Global Information Assurance Certification Paper

Offshore Outsourcing and Information Confidentiality

Foreign Practices and US Laws: Trends, Incidents, and Possible Solutions

Mark Lum
GSEC Practical Assignment
Version 1.4b Option 1
April 2004

TABLE OF CONTENTS

ABSTRACT	1
1 INTRODUCTION	2-3
2 TYPES OF INFORMATION BEING MOVED ABROAD	3
3 RECENT INCIDENTS	3-4
4 HIPAA AND GLBA: DATA PRIVACY	4-8
5 THE EUROPEAN DATA PRIVACY INITIATIVE	8-10
6 OTHER FOREIGN PRIVACY LAWS AND TRENDS	10-11
7 U.S. LAWS FALL SHORT	11-12
8 U.S. LEGISLATORS CALL FOR TOUGHER LAWS	13-14
9 SOLUTIONS	14-18
10 CONCLUSION	19-20
ENDNOTES	21-24

ABSTRACT

While recent news headlines of the past few months have focused on the controversial topic of offshore outsourcing of jobs from the United States to countries such as India, China, and Mexico, other headlines, relating to some of the effects of this phenomenon, have exposed problematic consequences and outcomes.

Some of the work moved abroad involves the transfer of large amounts of sensitive data, including financial records, Social Security numbers, and health records. One of the effects of this phenomenon has been the breach of confidentiality and the abuse of those records. While these criminal acts are covered under US and foreign laws, the lack of international convention and agreement (and in some cases the lack of enforcement) has left American consumers exposed, has raised questions of appropriate legal jurisdiction, and has raised the issue of accountability among the parties responsible for the information.

In light of some recent incidents, both American and foreign legislators are trying to address these questions and to close the legal gaps. Some companies are implementing technical and procedural steps to prevent the abuse of sensitive data.

While these trends are very recent and encouraging, the potential for abuse still exists. Perhaps, if there is some conformity in regulations and remedies, full disclosure of policies, procedures and incident reporting, and a recognized standard of technical safeguards -all provided by both American and foreign data privacy laws- only then will consumers feel some sort of assurance.

1 INTRODUCTION

The recent phenomenon of outsourcing of jobs from the United States to countries such as Mexico, India, Pakistan, and China has been, undoubtedly, controversial. The pain of lost jobs, however, has overshadowed other tangential and problematic aspects of this shift. Many of the lost jobs are the "back office" tasks handling copious amounts of sensitive information, including Social Security numbers, credit records, medical records, and other financial information.

While there are broad Federal and state laws that address the issues of information privacy, confidentiality, and the abuse of such data, the Internet is not bound by international borders, and American laws have limited influence in foreign countries. Those two factors then raise questions about the precarious nature and the potential flaws of sending sensitive data outside the United States.

These concerns were realized in October, 2003 when a disgruntled Pakistani medical transcriber posted the medical records of several patients at the University of California, San Francisco (UCSF) on the Internet. Upset at the lack of payment for her services, the transcriber sought to force the issue by compromising the information. (1)

The incident revealed that information sent offshore is prone to breach of confidentiality, that the obligations of those responsible for the integrity of the information are not well defined, and that consumers are not well informed of the potential problems or the actual incidents. The subjects of computer security and related law enforcement in India and Pakistan have been called into question, but the same issues can then be focused to other countries where work is likely to be outsourced and the subjects of computer security and law enforcement are equally questionable.(2)

Recent incidents have reinvigorated the debate over issues of information privacy and confidentiality in several areas. Firstly, the efficacy of current American laws is under new scrutiny. Secondly, the gaps among the laws of the United States, the European Union, and countries popular for outsourced services have become prominent points of scrutiny. As a result, some American politicians have introduced new pieces of stringent legislation that provide clear guidelines, strict accountability, and penalties in order to keep such incidents from occurring. Some foreign countries lacking tough legislation are beginning to implement laws to meet American and European standards.

The beneficial effects of legislation cannot happen quickly enough, and legislation is only one aspect of preserving the confidential nature of sensitive data. If enacted, some recent proposed legislation will impose strict regulations regarding the confidentiality of information, especially with regard to information outsourced to a foreign country. In order to meet these regulations and to maintain consumer confidence, American companies, privacy advocates, and information security professionals are looking at various methods, procedural and technical, to provide a higher level of security and assurance as more sensitive data are inevitably moved

abroad.

2 TYPES OF INFORMATION BEING MOVED ABROAD

Among the types of work being sent abroad over the past few years, data maintenance and processing tasks have become popular choices. These jobs handle sensitive data, including names, addresses, Social Security numbers, credit information, medical records, and other financial information. Countries processing all of this information include well-known destinations such as India, China, and Mexico, but also lesser known locales such as Jamaica, Ghana, and Guatemala. (3)

The trend is not forecast to slow down soon. Eighty six percent of executives surveyed believe that the trend to offshore outsource IT related work will increase dramatically. (4)

Oddly enough, the trend of outsourcing, while seemingly recent, had been forecast over five years ago. Pressure on companies to contain costs, to run efficient operations, and, ultimately, to boost shareholders' stock value is seen as the driving force behind the trend of offshore outsourcing. (5) The quest to contain costs is not limited to corporations or private companies either. Twenty nine out of forty one agencies in Washington state have sent jobs offshore. (6)

The inexorable trend of sending sensitive data has no end in sight. Americans are only now becoming aware of the potential problems of this practice as a few incidents have recently come to light. In the midst of this, consumer privacy advocates and legislators have begun to question the lack of control over sensitive information, the potential for abuse of data, and the ability to guarantee the confidentiality and integrity of work sent offshore.

