

BRIEFING PAPER

**“Practical Solutions”**

**Ensuring Protection of Sensitive Medical Information**

PREPARED BY:

HIPAA SOLUTIONS, LC

PETER MACKOUL, ESQ.,

&

CO-AUTHORED BY

KEN HUGHES, CCNA, CCDA, MCSE, CNE

HIPAA SOLUTIONS, LC

[WWW.HIPAA SOLUTIONS.ORG](http://WWW.HIPAA SOLUTIONS.ORG)

TOLL FREE: 877-779-3004

TABLE OF CONTENTS

1 OVERVIEW & BACKGROUND INFORMATION..... 3

2 INFORMATION TECHNOLOGY & MEDICAL INFORMATION ..... 3

3 PRIVACY AND SECURITY ..... 5

3.1 A MASSIVE BREACH IN TEXAS..... 6

3.2 THE STATE OF TEXAS & THE HEALTH INFORMATION TECHNOLOGY ADVISORY COMMITTEE, HITAC ..... 7

3.3 ANALYSIS OF A HIPAA NETWORK ..... 7

3.3.1 *Detailed Network Analysis Section*..... 9

3.3.2 *What about VPN connectivity?*..... 10

4 "REAL WORLD SOLUTIONS" ..... 14

## 1 OVERVIEW & BACKGROUND INFORMATION

The purpose of this document is to explore practical “real world” solutions that would assist in protecting the privacy and security of health and medical information related to the collection, storage and transfer of personal information in today’s world of information technology. The sensitivity of medical information is particularly significant in today’s technological environment, i.e., the improper release of medical information about an individual can cause that person to lose a job, health insurance coverage, or damage their family and personal lives with potentially catastrophic results. In addition medical data bases represent targets for identity theft, a rapidly growing phenomenon on the national level.

The irresponsible or casual use of information technology represents a threat to personal privacy and can have serious consequences on many levels. The routine collection, use and instantaneous transfer of medical information is performed by many organizations, including federal and local government entities, schools and universities, health care providers and private businesses, often allowing individuals no control over sensitive information about their personal lives.

As stated, although this problem is particularly significant today with the use of computer technology, it is not a new issue. Twenty six years ago, a Federal Appellate Court identified the governmental use of information technology as a threat to the personal privacy of all individuals specifically referring to personal medical records. That court stated: *“much of the concern has been with governmental accumulation of data and the ability of government officials to put **information technology** to uses detrimental to individual privacy, which have been facilitated by the spread of data banks and by the increasing storage in computers of sensitive information relating to the personal lives and activities of private citizens.”*<sup>1</sup>

This remarkable bit of insight occurred at a time when technology was developing and not nearly as advanced as today.

## 2 INFORMATION TECHNOLOGY & MEDICAL INFORMATION

A major reason for encouraging the utilization of information technology in the practice of medicine is the potential for saving lives and reducing the cost of providing healthcare. In testimony to the House Committee on Energy and Commerce, Dr. Bill Braithwaite, the Chief Medical Officer of eHealth Initiative stated: “. . . *the number of*

---

<sup>1</sup> U.S. v. Westinghouse, 638 F.2d 570 at 576

*deaths caused by medical errors in our healthcare system every year has been estimated to be 100,000 or higher. I think we would all agree; that is totally unacceptable. And in most cases it is the system that is at fault: we still practice medicine under the old paradigm where the doctor and the patient interact from memory to arrive at healthcare decisions for the patient. The only way to significantly improve the quality, safety, and efficiency of our healthcare system is to bring the information system into the exam room, as it were, and to change the paradigm of clinical practice so that it routinely involves the doctor, the patient, and the computer working together to provide the best healthcare advice possible. The way to implement this new approach is through direct interaction with a Clinical Decision Support System (CDSS). Such a system must be integrated into the clinical environment in a way that supports rather than disrupts the efficient flow of the process of healthcare. Since most of the data on which clinical decisions are made actually originate outside the exam room, the CDSS by itself is not functional without a way to access the sources of the clinical data, the labs, pharmacies, radiology centers, etc. This, then, is the impetus for eHI's emphasis on interoperable health information exchange initiatives.”<sup>2</sup>*

A Clinical Decision Support System is a comprehensive technology system, not simply an Electronic Medical Record, or EMR. An EMR is a computerized version of the paper records health care providers' use to record patient's information, treatments and diagnoses.

