient last name is not filled in on a standardised form, any administrative personnel who is familiar with the form should recognise that the data is missing immediately. Also, with standardised forms, healthcare organisations or clearing houses should eventually have software that automatically checks for missing fields as each form is processed. In fact, professional clearing houses that claim HIPAA compliance should already have such checks in place. Healthcare organisations looking for new clearing houses should ask questions about automated information completeness and other information integrity checks.

Checking for *completeness* of entire files is more challenging than checking for completeness of an individual form or record. Electronic and manual checks need to be in place to ensure that all forms or records are included in data entry, that the forms are not deleted or lost once entered and that sufficient back-up of entered data exists. Again, HIPAA does not directly address the issue of file completeness.

Perhaps the greatest challenge for healthcare organisations is going to be assuring the *accuracy* of health record content. One key to information accuracy is assurance of data entry quality, including the care and diligence of the data entry personnel, as well as the internal controls put in place to prevent data entry mistakes, such as incomplete records and transposition errors in identification numbers. Standardisation of forms and key data, such as the codes used to identify medical procedures performed, may also have a positive effect on data accuracy, so long as the coding schemes are contextually rich enough to aid effective decision making. Yet it is a mistake to assume that this standardisation process provides complete assurance of information accuracy. Problems with information accuracy in healthcare have recently been highlighted in the media. Thus it is imperative that healthcare administrators understand the limits on improvement of information accuracy resulting from HIPAA and make appropriate plans to use HIPAA as a starting point from which to build. To date, discretionary adoption and use of information technology designed to improve information integrity is slow. A study by a team from Boston's Brigham and Women's Hospital indicates that only 19% of respondents in a study of information integrity in emergency rooms said they bought technology to check doctors' orders for errors and only 38% of those respondents said that they fully implemented it.[1] Accuracy is clearly an important issue when addressing information integrity. Ensuring accuracy is a challenge that many institutions have yet to properly address. This challenge will be discussed in greater detail later in the article.

2.2 Information integrity and HIPAA's data processing requirements

The first phase of HIPAA implementation, the transaction and code set (TCS) standards, was finalised following a lengthy public comment period and required some healthcare organisations to be in compliance as early as October 2002. Small health plans, defined by the Department of Health and Human Services (DHHS) as those having less than 50 members, have until October 2003 to comply, but large healthcare organisations should have been in compliance since October 2002, unless they filed for an extension. Table 1 contains a list of current TCS standards. Each TCS standard delimits a set of data item definitions and corresponding allowable data values that are required in order to exchange information between business partners.

Table 1 EDI standard transactions

Transaction number	*Description*
837	Health claims or equivalent encounter information or coordination of benefits.
270/271	Inquiry/response concerning eligibility for a health plan.
278	Referral certification and authorisation.
276/277	Inquiry/response about the status of a healthcare claim.
834	Enrollment or disenrollment in a health plan.
835	Healthcare payments and remittance advice.
820	Health plan premium payments.

The transmission standards adopted in the TCS rule of HIPAA are based largely on well-known standards for EDI that have been used by large manufacturing, product distribution and retail organisations, collectively known as consumer packaged goods industries, since the 1970s. Table 2 depicts an example of an EDI transaction representing a response to an inquiry about eligibility for a health plan under HIPAA. The terse representation contains mandated data item fields as well as the data containing Robert Smith's eligibility request.

Table 2 Sample EDI message for transaction code 271[4]

```
ST*271*1234
BHT*0022*11**19950101*1319
HL*1*0*20*1
NM1*PR*2*ABC COMPANY*****PI*842610001
HL*2*1*21*1
NM1*1P*2*BONE AND JOINT CLINIC*****SV*2000035
REF*N7*234899
N3*55 HIGH STREET
N4*SEATTLE*WA*98123
HL*3*2*22*0
TRN*2*93175-012547*14-1726485
NM1*IL*1*SMITH*ROBERT*B***MI*11122333301
REF*1L*599119
DMG*D8*19430519*M
INS*Y*18
EB*1*FAM*30*GP
DTP*307*RD8*19950501-19950515
SE*18*1234
```