3 RECENT INCIDENTS

Even as concern about the amount of data being sent offshore has grown, several incidents involving the abuse of confidential, private information have occurred within the past year, fulfilling the worst fears of some consumers, legislators, and privacy experts. The incidents highlight the problems inherent in offshore outsourcing, the inability of U.S. laws to provide remedies, and the lack of procedural and technical controls by the parties outsourcing the data.

In October 2003, Lubna Baloch, a Pakistani transcriber, threatened to post the medical records of several University of California San Francisco Medical Center (UCSF) patients on the Internet. The medical records had come into Baloch's possession by way of a several American subcontractors. When compensation for her work did not arrive from the subcontractor, Baloch sent a threatening e-mail to UCSF. (1)

Reaction has been swift. Baloch has not received any further work from American sources. The American subcontractors hired by UCSF have also seen their work disappear. Legal action is pending against at least one of the American subcontractors.

In the same month, several offshore workers, based in Bangalore, India, employed by Heartland Information Services of Toledo, Ohio threatened to expose confidential information unless they received a cash payment. The officers of Heartland Information Services failed to notify clients and did not mention this incident when testifying before California legislators later in March of this year. Stewart Mandell, the head of HIS, denied any obligation to disclose the incident because training documents, not medical records, were stolen. (7)

In January of 2004, Wipro Spectramind, a New Delhi based telemarketing subcontractor for Capital One Financial Services, apparently lost its contract after an audit discovered that Wipro employees were, among other things, inflating credit terms available to customers. (8)

Although a Wipro audit had characterized the problem as “unacceptable practices,” it is clear that the employees were basing their actions on available customer credit information. Wipro took action, firing approximately thirty workers who worked on the Capital One account. However, after initial reports that Capital One had severed its ties with Wipro, other reports indicate otherwise. (9)

In each case, the status of the workers, either as a subcontractor or a direct employee, did not prevent the threat.

4 HIPAA AND GLBA: DATA PRIVACY

Considering the incidents noted in the previous section, the natural question to ask would be how the laws of the United States cover privacy issues and provide remediation when privacy is compromised.

For the sake of brevity and simple comparison, this section focuses only on the basic provisions of existing Federal statutes that address privacy issues in the two most sensitive types of information being sent abroad: medical records and financial records. This section is not intended to be a detailed examination of the mandates of either act. Rather, a few highlights are noted to provide how privacy is addressed, how information is used or accessed, and how information is secured.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses medical information privacy issues. The Gramm-Leach-Bliley Act of 1999 (GLBA) addresses financial information privacy issues.

HIPAA limits how patients' medical information can be used by health plans, hospitals, and others defined as covered entities, e.g. pharmacies. HIPAA also covers the transmission of information: written, orally, and electronically. (10)

The Gramm-Leach-Bliley Act of 1999 (GLBA) addresses financial information privacy issues. GLBA covers privacy in three broad ways, the Financial Privacy Rule, the Safeguards Rule, and Pretexting. (11) (12)

The following tables provide a quick, simple, comparative overview of some of the provisions in HIPPA and GLBA.

The first table compares how definitions shape HIPAA and GLBA. The definitions drive how HIPAA and GLBA are implemented. (10) (11) (12)

Important Definition Distinctions Between HIPAA and GLBA

HIPAA	**GLBA**
HIPAA defines the obligations of those who provide service and are responsible for patients' information.	GLBA defines the rights of those who receive services.
Covered entities are responsible for patients' information and its confidentiality.	*Consumers* are considered to be anyone who has obtained a financial product or service for a personal reason.
Hospitals and HMOs are typical examples of covered entities. *Contractors* are third parties that might handle confidential information covered by HIPAA.	*Customers* are defined as those who have a continuing relationship, e.g. a mortgage or brokerage account, with a financial company,
Contractors are not automatically bound by HIPAA. Specific terms in a contract between covered entities and contractor might bind a contractor to HIPAA's obligations.	*Customers* are entitled to automatic receipt of a financial company's privacy policy, on an annual basis, for as long as the relationship lasts.
	Consumers only receive notification of a financial company's privacy policy if the company shares information.

HIPAA clearly defines the covered entities and applies the mandates to them. However, contractors are not bound by HIPAA unless contractually obligated. HIPAA makes no distinction in its definition of a patient. In contrast GLBA makes a distinction between customers and consumers, giving greater leeway to financial companies in terms of privacy policies, notification, and the sharing of information with other parties.

The second table compares how HIPAA and GLBA address privacy of confidential information, the sharing of such information, and any other privileges. (10) (11) (12)

Privacy of Confidential Information under HIPAA and GLBA

HIPAA	GLBA
Covered entities may not use patients' information for marketing purposes. Patients must specifically authorize this.	Financial companies may share information with third parties that do data processing or account maintenance.
Covered entities must provide a notice of privacy practices, the use of medical records, and patient's rights, usually upon a patient's first visit.	Financial companies may share information with marketing, Neither consumers nor customers may opt out of this.
Covered entities must provide written procedures addressing who has access to information, how it is accessed, how it will be used, and when it will be disclosed.	Financial companies must provide a clear privacy policy. The policy should note what information is shared, how it is collected, and with whom it is shared.

With regard to the use of private information for marketing purposes, it is important to note that HIPAA requires patient authorization. Conversely, GLBA allows this and denies consumers and customers the right to prohibit or opt out of this feature. It is also important to note that HIPAA and GLBA provide penalties, including fines and imprisonment, when information is abused, both unintentionally or purposely. HIPAA and GLBA also mandate that notice must be given when information has been compromised.