Utilizing EMR's alone could reduce the cost of providing healthcare according to Blackford Middleton in his testimony to the National Committee on Vital and Health Statistics (NCVHS). Middleton stated: *“Studies we have done at the Center for IT Leadership in Boston suggest that electronic health records with advanced computerized provider order entry capabilities could save the country \$44 billion if adopted nationwide. These tools when well designed and implemented can impact physician behavior and decision-making at the point of care. However, to achieve maximal value from healthcare information technology, we need not only to adopt tools that improve clinical information management and decision-making at the point of care, but also to link these systems to one another so that appropriate healthcare information is available wherever and whenever it is needed for patient care. This creates an interconnected, electronic healthcare system, and produces significant additional value for the US healthcare delivery system. In our analysis of the value of healthcare information exchange and interoperability at the CITL, we find that if clinical information were readily shared across key members of the healthcare delivery system (doctors' offices, hospitals, laboratory centers, radiology centers, payers, and public health agencies) an additional \$78 billion potential savings is available.”*<sup>3</sup>

---

<sup>2</sup> Please see the Testimony of Dr. Bill Braithwaite to the Subcommittee on Health, House Committee on Energy and Commerce, March 16, 2006, and page 3 to 4.

<sup>3</sup> Testimony of Blackford Middleton to the National Committee on Vital and Health Statistics (NCVHS) dated July 26, 2006

Although the testimonies above are accurate, the current status relating to privacy breaches from health care providers, insurers and schools and universities is abysmal. For example, according to the Privacy Rights Clearinghouse, a non-profit national privacy organization, over 90 million identities have been lost via data breaches sensitive data have occurred since February 15, 2005, (or since the Choice Point breach).<sup>4</sup> Many of these breaches occurred with health care providers, insurers, government entities, schools and universities. This situation illustrates that, although there is a focus on developing the technology to save lives and money in the health care arena, the attention to security and privacy issues is grossly inadequate and is years behind the technology that can deliver the efficiency and reliability needed to deal with the information.

### 3 PRIVACY AND SECURITY

As stated above, the number of data breaches occurring on a frequent basis is overwhelming with over 90 million records compromised since 2005. Introducing information technology into the examination room and healthcare arena without seriously addressing basic privacy and network security precautions has every potential of being an unmitigated disaster. It could result in many more data breaches of private medical and financial information.

While existing privacy and security regulations are focused on requiring organizations to follow 'best business practices' in relation to the use of private medical information, financial information, and network security practices, in reality many of the regulations intended to protect sensitive information are given minimal or cursory attention in an overwhelming number of organizations due to costs of compliance, misunderstanding of regulations, complexity and a general unwillingness to make changes in existing organizational operations to address privacy and security.

In 1996, Congress passed the Health Insurance Portability and Accountability Act, (HIPAA) along with the Privacy, Security and Transactions rules to ensure that organizations follow best business practices. These rules would reduce the number of data breaches significantly. However, as the number of breaches indicate, many, if not most, organization don't appear to be adhering to the current regulations although the Privacy rule was required in 2003 and the Security rule in 2005. Since medical data bases often contain medical, demographic and financial information about individuals, the improper release of information in these data bases can result in damage to individuals, both personally and financially. When the risks and costs associated with

---

<sup>4</sup> Please see the following web site for more information on these numbers: <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

identity theft and national security are added in, it is obvious that attention to the issues of privacy and security must be improved quickly.

The HIPAA Privacy rule created a class of information called “Protected Health Information,” or PHI that protected personal medical information. But, since those regulations were passed, the number of security breaches has been overwhelming and the testimony of the two experts presented above indicates that the regulations have not been effective in protecting the private information of many citizens.

A major factor in the lack of effectiveness of the HIPAA privacy and security regulations is the lack of consistent enforcement of the regulations by agencies tasked with enforcement. Currently, HIPAA enforcement is “complaint driven” and the enforcement agencies depend heavily on “voluntary compliance” which has created the attitude in many organizations that the regulations don’t need to be taken very seriously and can be addressed with minimal effort. Many consulting groups, insurance and legal specialists have also advised their clients that until there is aggressive enforcement across the board on HIPAA, little resource has to be expended on compliance.