Since EDI standards have been in use for several decades, they are well understood and many of the technical and managerial lessons learned by consumer packaged goods companies are directly applicable to healthcare companies. However, while the maturity of EDI can improve implementation efficiencies, the potentially bad news is that EDI is a technically rigid standard best suited to the large, centralised systems architectures popular in the 1970s. While these older architectures still exist in healthcare, as well as consumer packaged goods, more efficient methods for standardising data and forms have emerged that are better suited to modern, decentralised systems architectures that represent a larger percentage of the systems in use by companies today.

2.3 XML and EDI in healthcare

A popular method of data standardisation for modern systems architectures is use of eXtensible Markup Language (XML) to translate data codes into information with standardised meaning. Absent designation of specific XML standards in HIPAA, many healthcare companies with modern systems architectures are engaging in double data standardisation processes. Data is first standardised using the mandatory EDI classifications for compliance purposes and then translated again into XML for better data handling by the more modern systems architectures. Table 3 shows how one line in the EDI example of Table 2 might appear in an XML transaction.

Table 3 XML translation of one line in sample transaction 271[5]

EDI Transaction Line	NM1*1P*2*BONE AND JOINT CLINIC*****SV*2000035
XML Equivalent	</Hierarchical-Level> <Individual-or-Organisational-Name> <Entity-Identifier-Code Code= “1P Provider”/> <Entity-Type-Qualifier Qual= “2 Non-Person Entity”/> <Name-Last-or-Organisation-Name>BONE AND JOINT CLINIC</Name-Last-or-Organisation-Name> <Identification-Code-Qualifier Qual= “SV Non-Person Entity”/> <Identification-Code>2000035</Identification-Code> </Individual-or-Organisational-Name>

In healthcare, many consulting firms have emerged that apply XML standards on top of the mandated EDI standards to improve information sharing. Information integrity issues may ensue in this scenario. Since standard XML data definitions have not been developed and matched to the HIPAA EDI standards, the unique identifiers and coding schemes employed via XML by one healthcare company may or may not resemble the HIPAA EDI standards and also may or may not resemble the XML data coding schemes used by another healthcare company. Thus, coding schemes may potentially become more complex than ever, although this will not necessarily be the case. In addition, the act of translating data twice subjects the data to potential accuracy problems. Just like the information passed along during the childhood gossip game where person B tells person C something they heard from person A, data that is translated and coded twice is subject to a higher likelihood of misinterpretation or error.

3 Data quality

The quality of data entered into healthcare systems is another important issue to address. Poor data quality is costly. It lowers customer satisfaction, adds expense, and makes it more difficult to run a business and pursue inter-organisational information integration and internal business process improvements. According to Thomas Redman, 1–5% of corporate data contain errors and organisations lose 8–12% of their potential revenue directly attributable to information quality problems (Redman, 1998). In a study of customer data errors in the US insurance industry, InformationWeek reports that an average of 2.55% of customer records contained name-related errors, 15.50% were duplicates, 0.92% contained address errors, and 1.09% had missing relationships (Information Week, 1999). Error rates like these would prove costly for health insurers and providers alike. If minimal error rates could be obtained for healthcare data, it is likely that patients would benefit from lower costs and unnecessary procedures as well.

4 Electronic medical records

HIPAA legislation is one step toward the development of universally standardised electronic medical records (EMR) for patients that may be shared across multiple providers, insurers and other authorised entities. Because the ultimate goal of EMR is to have one point of entry for information that is shared among many entities, it is critically important that organisations have information integrity checks on data at the points of entry. While standardisation of key codes will help with data quality, there are still numerous opportunities for errors in data entry, including transposition of numbers in key fields and incorrect information entered in non-standardised fields. At the same time, in the absence of EMR, manual re-entry of data from one organisation to the next, across trading partners, increases the opportunity for data entry error, but reduces the number of users exposed to such errors to only users inside one organisation. Thus, electronic sharing of information under HIPAA increases data quality on one level, but leaves the door open for new systematic problems with data quality.