The third table briefly compares the security provisions and techniques that HIPAA and GLBA mandate for their subjects. Many of the techniques and procedures are comparable and are considered to be part of the best practices in information security. (13) (14) (15)

Security Provisions under HIPAA and GLBA

HIPAA	GLBA
A broad security standard applies to all entities, public and private, large and small. The standard is technology neutral, comprehensive, and scalable.	Financial companies must perform risk assessment to identify threats, vulnerabilities, and the likelihood of such.
Administrative procedures need to address processing of records, configuration of security, personnel, training, documentation, etc.	A policy to mitigate risk, using technology, procedures, and training must be formed.
Security techniques employ access controls, encryption, passwords, and many other forms of authentication.	Security controls, including encryption, access control, detection and response, must be implemented to maintain confidentiality, integrity and access.
Alarms, event reporting and notification and audit trails need to be used if data are transmitted over a network.	Security must be monitored continuously to prevent harm to sensitive data.

It is worthy to note that HIPAA and GLBA seek to define a broad scope of procedures to address the likelihood of compromised information.

Both HIPAA and GLBA provide civil and criminal penalties when information is breached. HIPAA may impose civil fines from $100 per violation up to $25,00 per annum. Criminal penalties, assessed when information is knowingly compromised, may range from a $50,000 fine and one year of imprisonment to a $250,000 fine and ten years of imprisonment. GLBA assesses penalties under Section 8 of the Federal Deposit Insurance Act. Fines can reach $1,000,000 and prison terms may range from five to ten years. (10) (11) (12)

GLBA also forbids “pretexting.” Pretexting is the use of false pretense in order to gain information, usually names, addresses, Social Security numbers and other sensitive, personal information. Rather than exploiting the information, pretexters sell this information to others who usually do so. GLBA forbids the use of stolen, false, forged or fraudulent documents or statements to gain information. This rule also forbids using another party to accomplish the same tasks. Penalties also fall into the range of five to ten year prison terms. (12) (16)

HIPPA restricts the flow and use of sensitive data to a greater degree than GLBA. However, GLBA allows information to flow more freely, based on the distinction of definitions of *consumer* and *customer*. The biggest difference, perhaps, is that GLBA distinctly allows the use of private financial information for marketing

purposes.

Both HIPPA and GLBA have admirable sets of mandates to address how information needs to be secured in order to maintain the privacy of individuals. In spite of these apparent safeguards, we have experienced recent incidents.

5 THE EUROPEAN DATA PRIVACY INITIATIVE

Although the regulations, stipulations, and penalties of HIPAA and Gramm-Leach-Bliley seem to be well defined, these two regulatory statutes cannot compare favorably with the European Data Privacy Initiative of 1995. Of all the data privacy laws in the world, the European Data Privacy Initiative is widely regarded as the most stringent with regard to the use and flow of private, confidential information. (17)

First and foremost, all citizens within the European Union enjoy equivalent protection under this law. In addition, individual countries within the union may alter the law to increase privacy and to suit their own needs. The directive applies to any operation performed on a set of personal data. The operations include the collection, storage, and disclosure of data in automated (computer database) and non-automated filing systems. Data kept for personal reasons (e.g. a diary) is exempted. The directive also provides exemptions when law enforcement, public security, and defense issues arise.

Definitions from the European initiative are relatively simple and broad. Whenever a person discloses any personal information, e.g. an application, she becomes a *data subject*. Any entity, regardless of being a person or a body, that "determines the purposes and the means of processing, both in the public and in the private sector," is a *data controller*. (17)

Data controllers bear the brunt of regulation and must observe the rules of the country where the data controller or its business reside. If a data controller is not within the European Union, then the rules of the country where physical equipment is located apply.

Unlike HIPAA and GLBA, the European Data Privacy Initiative applies to all information without regard to its specific nature, i.e., health or financial records.

Data controllers must adhere to these rules. (17)

1) Data must be processed fairly and lawfully.

2) Data must be explicitly collected for legitimate purposes and used accordingly.

3) The data must be relevant.

4) The data must be accurate and up to date.

5) Data controllers must provide reasonable measures for data subjects to rectify, block or erase incorrect data.

6) Data that identifies individuals must not be kept longer than necessary.

7) Member states must establish at least one supervisory authority to monitor how the directive is applied. These authorities must maintain a public register of data controllers.

8) Data controllers must notify the supervisory authorities when they process data. EU states may waive this requirement if the processing does not have particular risks or if the data controller appoints an independent person in charge of data protection.

Member states of the EU may determine which data processing operations carry any risk. They may also require that their supervisory authorities run a check before any data processing begins.

The limitations on data controllers also address when data may be processed. (17)

1) Data can only be gathered and processed when the data subject has given free and unambiguous consent after being adequately informed.

2) Data processing is necessary when when the performance of a contract involves the data subject. Data processing for billing purposes is an example.

3) Data processing is necessary wherever required by law.

4) Data processing is necessary when it protects the interest of the data subject's life.

5) Data processing is necessary when officials need to carry out tasks of public interest.

6) If a data controller or a third party has a legitimate interest to process data, it may do so. But his concept does not override the data subject's right to privacy.

The European Data Privacy Data Initiative places strict regulation on sensitive data. Ethnic origin, political affiliations, religious beliefs, union memberships, health data and sexual preference are forbidden from processing. (17)

Data subjects have the right to be informed when they are the subjects of data processing. Subjects have the right to know who is doing the data processing, the

purpose of the processing, and the recipients of the data. Moreover, subjects must be informed when data are obtained directly or indirectly from third parties. (17)

Data subjects have the right to access data about themselves, including querying any data controllers to learn if they have processed any information. If data are erroneous or unlawfully processed, the data subject has the right to seek correction, blocking of that data, or to have it erased. Data subjects may require data controllers to notify any affected third parties. (17)

The European Data Privacy Initiative allows the transfer of data to non-members of the European Union only when those countries outside the union can guarantee adequate protection equal to that provided by the initiative. If such a guarantee cannot be made, data transfer is prohibited. If one member of the European Union finds that it cannot transfer data due to a lack of a guarantee, it must inform the European Commission. The commission, after examination, may extend the ban to the whole community. It may also reverse the ban. Either way, no member of the European community would be allowed to transfer data to a non-member while other members of the union are banned from doing so. (17)

6 OTHER FOREIGN PRIVACY LAWS AND TRENDS

It is worth briefly noting that other foreign countries, using the model of the European Union, have enacted or have begun to enact tough privacy laws. Furthermore, in light of incidents where information has been abused, the countries that have reaped the benefits of outsourced work have realized that they would not be able to continue doing business with Europe or the United States if they did not provide legal reform to address the problems and to provide assurance to their customers.