### 3.1 A MASSIVE BREACH IN TEXAS

As an example of how local government agencies are at fault in addressing security issues, one of the largest “breaches” nationwide in a local government entity occurred in Texas. While a highly publicized 2006 Veteran’s Administration breach involved 26 million records, according to a series of articles in the Fort Bend Herald-Coaster, in 2004 the County Clerk in Fort Bend County sold over 20 million records containing the personal, financial and medical information of citizens of the Fort Bend County for approximately \$2,000 dollars. The sale of records, many of which contained PHI, may be subject to potential civil and criminal sanctions although no action has been taken at this time. The government entity in this case claimed that the State Public Information Act required and allowed the release of this data, although case law indicates that medical information cannot be released under the Public Information Act.

Although this incident was widely reported in local and national media sources, no enforcement activity was ever taken. One article reported on the sale as follows: *“In what was one of the largest breaches nation wide, coming close to the VA breach In what could be the largest single transfer of a county asset to a private company in the history of Texas, Fort Bend County Clerk Dianne Wilson recently sold every document ever filed with the county clerk’s office to a Florida-based company. Red Vision paid the county approximately \$2,000 to transfer twenty million records by USB cable. This may also be the cheapest price ever paid by a private company for the bulk purchase of document images held by a government agency.”*

Also, *“according to Wilson, this was just business as usual. In an interview with B.J. Pollack of the Fort Bend Herald she said she sells the records “every day” in bulk to companies like Red Vision and has since 1995.”*

Finally, *“an asset that took Fort Bend County taxpayers 167 years to create and ten years to digitize was transferred to Florida in approximately 150 hours.”*<sup>5</sup>

The above scenario highlights the lack of serious enforcement which seems to be common as it relates to HIPAA and consequently, organizations are not motivated to take the Privacy and Security rule seriously and do not take the mandated steps required to comply with the privacy and security regulations of HIPAA. The lack of enforcement action in situations such as the Fort Bend scenario sends a clear message that there are few consequences to non-compliance with HIPAA.

This situation also points out that a key factor in implementing technology in both the healthcare and public arenas must be a commitment by all organizations involved in this process to consistently utilize and implement “best business practices” or regulations like HIPAA, at the personnel and organizational levels. Too often these best practices are disregarded as being unimportant. In sum, there must be a commitment to both improve technology and business practices.

### 3.2 THE STATE OF TEXAS & THE HEALTH INFORMATION TECHNOLOGY ADVISORY COMMITTEE, HITAC

The State of Texas recently finished “The Roadmap for the Mobilization of Healthcare Information in Texas,” which can be obtained at the following location. Please see <http://www.dshs.state.tx.us/chs/shcc/default.shtm> for an in depth analysis of these issues. This report was created by a committee made up of representatives from a broad range of public and private healthcare stakeholders and addressed Health Information Exchange, HIE, and Health Information Technology, HIT.