Research on the privacy and security issues related to electronic patient records predate HIPAA implementation. Buckovich *et al.* (1999) derived a set of guiding principles to protect electronic patient records, and noted that almost half of them could be addressed with appropriate technology. A report by Connecting for Health, a group of healthcare leaders supported by a private philanthropy, has proposed that a set of de facto standards for medical information sharing be adopted as a national standard. According to David Liss, VP of government relations at New York-Presbyterian Hospital, ‘You have to have interoperability for clinical health information, otherwise it cannot be shared, and standards are the linchpin of interoperability.’ (Information Week, 2003). The report also projects a set of best practices for privacy and security, and states that best practice examples take HIPAA as a minimum requirement in this area.

4.1 Web technology use and integrity

Yet another information integrity issue related to the new TCS standards is the choice of information technologies selected by individual healthcare entities for implementation of HIPAA requirements. Web technologies can provide value to healthcare organisations in their HIPAA compliance effort. According to a College of Healthcare Information Management Executives (CHIME) survey of CIOs, 85% of respondents said that they intend to use the internet in their HIPAA compliance efforts (Gue, 2001).

High usage of the internet is due to lower cost of infrastructure as well as the ubiquitous availability of the internet for creating inter-organisational connections. Yet the public nature of the internet means that virtual private networks (VPNs) and other methods of security are necessary for ensuring security of information.

4.2 Unique identifiers and integrity

The proposed rule on unique identifiers will require healthcare providers and employers to use Individual Healthcare Identifiers. Employers will use their Federal Employer Identification number (FEIN) and providers will use a 10-digit number assigned by the Healthcare Financing Administration (HCFA). Unique identifiers for individuals (i.e. National Patient ID) are not currently mandated in the proposed rule, but may be part of the final regulation.

Unique identifiers share similar characteristics with the TCS standards, in that they mandate the use of a common format and data value set. With this added requirement, communications with business partners are improved, as the probability of reaching a legitimate and correct business partner increases. Automated audit checks can be put in place to ensure, at least, that unique codes are valid within specified parameters. Perhaps the greatest information integrity risk here is that unintentional data entry error is higher for fields such as ten-digit identifiers than it is for fields containing logical information such as procedure description. Cross validation, such as confirmation of procedure type or physician name with identifier codes, will ensure better data accuracy.

To summarise, as information integration efforts are being implemented, information integrity issues must be managed at the following levels:

- data entry and subsequent data modification
- information storage and retrieval methods
- data transmission to external constituents.

4.3 Information integrity and HIPAA's data protection requirements

The privacy requirements were issued to protect the confidentiality of a specific subset of patient data known as protected health information (PHI). PHI is defined as any individually identifiable health information, created or received by a covered entity. HIPAA designates PHI as past, present, and future physical or mental health of an individual, condition of an individual, provision of healthcare, and past, present, and future payment for the provision of healthcare. Specific PHI record elements include name, address, employer, relatives' names, date of birth, telephone number, e-mail address, IP address, social security number, medical record number, member or account number, photos, voice, fingerprints, vehicle or other device serial number, certificate/license number, admission date, discharge date, date of death, any age over 89, health plan beneficiary numbers, and any other unique identifying number, characteristic or code. The final Privacy Rule was passed in April 2001 requiring covered entities to be in compliance by April 2003. The rule applies to health information in all forms, including electronic, oral and paper.