Australia enacted its Federal Privacy Act in 1988. This legislation, containing eleven principles, affects government agencies. (18) The National Privacy Policy affects some private businesses and health care providers. (19) Part IIIA of the Privacy Act specifically addresses credit providers and credit reporting agencies. (20) This act has been amended through the years and is almost as stringent as the European standard.

In May of 2003, Japan adopted tough privacy standards as well. In a fashion similar to the European standards, the language is broad, rather than specific, and provides a wide range of rights and remedies to individuals, and limits the flow of information outside of Japan. (21)

Encouraging news is coming from India, the destination for a great deal of outsourced data processing functions. The country's Ministry of information Technology and the National Association of Software and Service Companies (Nasscom) are working to draft legislation similar to the European standard. (22) India's push to adopt tough privacy rules is driven by the desire to provide better assurance for its customers as well as to expand business relationships and opportunities with the United States and the European Union. These new standards

would supplement the Information Technology Act of 2000. (23)

For a quick overview, a map, detailing where tough privacy laws exist-and where they do not- may be found at this URL:

http://sfgate.com/cgibin/object.cgi?object=/chronicle/pictures/2004/03/28/mn_offshoreprivacy28gr.jpg&paper=chronicle&file=MNGFS3080R264.DTL&directory=/c/a/2004/03/28&type=news

7 U.S. LAWS FALL SHORT

Since HIPAA and GLBA address the confidentiality of data, address unacceptable use of the data, and provide remedies for violations, how did the incident between UCSF and the Pakistani transcriber occur and leave behind questions of accountability and remedy in its wake? The weaknesses of HIPAA and GLBA can be found in the application of the regulations and the inability to enforce those regulations outside the United States.

The first weakness of HIPAA is that its privacy rule applies only to covered entities (e.g., hospitals, HMOs). Contractors and subcontractors, foreign or domestic, are not bound by the rule. However, subcontractors are likely to be defined as business associates under HIPAA's privacy rule and would be contractually obligated to protect data under their agreement with the covered entity, HIPAA only affects the covered entity. (24) Contractors and subcontractors need only to answer to the terms of their contract with the covered entity.

The U.S. Department of Health and Human Services, which oversees HIPAA, only has the authority to regulate covered entities. Business associates must agree to be considered as covered entities before the Department of Health and Human Services could take any action. Even though foreign business associates are contractually bound to protect data, the ability to enforce such an agreement would fall under the jurisdiction of a foreign court. Foreign courts and laws may cover the abuse of data in a strict manner, or they may not. This uncertainty is where the ability to enforce HIPAA and the topic of outsourced data becomes questionable and frustrating. Even though covered entities may require that any dispute with a offshore business associate be handled in U.S. courts, the business associate remains offshore, rendering any judgment or other remedy potentially useless. (24) The inability to enforce contractual obligations in a foreign setting is HIPAA's second weakness.

HIPAA places the burden on covered entities to address a breach of confidentiality, regardless of whether the covered entity or a business associate has committed a violation. If the covered entity cannot rectify the problem caused by a business associate, it must terminate the relationship with the offending business associate. However, HIPAA does not require covered entities to monitor how their business associates are handling sensitive data. (24) This third weakness in the HIPPA rules leaves covered entities exposed to litigation. We will have a better understanding of legal liabilities as they apply to covered entities and business associates when the

pending litigation of the UCSF incident is resolved.

The mandates of the Gramm-Leach-Bliley Act are similar to HIPAA. GLBA requires adequate provisions for the security and confidentiality of financial information. Security breaches (domestic and foreign) must be fully disclosed. When a bank or any other financial institution uses a third party contractor (domestic or foreign) to process information, it does not avoid the responsibility for the confidentiality of the information. The weaknesses of GLBA are similar to HIPAA's as well, notably the lack of enforceability of GLBA's provisions in a foreign jurisdiction and the lack of oversight over contractors.

A comparison of the main differences between Federal privacy laws and the European Union Data Privacy Initiative shows two different philosophies that govern how data are treated. U.S. regulations, while seemingly tough, are built around the concept of allowing business to operate in a cost effective fashion and to send data offshore without a complete accounting of the security risks and remedies, thus creating huge potential for the abuse or compromise of data. European regulations, on the other hand, set a tough standard for all data, basing the standard on one principle: the rights of the individual. Data processing, moreover, is subject to regulatory oversight.

Rather than considering data as a single issue for consideration, Federal regulations are specific to the type of data being processed, and so HIPAA and GLBA address the issues of medical and financial data. The European Union model simply treats data as a single issue without regard to the type of information. Where HIPAA and GLBA go to great lengths to define customers and consumers, covered entities and business associates, and opt out versus opt in privileges, the European Union model simply defines data subjects and data controllers. This model also assumes that individuals have opted in for full privacy rights.

U.S. data privacy laws spell out required action but rely on voluntary compliance. In the European Union, member states have a data authority to monitor how data is processed. Moreover, those who process data, known as data controllers, must be publicly registered. By making data processing and the associated privacy issues less transparent, the mandates of the European Union initiative, notably with regard to the rights of the individual, are less ambiguous than the U.S. laws.

Finally, the standards of the European Union have precluded the issues of information compromise and abuse in an offshore setting due to the concept of guaranteed equivalent protection. If one member of the European Union, wishing to send data abroad, cannot find sufficient protection under a non-member's laws, it is prevented from sending the work offshore. When such a situation occurs, all of the other members of the European Union are prohibited from doing so as well.