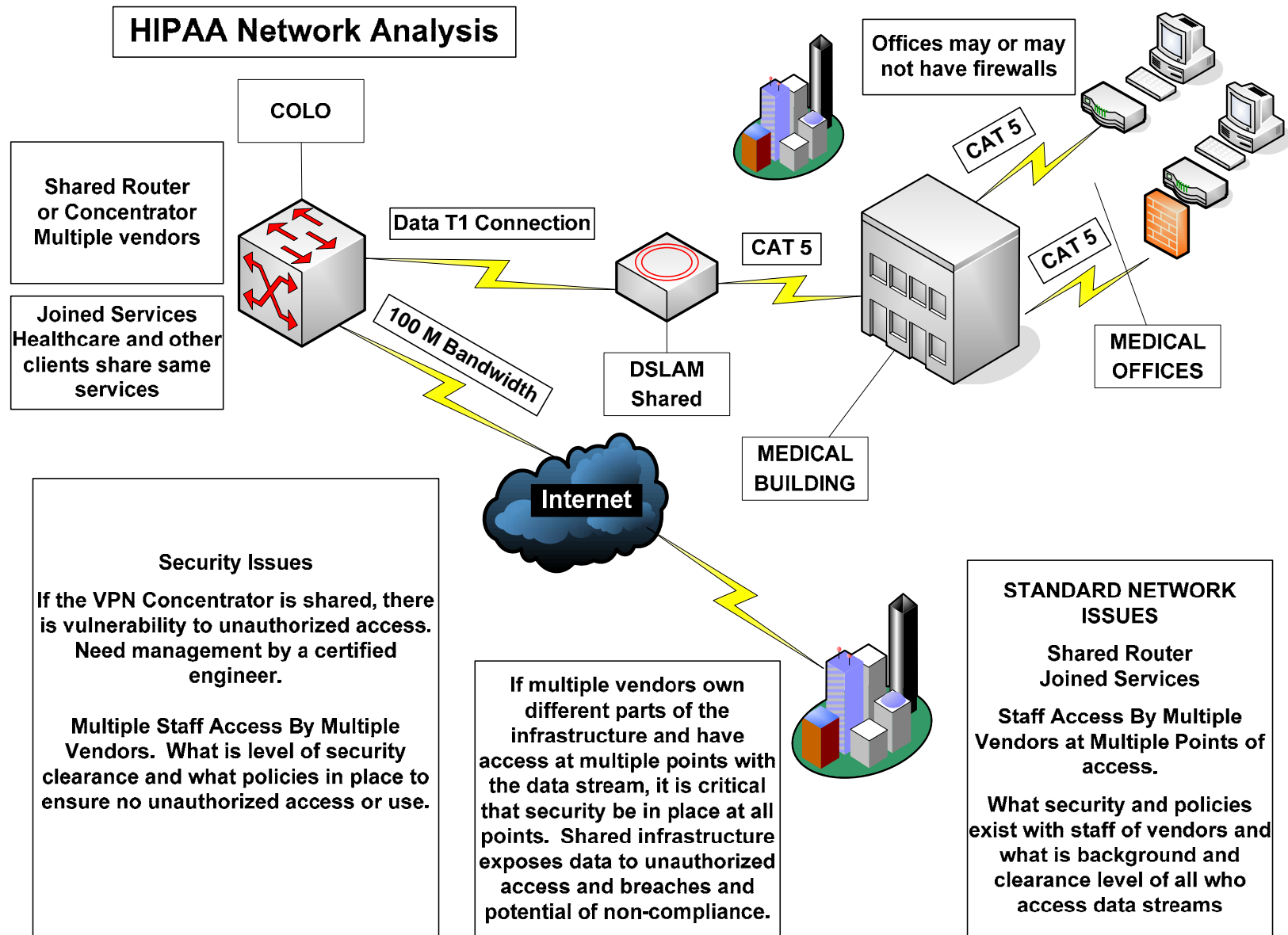
### 3.3 ANALYSIS OF A HIPAA NETWORK

The “HIPAA Network Analysis” diagram below represents a generic example of a common network structure that is often represented to be “HIPAA compliant” and the analysis following the diagram explains how this situation may expose users to data security breaches

This common structure indicates that many organizations do not take the necessary steps to ensure compliance with the HIPAA Security rule.

---

<sup>5</sup> <http://www.davickservices.com/Courthouse%20for%20Sale%20-%20Cheap.htm>



### 3.3.1 DETAILED NETWORK ANALYSIS SECTION

In many areas across the nation, physician's offices access Internet connectivity through the "physician's plaza" where their offices are located. Often, the physician plaza will connect all the offices to a common switch which is then connected to the Internet as denoted in the illustration above. The decision to protect each of the local area networks in an individual office is made by the individual physician offices. Many physicians automatically assume that if they use common routers from their local computer store such as a "DLink" or "LinkSys" their network will be protected, or they don't use routers which means that neither situation provides adequate protection for the network and the data transferred over it. .

One potential vulnerability in this situation is that the default passwords for routers need to be changed when implemented. Any high school student who has been through a basic networking class knows that all a hacker needs is the default user name and password for the router and they will be able to access the physician's network and all of the data, including PHI, stored on that network.

A simple change to the router will also allow the hacker to access any computer on the physician's network. Next the hacker would need to gain access to the physician's server, but this may not be difficult, because most physicians don't implement strong passwords on their practice management system.

These scenarios show why a seemingly secure network is often insecure. It would not take much effort for identity thieves to move into an office in a physician's plaza and obtain a wealth of information with very little "hacking knowledge" and this example only discusses 'hard wired' connectivity, not wireless vulnerabilities.