The original draft of the privacy rule called for patient consent before information could be released beyond the treating physician and the insurer. However, in the final version of the rule, legislators removed the consent requirement, stating that it was deemed an administrative burden to patients, physicians and insurers. This change in the privacy rule has been quite controversial and several lawsuits are currently pending in efforts to reinstate the patient consent requirement. Opponents of the final ruling, including a national patient advocacy group called 'Citizens for Health' argue that the Rule:

> "eliminates the right of citizens to control the use and disclosure of their personal health information for most purposes and grants blanket 'regulatory permission' to thousands of entities (insurers, clearing houses, law firms, consulting firms, billing and collection firms, potential purchasers, and many others) to gain access to that information without the citizen's knowledge or consent and even against his or her wishes." [2]

4.4 HIPAA's privacy rule and PHI integrity

Interesting information integrity issues surround this controversy and the outcome of the pending lawsuits will have a great impact on the processing and management of PHI. In particular, there are a number of ways that the handling of PHI can affect information accuracy. First, and perhaps most simply, patient consent increases the likelihood of ethical use of patient data and acts as an informal but effective oversight function for use of health data. Under the current legislation, employers, pharmaceutical associates, and groups performing controversial health information research may be more likely to use their authorised access for questionable purposes if patient awareness and consent are waived.

Here are several possible scenarios related to one simple example. If a research organisation could collect patient information from multiple sources across the country without consent or verification, it would be much easier to amass large databases of information around a common phenomenon, such as the effectiveness of a particular new drug on the treatment of an ailment such as ulcers, cancer, or AIDS. If information from all of these sources is standardised and data is input with reasonable accuracy, then study findings may lead to a quicker understanding of the benefits and problems related to use of that drug. On the other hand, if, as described earlier, data goes through two or more transformations before entering a database for research without any independent verification, the odds of data inaccuracies increase, making the results of the study less reliable. Yet the large-scale effort may falsely lend credibility to the study, which may have misleading and potentially devastating implications for either the pharmaceutical company or the patients taking the drug. In an even less desirable scenario, a research organisation with questionable ethics will find it easier to change a few values in data records here and there to manipulate study outcomes to obtain results favourable to a pharmaceuticals company sponsoring the study. It would be nice to think that this is a far-fetched scenario, but now-infamous companies like Enron, Arthur Andersen, Worldcom, and Tyco provide ample evidence that a precursor to unethical use of data is the absence of adequate checks and balances on data input for decision-making purposes.

From a data management perspective, organisations that share information often make copies of data for legitimate purposes, but then may modify records according to their own internal needs. Data warehouses combine data from multiple sources and possibly different points in time. Individuals often download data sets for personal access or analysis, and don't retain the original data values or replace updated fields over time. In the absence of guidelines for update and maintenance of individual records, ubiquitous sharing of patient data can lead to confusion regarding which copy of a patient's record is most up to date or most accurate.

4.5 De-identification of PHI and information integrity

Yet another issue related to privacy is the assurance of effective de-identification of PHI. Nineteen elements must be removed in order for PHI information to be shared with research organisations, and other organisations beyond the immediate care providers. Such de-identification is likely to take place electronically. Information integrity problems may occur if private information is entered in the wrong fields, the wrong fields are selected for de-identification or if the de-identification software malfunctions and skips records for cleansing, skips fields because of poor formatting (e.g. if the field begins with a space), etc.

De-identification may also act as an indirect incentive to manipulate data files in order to increase the likelihood of a particular research outcome. Once the data is de-identified, it becomes much more difficult to audit the accuracy of the remaining record information, especially if patients are unaware of their information's participation in a study. Currently, no safety mechanisms are in place to protect the integrity of de-identified health data.

The privacy and security rules are closely linked and designed to be compatible; however there is a distinction between the two. While information can be secure without being private, it is impossible for it to be private without being secure. Where privacy deals with the patient's specific rights regarding his or her own personal health information, security affects the efforts that an organisation must take to protect and control access.