8 U.S. LEGISLATORS CALL FOR TOUGHER LAWS

As the notoriety of the UCSF incident has increased, as a few other incidents have come to light, and as the dangers of outsourcing sensitive data have become prominent points of discussion, the mandates of HIPPA and GLBA have also come under scrutiny, leading American politicians to start proposing, new, tougher pieces of legislation that would tighten the flow of information going abroad, further define the roles and responsibilities of all parties involved in the process of handling information, and provide more remedies and a higher level of assurance for Americans.

In 2003, California adopted Senate Bill 27 (SB 27), introduced by Senator Liz Figueroa. SB 27 empowers consumers to discover what types of information companies maintain about them, what third party companies receive the information, and the names of those third party companies. In lieu of providing this information, companies may provide a privacy policy with an opportunity to opt out of information sharing.(25)

SB 27 partially accomplishes an aspect of the European Data Privacy Initiative. Consumers now have the ability to know who is collecting information, what sort of information is being collected, and where the information is being sent. In contrast to the European initiative, SB 27 does not provide an automatic "opt in" of privacy to consumers in order to eliminate data sharing.

Senator Figueroa has another proposal before the California Senate that would affect medical and financial privacy as well as outsourcing. SB 1451 proposes that all work involving confidential information sent outside of California will be subject to California's privacy provisions regardless of where the work is performed. Non-California sub-contractors will be subject to California's legal jurisdiction when any related law is violated. California's customers must be notified when any confidential information is sent outside of California. (26)

The problem of enforcing California's jurisdiction in a foreign setting seems to problematic. To that end, if a Californian has her privacy right violated by an overseas sub-contractor, Senator Figueroa is contemplating legislation that would allow the Californian to sue the American hiring party. Senator Figueroa is also considering legislation that would prohibit hospitals from sending clerical work offshore. As none of these issues were covered under the California Confidentiality of Medical Information Act, these proposals are a reaction to the effects of outsourcing. (27)

On the Federal level, Senator Dianne Feinstein of California is considering stricter legislation aimed at financial institutions. In March 2004, Senator Feinstein sent letters of inquiry to the U.S. Comptroller of the Currency (OCC) and the CEOs of several corporations, asking what safeguards were in place for personal information sent abroad. The letter also discussed the possibility of legislation to provide such safeguards. Senator Feinstein also asked the General Accounting Office to investigate the extent to which personal data has been sent abroad by private and

public sources. (28)

Referring to the some of the regulatory rules under the Gramm-Leach-Bliley act, Senator Feinstein notes that these lack enforcement abroad. The senator's letter of inquiry to the OCC seeks to establish how many financial institutions are using offshore contractors, how those contractors are audited, how many enforcements have been started by the OCC after American privacy has been violated by third party contractors in foreign countries, to identify OCC examiners reviewing outsourced contracts, and to identify the number of breaches by offshore contractors. Senator Feinstein's query also asks the OCC to compile statistics for domestic contracts.(28)

The issue of data sent offshore and the risk to its privacy has shown that our current laws (HIPAA, GLBA) do not adequately cover or protect American consumers and customers when information is sent abroad for processing. While some will note that information can be compromised domestically, Senators Feinstein and Figueroa are correct to note that our laws are not enforceable in other countries. Out of responsibility for their constituents, these legislators have begun to consider and introduce restrictive legislation that will clearly define responsibilities, remedies, and penalties. One of Senator Figueroa's proposals may simply halt the flow of medical data headed for foreign countries.

9 SOLUTIONS

Solutions to the problem of data at risk offshore may be broadly placed in three categories: legal, procedural, and technical. The recent spate of incidents of compromised information in offshore outsourcing scenarios has forced some firms to apply procedural and technical solutions to reduce the chance for compromise or abuse of sensitive data. Legislators have reacted by proposing and introducing laws that deal strictly with the offshore nature of the problem. The immediate future seems to hold a combination of technical, procedural, and legal solutions, all of which must work together in order to provide a higher level of effective data protection.

The UCSF incident stands out because the medical records were sub-contracted a second time, sent abroad without any notification to UCSF and without any supervision of the transcriber in Pakistan. Even though HIPAA broadly covers medical transcriptions, this episode exposes a lack of checks, balances and clear procedures, and careless handling of private, sensitive data.

However, some companies have used some foresight to tackle the problematic nature of outsourcing sensitive data. They have started to apply a variety of means to assure confidentiality when information is sent offshore.

In light of recent news headlines, CNA financial Corporation in Chicago, which outsources some billing functions overseas, has implemented many precautions to

protect data, including allowing access to necessary information only and locating all servers within the United States. (29) CNA's implementations offer a starting point where some finer aspects of information security may be applied in order to achieve a higher degree of control over information at risk.

Out of all the concepts of information security as they relate to data and the people who handle the data, the principle of least access privilege is most appropriate and can be applied to an offshore outsourcing work center. Considering that the medical records from UCSF were sent abroad without any safeguards, least access privileges will need to play a larger role in the offshore outsourcing of critical data.

CNA only sends necessary bits of information to be processed. However, these may include Social Security numbers, credit card numbers, and other bits that can be exploited. Even though the amount of information is limited, it is still vulnerable.

CNA first applies the concept of least access by creating work facilities that are essentially clean rooms. (29) From a physical perspective, information is controlled as it is contained within the room. Employee access could be controlled and monitored, perhaps using some form of biometric authentication such as hand scanning. The purpose of access monitoring is to prevent impersonation or illegal entry. Employees may be monitored when exiting; security cameras inside and outside the facility are a possibility. Physical checks may be part of the process as well. These practices address the aspect of unauthorized access.