Another problem is that many physicians connect a wireless router to their network and hackers can access those networks, by sitting in a vehicle outside of the physician's office. This could also give the hacker access to all other physicians that are connected to the wired network. It only takes one open hole to expose the total network.

In yet another common situation, the use of POP3 mail servers from Internet providers can create vulnerabilities. As the illustration above demonstrates, an Internet Provider will commonly implement an email server at a 'COLOCATTION' site where common servers reside. This allows all the physicians to send email between their offices and 'send / receive' Internet email. This design makes it easy for physicians to use email; however, it is an inadequate security architecture.

POP3 mail servers are inherently insecure and, in most cases, the Internet Service Provider, (ISP), does not implement any kind of mail encryption for the providers. This is important because POP3 is typically sent as clear text across the wire which means a network "Sniffer" placed in the right spot can capture the data in the emails sent by physicians, i.e., capture the PHI or other sensitive information.

### 3.3.2 WHAT ABOUT VPN CONNECTIVITY?

Some ISP's provide a "secure" network by offering Virtual Private Network (VPN) connectivity. This means that any data transmitted between the ISP/COLO site will be encrypted. While this might seem to be good for security, it is important to understand what types of data may actually be transmitted to the ISP/COLO.

First, email would be transmitted. In this case, the POP3 e-mail that is usually clear text would be encrypted. That is good but, the data is only encrypted from the physician's office to the ISP/COLO. The ISP mail server then receives the message to be delivered to the recipient. The mail server sends the message in an unencrypted form to the recipients mail server and then ultimately to the users mail box on their workstation.

The second type of data that would be encrypted is general Internet surfing. So, does this truly need to be encrypted? The answer depends on the site that is visited. Remember the data is only encrypted between the physician site and ISP/COLO site.

In short a would-be hacker posing as a medical vendor renting space in the same physician plaza as physicians could probably obtain the same VPN connection to the ISP/COLO as physicians. In reality, the physician plaza has allowed the hacker to route any office traffic into any of the other offices that also connect to the VPN. This kind of routing can be protected, but MUST be managed by a certified engineer.

### Regional Health Information Organization (RHIO)

The next illustrations directly below represent a secure network design for the use and disclosure of PHI. They are entitled "Regional Health Information Organization Secure Design".

If a system for the exchange of health information is designed from the ground up to be secure, the flow of information is not a difficult task between systems. The RHIO, as conceptualized by the Federal Health Information Technology program, is a valid model to consider for the exchange of health information.

In most RHIO's, information exchange between physicians, hospitals, external labs, and external radiology centers occurs in a variety of transactions. Two basic approaches to a RHIO design are the "federated" and the "non-federated" models.

In the federated model, each individual entity's data resides in its facility. Special programs are created to search the data and aggregate it into a "Unified Electronic Medical Record". In the non-federated model, multiple entities share a common database with role based security to access the data.

Both models have pros and cons but, they both adhere to strict security policies for sharing data. In the RHIO diagram example below, it is important to notice that all

connections to the RHIO are encrypted which is a requirement for any facility sending data to the RHIO. This is already a requirement of HIPAA.