4.6 HIPAA's security rule and information integrity

HIPAA security requirements govern physical access control, security officer designation, control of hardware and software, chain of trust agreements, internal audit, security incident procedures and a security management process. As the last of the regulations to be passed, compliance is not mandated until April 21, 2005. The security rules will have an impact on both the organisational and technical policies and procedures of healthcare entities. The security rule component is intended to provide a consistent level of protection for healthcare information and includes both mandatory and discretionary implementation features. Organisational practices, such as documented security policies, assignment of a security officer, ongoing education and training, employee background screening and violation sanctions, will be required. Required technical practices that must be implemented include authentication, access controls, and audit trails, physical safeguards, disaster recovery plans, and external system access protection. While HIPAA has determined what an organisation must do to provide security of health information, it does not dictate how it must be done. Moreover, HIPAA does not provide for specific technology to be implemented, enabling the healthcare organisation to apply measures that are appropriate to its size, needs and infrastructure. The standards proposed by DHHS for securing health information have been designed to be technology neutral in order for organisations to address their specific business needs and to provide flexibility for incorporating state of the art security features and products. DHHS sought the input and feedback from many industry experts in the area of security during the proposed regulation development process.

The security regulation also requires organisations to identify areas of vulnerability and level of risk and furthermore requires the implementation of a plan to minimise this risk. This means an organisation must identify and assess its risks and then implement controls to reduce the possibility of their occurrence. Risk is the 'possibility that an event or action will cause an organisation to fail to meet its objectives (or goals).' (Gelinas and Sutton, 2002, p.212). An organisation must assess the level of risk it is willing to assume while considering the potential business exposure that could result. HIPAA states that the security policy should be reasonable, scalable and justifiable; therefore an organisation should undertake a cost, benefit and risk analysis to select specific levels of security measures and standards for their organisation. An example in the proposed rule cites the vast differences that a small, rural physician practice and a large health plan would have in their contingency plans for system emergencies. Where the small office would have only a few pages of policy on addressing diskette storage and computer back up procedures, a large health plan or provider would have multiple volumes to address issues including off-site storage of electronic media (Department of Health and Human Services, 1998). However, the minimum standards identified in the proposed rule must be implemented by all covered entities.

Risk management also refers to the way in which partnering organisations share risk in inter-organisational relationships. To offset the potential of a security or privacy infraction, some healthcare organisations are assessing the need for cyberinsurance, insurance policies that protect against civil lawsuits. Others are seeking strengthened contracts with software vendors and IT suppliers that cover responsibility for software flaws that result in privacy breaches (Willoughby, 2003).

Security of data has surfaced as an issue in the current healthcare environment due to the increase in use of electronic versus paper medical records. The consolidation of the industry into integrated delivery systems requires secured, electronic sharing of health data among network providers. The proliferation of interactive patient medical charts, wherein the patient is allowed to access and amend a 'designated record set' which includes enrollment, payment, claims and medical records, will bring the issue of security to the public forefront. Several researchers have already studied the use of interactive patient charts, concluding that it is difficult to provide an adequate degree of access while meeting both security and ease-of-use demands of patients and medical staff (Ross, 2003; Masys *et al.*, 2002; Prady *et al.*, 2001).

Clearly, security is not just a technology issue. Technology-based controls can inhibit intrusions by someone outside the organisation who tries to penetrate internal systems. But even when the tightest IT controls have been put in place there are still ample opportunities for infractions that result from unauthorised physical intrusion when personnel are not aware of HIPAA-conforming policies and procedures. Even more common are infractions caused by unintentional misuse of information by healthcare personnel (usually improperly trained or incented personnel), or intentional and/or criminal misuse by personnel.

As is the case with privacy requirements, revised or new policies and procedures must be implemented across a wide range of processes and jobs to govern the human aspects of these regulations. Policies, education, training, measurements, and reward systems must be implemented on an enterprise level requiring a commitment from top leadership in the organisation, including the CEO and CIO. The importance of cultural and attitudinal changes cannot be overemphasised. Thomas Hanks, co-chair of security and privacy for WEDI believes that 'The largest threats to data security come from employees who do not follow an organisation's procedures, or who are not properly trained. About 90% of security is between the ears. There is not enough technology we can buy to protect our information without cultural change.' (Goedert, 2001).