Within the clean room, every means of transferring or manipulating data is controlled as well. Employees have access to terminals only. There is no possibility of transferring data via hard drives, CD or DVD/ROM, floppy disk drives, or USB ports. External e-mail is not allowed in the clean room. Photocopiers are absent as well. (29) If legally permissable, keystroke logging and telephone monitoring are other means of surveillance that might be employed in the clean room. Since the old fashioned method of copying via pencil and paper is a possibility, these too might be eliminated from the clean room, especially if the data processing tasks simply require interaction with the terminal.

Offshore workers should be classified as data custodians. Data custodians have temporary ownership of data and limited rights to what they may do with that data.

Some precautions might be taken before information is sent abroad. Non-essential yet confidential information could be stripped or encrypted before being outsourced. Servers, as in the CNA examples, should be located in the originating country of the data. Data backup should occur in the originating country as well. (29) Public key encryption and signatures could be used to confirm the identity of users logged into sensitive data. These methods allow a degree of control from a domestic perspective.

Since the crux of the issue seems to be that outsourcing has lost control of

confidential information, the best form of control ought to focus on the users and their access to information.

A policy of Mandatory Access Control (MAC) with rule or role set based access privileges is a good choice. MAC is simply a process that enforces security rules in relation to the sharing of data. The principles of MAC reinforce the concept of security from the originating server to the clean room on another continent. These principles offer a greater degree of control on how the data will be processed in a clean room. Only the administrator has the right to change security levels. All data have a security level. Users may or may not have privileges to access data at lower and higher classifications. All user data are classified. All users have clearance levels. Users cannot give clearance to another person. Access can be restricted in other ways, including availability according to the time of day. For example, an offshore clean room would only have access to data during business hours, greatly reducing the chance of compromise during an after hours break in. (30)

Some argue that MAC is too extreme and is appropriate for military or top secret applications. Others argue that Discretionary Access Control (DAC), while intended for commercial or civilian use, is too weak. “Role based access control, in many applications is concerned more with access to functions and information than strictly with access to information.” (31)

Information access can also be taken into consideration with the academic models of Bell-LaPadula or Biba. Bell-Lapadula supports MAC by determining access rights as related to the security levels of subjects (data users) and objects (data).(32) Access rights include read-only, append (but not read), execute (neither read nor write), and read-write. Subjects may only read down, i.e. gain access to data at a lower security level. Subjects never gain access to information at a higher security level. Subjects may only append upwards, thus preventing information being passed to lower levels of clearance. (33)

MAC might best be supplemented by the Biba model of access control. This process focuses on controlling object modification. Integrity is defined as the prevention of unauthorized modification. (34) Subjects' actions are limited. Subjects may not execute objects with a lower level of integrity, nor may they modify objects at a higher level of integrity. Subjects may not request services from other subjects who have a higher level of integrity. (35)

Other forms of technical control focus on the employees. A high priority should be placed on employee screening and selection. CNA demands that employee turnover be kept to a low rate. Employees would then become well known within the organization. (29) Employee training and education, especially with regard to compliance with HIPAA or GLBA, set a level of expectation within the offshore operation.

The UCSF incident revealed that almost no technical controls were applied to the medical records. The reaction to Lubna Baloch's threatening e-mail also indicates

that UCSF was procedurally unprepared to handle the incident. (1)

From a technical perspective, the ability to secure data once it has been sent offshore and to guarantee that whatever work performed on that data remains confidential and retains integrity requires a great deal of planning that focuses on controlling access to sensitive information or controlling the processes that any foreign worker may perform on such information.

Technical solutions provide means of prevention and detection. Technical solutions to the problems caused by outsourced information can be developed, implemented, and strongly reinforced through policies and procedures formulated to address potential problems. From an information security perspective, three practices, business continuity planning, risk assessment, and auditing help to define the technical solutions to be applied.

Any business that sends information abroad and is covered by the mandates of HIPAA or GLBA needs to consider information abuse or compromise as an eventuality and not a mere possibility. This is the first premise of business continuity planning (BCP) with respect to information sent abroad.

BCP defines both the problem and the objectives sought to address the problem. A defined security policy seeks to protect information, identifies issues at risk, personnel involved, procedures to be followed, and contingencies wherever possible. The security plan needs to be clearly written and should be anticipatory. Risk assessment further defines the problem, forecasting the impact on the business in legal and financial terms when an incident occurs and policy is violated. Aside from legal fines, financial risk would also take into account the potential loss of business, poor public relations, and the potential impact of lawsuits. (36)

BCP provides the structure to implement prevention, detection, and response. Some of the previous technical suggestions to ensure security of outsourced information would be considered. Aside from procedures and policy, BCP establishes standards, time lines, project delivery, and documentation to support the processes and their eventual implementation.

The purpose of BCP is to prepare for any type of disastrous scenario. With the assumption that confidential information sent offshore can be breached and abused, backup and disaster recovery strategies, lists of key personnel to handle the incident, documents and procedures, and the recovery phase itself would be recorded in the plan. These elements will help a business to recover quickly, limit further damage, and move ahead.

The plan may look good on paper, and so it requires testing and auditing. Auditing, especially when done by a disinterested party, is seen as a critical way to test the durability of any system where information is sent offshore for processing. (29) Audits will test whether the procedures and guidelines are working. Audits done at intervals will confirm that the procedures are holding up, or if they have changed, leaving the business vulnerable. Audits should also examine the procedures,

policies, and business continuity plans of offshore business partners. (37)

HIPAA and GLBA spell out most of the technical solutions listed above, yet information still remains vulnerable. While business continuity planning and risk assessment can help to implement technical solutions to the problem of data confidentiality and offshore outsourcing, only accountability under a set of laws that governs the process can provide the assurance and effectiveness of policies, procedures, and audits.