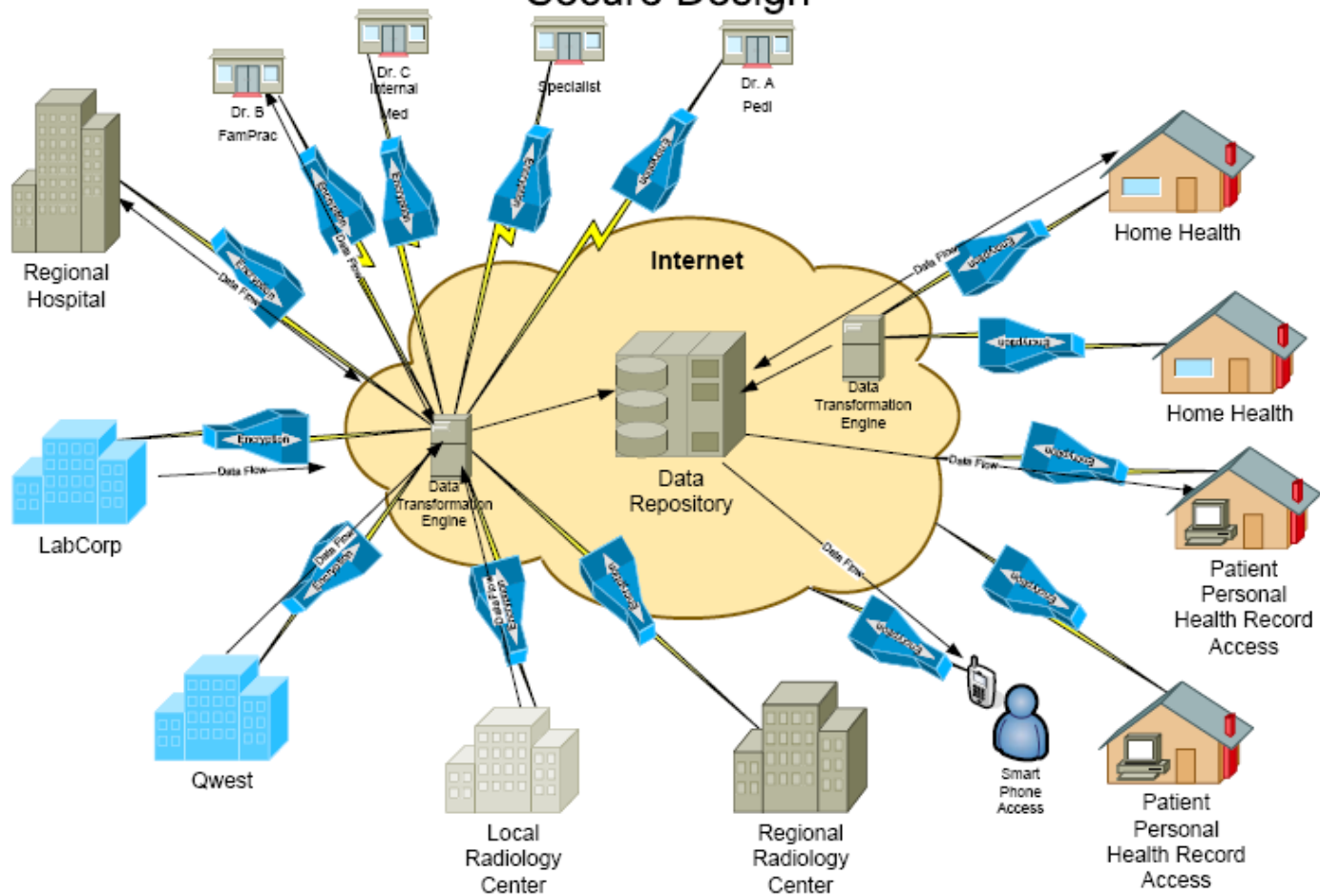
The repository itself is the data location where information sought by an identity thief or hacker would reside. Multiple layers of security should be in place at the data repository facility. The physical security of the location should use authenticated access which could be a security guard located at a sign in station, utilization of a smart card entry system, or even a biometric access technology. Each of these approaches would allow for the logging of physical access to the facility.