The integrity of security controls put in place will have an impact on consumer trust of organisations. Unfortunately, one breach of such trust may have a devastating effect on e-health initiatives. Therefore, a comprehensive yet affordable plan is needed within each healthcare organisation and across all partnerships and alliances to ensure that public trust is maintained. And given that HIPAA changes are likely to be ongoing, it will be important to information integrity to conduct frequent audits of information transmission, data storage, and all the other components of the HIPAA strategy to ensure that the organisation remains in compliance and continues to meet the expectations of the public it serves.

5 Practitioner implications

HIPAA is costing billions of dollars, and its benefits are yet to be observed or understood. As the legislation's reality unfolds, healthcare organisations and other involved parties should strive to achieve the highest level of benefit from the implementation choices they make. Yet the benefits are slow to come, and the costs in both time and money continue to mount. Newspaper articles abound with stories of unintended consequences of the legislation (Stockman, 2003). With such a wide impact, administrators and medical staff are rightly concerned that their organisations adopt the best possible response to the legislation. While we cannot prescribe a 'one size fits all' solution to the challenges HIPAA presents, this article does present a number of important issues concerning the quality and integrity of the information protected by the regulations.

Approaches to addressing HIPAA will range dramatically depending on the systems, procedures and controls already implemented, and the size and complexity of information sharing within and between organisations. Early adopters of HIPAA solutions, who are willing to share their plans, results, and mistakes with others in their industry, can help partner organisations and other healthcare providers control escalating healthcare costs and aid continued improvement in information integrity. Trade press publications can provide leads on solutions to specific organisational shortcomings. Nonprofit organisations, such as URAC and the Healthcare Information and Management Systems Society, are working to provide generic guidelines and best practice examples as implementation guides (Vijayan, 2003). However, absent careful study and analysis of the impacts of particular approaches and interventions, practitioners must make expensive and vital decisions about the best approach to adopt to meet their own organisations' needs.

6 A call for field research

Healthcare researchers can help by conducting field studies of early adopters, focusing on the impact of HIPAA on the integrity of information maintained by organisations and shared with their partner firms. We echo Wen and Zhang (2002) in their call for research to document the real impacts of the legislation. They present a framework for identifying privacy issues within the confines of HIPAA, and challenge the research community to assess the technical, managerial and legal issues within it.

Building on existing studies of information quality and standards issues,[3] field research could identify best practices in information integrity, as well as present cost – benefit comparisons of competing approaches. Other topics of interest might include:

- Challenges to implementing HIPAA and what organisations have done to overcome them – examples of potential challenges are:
  - converting data to a standard format
  - converting paper to electronic data
  - technology required to store, transfer and secure data (update or replace existing systems)
  - identifying appropriate personnel to maintain systems, ensure compliance
  - cost to develop security processes (procedures to ensure that the rules are being followed with respect to securing personal and medical information of patients)
  - cost to develop privacy processes
  - consulting costs.
- The expected benefits of HIPAA compliance and the extent of the benefits – examples of potential benefits are:
  - medical efficacy (and why – speed of access to patient information, ability to view entire patient history more readily, ability to spot trends for groups or individual patients, ability to share patient information more readily with other physicians, etc.)
  - administrative efficiency (and why – reduced errors in billing, reduced time spent with paper work, reduced time in data entry, etc.)
  - decreased costs
  - HIPAA presents a platform for building other e-business opportunities.
- The expected impacts of HIPAA compliance on:
  - timeliness of patient care
  - insurer/provider relationships
  - insurer/employer relationships
  - insurer/patient relationships

  - risk to patient record privacy
  - risk to patient record security
  - data integrity
  - data availability.
- Interaction of HIPAA compliance of the target organisation with other elements of the organisation's business and business relationships:
  - changes to business processes as a result of compliance
  - effect of business processes on compliance
  - changes to relationships with partner organisations as a result of compliance
  - effect of relationships with partner organisations on compliance
  - changes to business processes of partner organisations as a result of compliance
  - effect of partner organisations' business processes on compliance
  - effect of partner organisations' information systems architectures and infrastructures on compliance decisions of target organisation.