The current problem is that laws on information privacy around the world are disparate. When laws and enforcement around the world range from stringent to nil, questions of legal jurisdiction and remedies will certainly arise when information is compromised, leaving aggrieved parties confused and dissatisfied.

The best solution would be an international standard. The European Union's laws are the best example of a unified standard. With India, Japan, Australia, and others bringing similar pieces of legislation into existence, continuity would reduce the amount of ambiguity, especially if such laws addressed how remedies might be provided in foreign jurisdictions.

American laws, however, assume compliance by covered entities and financial companies. The laws seek to provide some protection, but they also leave many exploitable holes where data can be abused. Politicians are seeking to assure the confidentiality of private data shipped offshore by creating laws with strict wording and regulations about how information can be handled or processed. In other instances, outsourcing may be banned. (26) (27) (28)

Full public disclosure of offshoring practices, including notification of what types of data are being moved will increase public awareness. Laws already exist regarding public disclosure when private information has been breached or compromised, but the responsible parties aren't very forthcoming when making these announcements. (7)

For the moment, legal experts feel that contractual obligations are the best way to ensure confidentiality when information is shipped to countries beyond U.S jurisdiction. In order to prevent problems and to provide recourse if the contract is broken, all stipulations must be clearly spelled out in the contract. (24)

A strong combination of procedures and technical solutions driven by clear, consistent laws and enforcement can go a long way towards making the offshore outsourcing a much safer experience and process. However, there is no guarantee that current proposed legislation will pass or, should the proposals become law, that they will have much teeth to close the loopholes and deficiencies in HIPAA and GLBA. Without the mandate of clear, stringent laws, the confidentiality of information sent offshore will depend on businesses voluntarily taking the detailed steps of business continuity planning to prepare for threats and spending the money to implement technical safeguards.

10 CONCLUSION

As the Internet has helped to create a global market, the vulnerabilities and shortcomings of the different laws have been exposed

Some steps are being taken internationally to increase the assurance of data confidentiality that is offshore outsourced. Most of these involve defining and implementing laws. Many aspire to meet the standard of the European Union.

A huge disparity exists among the European standard, the gamut of US laws, which address privacy to varying degrees, and the laws or lack thereof in other countries. In legal terms, the solutions might be more comforting if all laws met the European standard, the toughest in existence.

As discussed, technical solutions will provide a greater degree of assurance, but not necessarily a greater level of comfort with the knowledge of information being processed in far away lands.

Creation of a comprehensive BCP, performing a thorough risk assessment with the principles of prevention, detection, and response in mind, establishment of clear procedures and responsibilities, and installation of a variety of technical controls establish a strong foundation for a secure operation. Third party audits can examine the whole process to reveal strengths and weaknesses. With a consistent set of international laws that detail well-defined regulations and remedies, a much greater degree of comfort for all involved in the process of outsourcing might exist.

However, questions remain.

Although US legislators are pushing for stricter regulations, will these become legislation?

If California becomes the leader in strict regulations, can we assume that the other states will follow?

Why should the issue be addressed on a state-by-state basis? Why shouldn't there be a comprehensive Federal policy administered by the office of a privacy “czar?”(38)

American businesses argue that the cost of implementing a model similar to the European Union is too expensive and burdensome. (39) While big companies, such as CNA, can maintain a staff dedicated to information privacy and compliance, will smaller companies voluntarily follow suit?

In a British Broadcasting Corporation report noting that information work is going to the Philippines, the effect of political instability on business and sensitive information is questioned. (40) How can the outsourcing of sensitive data be done safely where the threat of war or political instability exists?

As of this writing, there are no guarantees of an acceptable solution. Incidents are happening. Lawsuits have yet to be settled. New legislation is around the corner. While information and data privacy laws around the world seem to be tightening, they still are not equal or consistent. Technical and procedural remedies are not clearly defined. Some big companies are taking the lead to implement controls, but only because they have the resources to do so. As this paper comes to an end, there are too many factors in doubt to draw a reasonable conclusion as to how outsourced data will be secured on distant foreign shores.

ENDNOTES

(1) Lazarus, David. “A tough lesson on medical privacy. Pakistani transcriber threatens UCSF over back pay.” San Francisco Chronicle. 22 October 2003. URL:http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL (11 March 2004).

(2) Kirby, Carrie. “Hacking danger for outsourced records hard to gauge.” San Francisco Chronicle. 28 March 2004. URL:http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/03/28/HACKING.TMP (10 April 2004)

(3) “Exporting Privacy.” San Francisco Chronicle. 28 March 2004. URL:http://sfgate.com/cgi-bin/object.cgi?object=/chronicle/pictures/2004/03/28/mn_offshoreprivacy28gr.jpg&paper=chronicle&file=MNGFS3080R264.DTL&directory=/c/a/2004/03/28&type=news (10 April 2004).

(4) “Outsourcing going to grow.” CNNMoney. 26 March 2004. URL:http://money.cnn.com/2004/03/26/news/economy/outsourcing_survey/index.htm?cnn=yes (10 April 2004).

(5) Klepper, Robert and Jones, Wendell O. “Trends Favoring Outsourcing.” Fred Beshears Articles Index. 1998 URL:http://ist-socrates.berkeley.edu/~fmb/articles/outsourcingtrends.html (5 April 2004).

(6) King, Ledyard. “Washington is sending state jobs overseas.” Seattle Times. 10 April 2004 URL:http://seattletimes.nwsource.com/html/localnews/2001900132_offshoring10.htm(10 April 2004).

(7) Lazarus, David. “Extortion threat to patients' records. Clients not informed of India staff's breach.” San Francisco Chronicle. 2 April 2004 URL:http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/02/MNGI75VIEB1.DTL (10 April 2004)

(8) “Capital One axes India call center deal.” Yahoo!Finance. 25 March 2004 URL:http://biz.yahoo.com/rf/040325/finance_capitalone_india_1.html (12 April 2004).