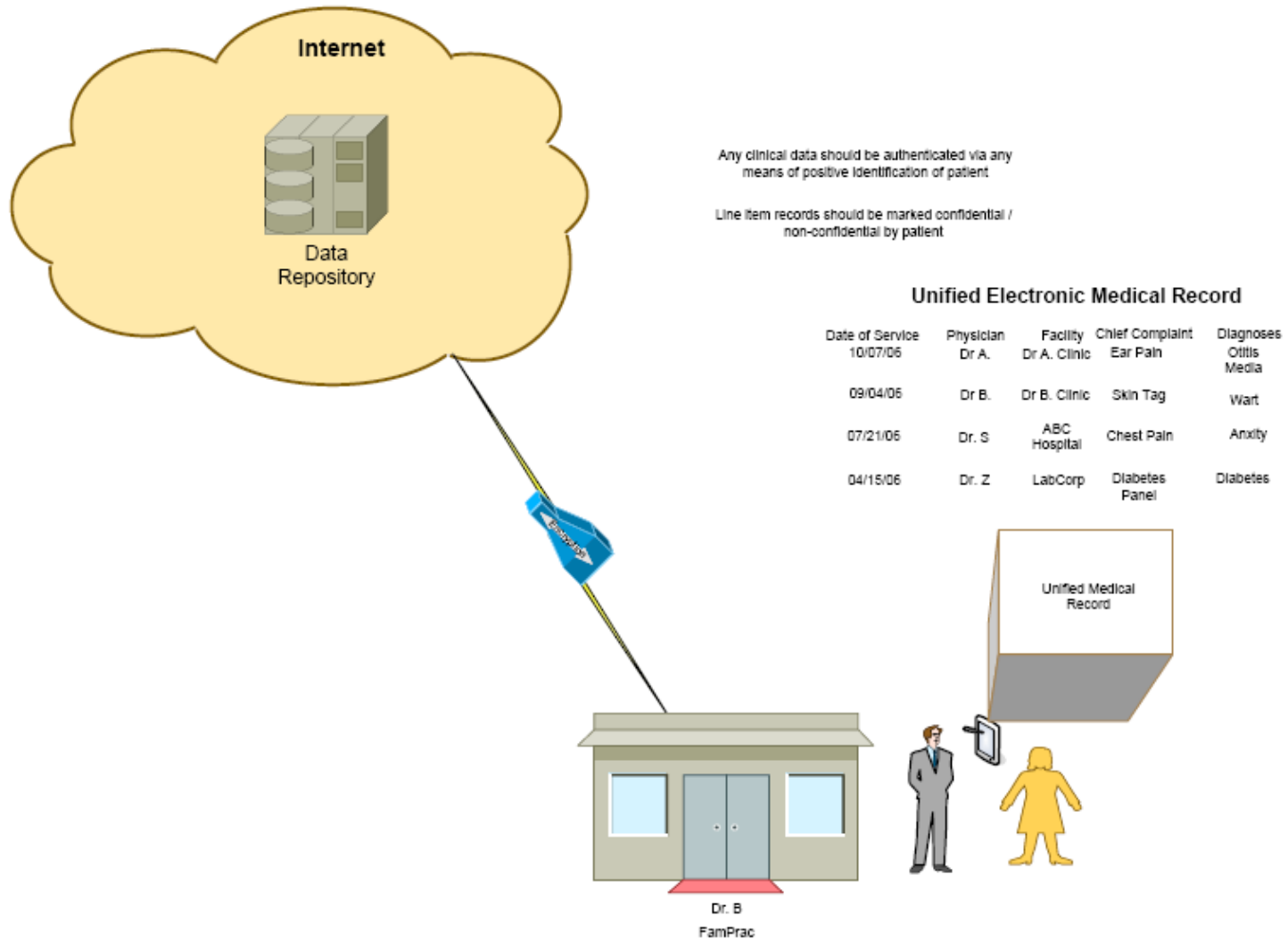
The next layer of the security component would address concerns that deal with physical connectivity to the data repository servers. Any direct connection to the Internet should include a multi-layered firewall design that is implemented with fail-over taken into consideration. Firewall access-lists should be configured such that only required servers which need to communicate with each other are allowed to do so. The communication between databases should be done with non-documented TCP ports.

Obviously, any kind of access to the server by server administrators should utilize a strong password system and when a patient or physician attempts to access the data, authentication should be mandated and logged for every view of PHI data.

These are just a few high level considerations that should be taken when considering a RHIO design that involves technological “best business practices”. A detailed security design for a RHIO such as that portrayed in the diagram below is beyond the scope of this summary document. The main points to be considered are that every level of security should be addressed from the ground up when storing PHI data in a centralized repository and security should include “best practices” for both physical and technological security.

## Regional Health Information Organization Secure Design





#### 4 "REAL WORLD SOLUTIONS"

The recommendations that follow in this section are based upon the analysis provided in this paper and would address many of the issues that have been identified as problematic.