This list begins to develop a framework for analysis that will be needed to understand the impacts of HIPAA on information integrity. The reader is encouraged to join us in participating in the discovery and creation of exemplars of how individuals, organisations and indeed, the nation may best benefit from the intended and unintended consequences of HIPAA compliance.

References

Brewin, B. (2003) 'New HIPAA security rules could open door to litigation', Computerworld. Available from: www.computerworld.com Quicklink 36500, February 20, 2003.

Buckovich, S.A. Rippen, H.E. and Rozen, M.J. (1999) 'Driving toward guiding principles: a goal for privacy, confidentiality and security of health information', *Journal of the American Medical Informatics Association*, Vol. 6, No. 2, pp.122–133.

'Department of Health and Human Services: Security and Electronic Signature Standards: proposed rule', *Federal Register*, August 12, 1998.

Goedert, J. (2001) 'The first step toward security', *Health Data Management*, New York.

Gue, R. 'Where HIPAA and e-health strategies meet', HIPAA Advisory. Available from: http://www.hipaadvisory.com/action/strategies/, accessed October 6, 2001.

Hellerstein, D. (2001) 'HIPAA where do providers stand?' *Healthcare Management Technology*, January, Vol. 22, iss. 1, pp.14–17.

InformationWeek Online (1999) 'Innovative system's comparative data assessment'. Available from: www.informationweek.com/cdq/table.fhtml.

InformationWeek (2003) 'Health-care needs standards for sharing data', *InformationWeek*, 2003, Available from: www.informationweek.com/story/showArticle.jhtml?articleID=10300268.

Masys, D., Baker, D., Butros, A. and Cowles, K.E. (2002) 'Giving patients access to their medical records via the Internet: the PCASSO experience', *Journal of the American Medical Informatics Association*, Vol. 9, No. 2, pp.181–191.

Prady, S.L., Norris, D., Lester, J.E. and Hoch, D.B. (2001) 'Expanding the guidelines for electronic communication with patients: application to a specific tool', *Journal of the American Medical Informatics Association*', Vol. 8, No. 4, pp.344–348.

Redman, T. (1998) 'The impact of poor data quality on the typical enterprise', *Communications of the ACM*, Vol. 41, No. 2, pp.79–82.

Ross, S.E. (2003) 'The effects of promoting patient access to medical records: a review', *Journal of the American Medical Informatics Society*, Vol. 10, No. 2, pp.129–138.

Stockman, F. (2003) 'Patient privacy laws seen as barrier to law enforcement probes', *Boston Globe*, p. B12.

Ulric J. Gelinas, Jr. and Sutton, S.G. (2003) Accounting Information Systems, 5th edition, Cincinnati: Southwestern.

Vijayan, J. (2003) 'Guidelines for HIPAA compliance in the works', *Computerworld*. Available from http://www.computerworld.com/security topics/privacy/story/0,10801,87492,00.html accessed as of May 17, 2004, publication date, November 24, 2003.

Wen, K-W. and Zhang, Y.J. (2002) 'Research issues on medical information systems facing the implementation of HIPAA', *International Journal of Healthcare Technology and Management*, Vol. 4, Nos. 1/2, pp.93–105.

Whitman, M. and Mattord, H. (2003) Principles of Information Security, Canada: Course Technology, p.13.

Willoughby, M. (2003) 'New regulations have companies turning to risk management', *Computerworld*. Available from: http://www.computerworld.com, QuickLink 38940.

Notes

[1] http://www.bizjournals.com/industries/health_care/hospitals/2003/08/18/boston_newscolumn1.html

[2] www.medicalprivacycoalition.com

[3] See, for example, the proceedings of the annual MIT Information Quality Conference, Cambridge, Massachusetts, USA.

[4] http://www.redix.com/hipaa22211.htm.

[5] http://www.redix.com/hipaa22211.htm.