(9) “Capital One did not halt contract.” Yahoo!India Finance. 24 March 2004 URL:http://in.biz.yahoo.com/040324/65/2c6hu.html(12 April 2004).

(10) United States Department of Health and Human Services Office for Civil Rights. “HIPAA.” 4 August 2003
URL:http://www.hhs.gov/ocr/privacysummary.pdf(12 April 2004).

(11) United States Federal Trade Commision. “Financial Privacy: The Gramm-Leach Bliley Act.”
URL:http://www.ftc.gov/privacy/glbact/(12 April 2004).

(12) United States Federal Trade Commission. “In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act.”
URL:http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm(16 April 2004).

(13) United States Federal Trade Commission. “Standards for Safeguarding Customer Information; Final Rule.” 23 May 2002.
URL:http://www.ftc.gov/os/2002/05/67fr36585.pdf(16 April 2004).

(14) United States Department of Health and Human Services.”Health Insurance Reform: Security Standards.” 20 February 2003,
URL:http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf(16 April 2004)

(15) Langin, Daniel J. “Gramm-Leach-Bliley: Keeping Robbers and Regulators from the Door.” September 2002.
URL:http://www.securitymanagement.com/library/gramm_tech0902.pdf (\16 April 2004).

(16) United States Federal Trade Commission. “Pretexting: Your Personal Information Revealed.” January 2001.
URL:http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm(16 April 2004).

(17) “Data Protection in the European Union.”
URL:http://europa.eu.int/comm/internal_market/privacy/docs/guide/guide-ukingdom_en.pdf (14 April 2004)

(18) “Information Privacy Principles under the Privacy Act 1988.”
URL:http://www.privacy.gov.au/publications/ipps_print.html (17 April 2004)

(19) “National Privacy Principles.”
URL:http://www.privacy.gov.au/publications/npps01.html (17 April 2004)

(20) “Privacy Act 1988 Section 18c”
URL:http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s18c.html (17 April 2004)

(21) Worlton, Amy E. “Asia Opts for EU Style Privacy.” Privacy In Focus. June 2003. URL:http://www.wrf.com/publications/publication.asp?id=143056272003 (10 April 2004)

(22) Ribeiro, John. “India works on data protection law.” ComputerWeekly.com. 13 June 2003.
URL:http://www.computerweekly.com/Article122612.htm (12 April 2004)

(23) Ministry of Law, Justice and Company Affairs.“The Information Technology Act, 2000.” 9 June 2000.
URL:http://www.mit.gov.in/itbillonline/it_framef.asp (18 April 2004)

(24) Fox, Steve and Monson, Rebekah A.Z. “HIPAA and Foreign Outsourcing.” February 2004. HIPPAction HIPAAdvisory.com
URL: http://www.hipaadvisory.com/action/LegalQA/law/Legal44.htm
(10 April 2004).

(25) Mara, Janis. “California Debuts New Online Privacy Laws.” 5 January 2004.
URL:http://www.clickz.com/news/article.php/3295381 (10 April 2004).

(26) “Fact Sheet for SB 1451: Protecting Medical and Financial Privacy from Outsourcing.” March 2004.
URL:http://democrats.sen.ca.gov/senator/figueroa/ (18 April 2004),

(27) Zetter, Kim. “Outsourcing: Danger to Privacy.” 20 February 2004.
URL:http://www.wired.com/news/business/0,1367,62356,00.html (18 April 2004),

(28) “Feinstein Urges Treasury Investigation on Outsourcing Practices of American Banks.” 3 March 2004.
URL:http://feinstein.senate.gov/04Releases/r-banksoutsource.html
(10 April 2004).

(29) Collett, Stacy. “Outsourcing: Losing Control.” 15 March 2004.
URL:http://www.computerworld.com/securitytopics/security/story/0,10801,91085,00.html (18 April 2004).

(30) “Mandatory Access Control Chapter 8: Access Control and Authorization.”
URL:http://www.cgisecurity.com/owasp/html/ch08s02.html (18 April 2004).

(31) Ferraiolo, David and Kuhn, Richard. “Role Based Access Controls.” 15th National Computer Security Conference 1992.
URL:http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html (18 April 2004

(32) Shen, Hong Hai. “Bell LaPadula Model.” 4 November 1996.
URL:http://www.cs.unc.edu/~dewan/242/f96/notes/prot/node13.html
(18 April 2004).

(33) Manocha, Harsh. “Protection: Bell-LaPadula Model.” 1999.
URL: http://courses.cs.vt.edu/~cs5204/fall99/protection/harsh/ (18 April 2004).

(34) “Access Control Models.” The CISSP Open Study Guide Web Site.
URL:http://www.cccure.org/Documents/HISM/087-089.html (18 April 2004).

(35) “The Biba Model.” The CISSP Open Study Guide Web Site.
URL:http://www.cccure.org/Documents/HISM/023-026.html(18 April 2004).

(36) “Risk Analysis.” The Business Continuity Planning & Disaster Recovery Planning Directory. 1993-2003
URL:http://www.disasterrecoveryworld.com/risk.htm (18 April 2004).

(37) Vijayan, Jaikumar. “Offshore ops to get stronger privacy lock.” Computerworld 2 June 2003.
URL:http://www.computerworld.com/managementtopics/outsourcing/story/0,10801,81698,00.html (10 April 2004).

(38) “A Call for Creation of Federal Privacy Agency.” 30 October 2003.
URL:http://privacy.org/archives/2003_10.html (10 April 2004).

(39) “The EU Data Privacy Directive.” 26 July 2003.
URL:http://www.privacilla.org/government/eudirective.html (10 April 2004).

(40) “HSBC routes calls to the Philippines.” BBC News World Edition. (13 April 2004).
URL:http://news.bbc.co.uk/2/hi/business/3624851.stm (13 April 2004).