1. Agencies with responsibility for enforcement of HIPAA should begin to actively and visibly enforce HIPAA now as a method of ensuring that health care providers and all organizations, public or private, that are subject to HIPAA are capable of handling Health Information Exchanges and Clinical Decision Support Systems, or CDSS.
  - a) Enforce HIPAA: Enforcement of any law is critical to ensuring that those who are subject to the regulations will actually obey the law. The number of recorded breaches on record since the Privacy rule was made effective in 2003, shows that enforcement is required to ensure adherence to the regulations.
    - i) Solution: create a separate auditing branch of HHS or in another regulatory body within the federal government to audit affected entities and to raise awareness that the regulations should be taken seriously.
    - ii) Work with states to ensure a minimal amount of conflict between Federal and state regulations regarding privacy of information and public access to information under Freedom of Information laws.
2. Create a set of HIPAA certification requirements that vary according to the organization. For example, a set of rules that applies to hospitals and one that applies to "hybrid entities" such as local governments and schools. This should be an official set of requirements that these organizations must clearly adhere to according to Federal regulations. In other words, a set of certifications relating to one uniform set of medical privacy and security rules, not taking into consideration the myriad of State laws that exist which may or may not be currently enforced.
  - a) Utilizing current laws such as HIPAA would greatly decrease the difficulty of this task. Standards must be uniform and complete with clear tasks that organizations must follow. For example the HIPAA security rule is general. However, when combined with other detailed authoritative standards such as ISO and industry best practices, meat can be added to the bone as it were to

create a work flow process that is translatable to the daily operations of any organization dealing with PHI.<sup>6</sup>

3. Create an audit group that is responsible for oversight of organizations based on well delineated standards. This group must be funded and able to audit organizations with an ability to levy fines or take action based on findings.<sup>7</sup> While this may seem to add bureaucracy, in fact, it can alleviate the disruption caused by litigation, identity theft, criminal prosecution and damage to individual lives.
4. For stakeholders:
  - a) Offer to assist stakeholders who are tasked with becoming HIPAA compliant. For example, promote the creation of enterprise wide software solutions, or standalone software systems that can be easily integrated into a stakeholders daily work flow that enables stakeholders to comply with the Privacy and Security regulations of HIPAA or any variation of that law. Examples of this type of resource currently exists.<sup>8</sup>
  - b) Create an integrated solution that would fit into any CDSS and would enable stakeholders to utilize CDSS systems while complying with the Privacy and Security regulations. This combined system would enable a physician to utilize a CDSS system and at the same time take the necessary steps to comply with HIPAA. This type of solution is currently under consideration and in a design mode.<sup>9</sup>

---

<sup>6</sup> RESOURCES FOR HIPAA COMPLIANCE SHOULD BE SPECIFICALLY REFERENCED TO THE CODE OF FEDERAL REGULATIONS (CFR) AND SECURITY STANDIARDS SHOULD BE BASED ON “**BEST PRACTICES**” **STANDARDS INCLUDING: ISO** — (INTERNATIONAL STANDARDS ORGANIZATION); NIST (NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY); FIPS — (FEDERAL INFORMATION PROCESSING STANDARDS) & **THE CFR** — (CODE OF FEDERAL REGULATIONS)

<sup>7</sup> When the cost of identity theft and the impact on lives and finances of data breaches is considered, investing in an audit group has the strong potential of eliminating much of the damage caused by breaches and would also encourage the implementation of technology and “best business practices” in effected entities.

<sup>8</sup> HIPAA Solutions, LC is an organization in Texas that provides resources for HIPAA compliance efforts that are focused on comprehensive and easy-to-implement compliance resources targeted to the specific requirements of HIPAA. The resources include implementation modules, tools (including a PHI tracking tool), along with more traditional services for auditing compliance status and identifying noncompliance risks. These self-implementable tools do not require consulting services and are based upon standards from ISO, FIPS, NIST and international standards for HIPAA security.

<sup>9</sup> The Southeast Texas Healthcare (SETH) Regional Health Information Organization (RHIO) is currently in development on resources that will address this situation.

- c) Promote the development of easy-to-use and cost-effective solutions with a focus on innovation and not just repackaged older solutions with a new label on them, as is the situation with many “HIPAA compliance solutions” currently available.
- d) Provide stakeholder training on the use of these systems

In conclusion, the HIPAA regulations need to be addressed and enforced to ensure stakeholders comply with these mandates.

**HIPAA SOLUTIONS, LC**

**[WWW.HIPAASOLUTIONS.ORG](http://WWW.HIPAASOLUTIONS.ORG)**

**TOLL FREE: 877-779-3004**