Project Outline

I. Introduction Project Overview
   - A. Definitions
   - B. Case stories
   - C. Re-visit last project
   - D. What we are addressing now

II. Problem
   - A. Issues in the Security of Informational Flow
   - B. Relevant Illustrations
   - C. Identifying Attackers

III. Exploration of Alternatives
   - A. Basic Features of an Information Security Plan
   - B. Examples and Internet Resources of Security Features endorsed by the Computer-based Patient Record Institute
   - C. Access Control- Firewalls
   - D. Key Management - Encryption

IV. Systemic Methodology of Implementing a Data Security Plan for CPR
   - IV A. Understanding Key Legislation
   - V B. Recognizing Human Error
   - VI C. Systems Development Lifecycle Applied to Information Security

VII
   - VIII i. Project Planning
   - IX ii. Problem Analysis
   - X iii. Solution Design
   - XI iv. Solution Implementation
   - XII v. Support, Maintenance & Training
   - XIII vi. Implementation Cost Analysiss

V. Conclusions and Recommendations

I. Introduction

A computer based patient record provides clinicians with complete accurate data and allows for greater access to patient information. In our last project we investigated ways to reduce the cost of medical records keeping and to improve access to patient records for Kaiser Permanente of Ohio.

"A hospital laboratory clerk takes her teenage daughter to work with her one day. While her mother is busy the daughter gains access to a database of emergency room patients' name, their address and their telephone number. As a prank she proceeds to call everyone on the list to inform the men they have tested positive for HIV and the women they are pregnant. She tells one patient that she has tested positive for both - that patient attempts suicide. Such real life scenarios are the catch 22 of electronic information- the benefit of greater access to medical information brings new risk to the confidentiality of sensitive clinical data" (Bard, 1).
(More detailed information)

"Security is the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit and against the denial of service to authorized users of the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats" (National Research Council, 1991).

II. Problem

One of the issues for any health maintenance organization or hospital with a computer based record system is ensuring the security of patient data. Personal health information flows to doctors, clinics and hospital for direct patient care, it is also required for support activities such as administrative and quality reviews. Commercial users of personal information examine drug user patterns for marketing and profit /risk management. In addition, insurance companies, employers, public health departments and medical researchers use health information for a variety of social reasons.

With so many parties interested in personal health information is not a surprise that consumers fear the security of their health information. "A 1996 poll by Louis Harris & Associates found that seventy-five percent of survey respondents feared their health care information would be used for purposes other than health care services. Twenty-seven reported that their medical information had been improperly disclosed at sometime and almost thirty-five percent of those who had been affected said the disclosure has resulted in embarrassment and personal harm."(Bard, 1-2).

Insiders make innocent mistakes, and some knowingly divulge patient information, while outsiders may also threaten personal health data. "Consider the following true story: A celebrity checked into a prestigious hospital in the North East for a routine procedure. After the star left the hospital, it was determined that was there was an extremely large number of "hits" to the medical record. The hospital administrator went back to the computer system to track users who accessed the medical record and proceeded to dismiss everyone who could not justify his/her access. By the time it was all over more than 50 people had been let go or severely reprimanded" (Bard, 2). "A survey by the source computer security institute in fall of 1996 showed that there were 1,810 attempts of security breeches by insiders and 1,589 attempts by outsiders to access confidential information" (Entegrity).

III. Exploration of Alternatives

There are several technological approaches to securing patient data:

Access control and user authentication and technologies:

- Passwords
- Biometric user authorization
- Tokens
- Onetime passwords
- Network authentication: ~~:~~Kerberos
- Firewalls

Data Authentication

- Digital signatures
- Biometric user authentication

Tokens dumb and smart

Key Management

- Key management ~~i~~Issues for public key cryptography
- The real time importance of key escrow

Audit Trails

- ~~—~~Digital notary time stamp services

For our purposed we will explore two technological tools for securing health information:

- Firewalls
- Cryptography

Firewalls

Definition and Explanation

"A firewall is a term used for a barrier between a network of machines and users that operate under a common security policy and generally trust each other, and the outside world"(McCurley, 1). "A firewall can significantly improve the level of site security while at the same time permitting access to vital Internet services" (Wack, 1).

For visual see Screened Host Firewall

Functions

- "Firewalls do not provide protection from inside attacks." (Wack)
- "Firewalls provides access control and user services." (Ibid.)

Cost Data

- "A firewall can actually be less expensive for an organization at in all or most modified software and additional security software could be located on the firewall."

(Wack, Concentrated Security).

- One–Day tutorial on building Firewalls is approximately $3,000 US plus (travel, lodging cost airfare, hotel, local transportation meals, etc.) for up to eight people. Additional students cost $250 US each" (Great Circle Associates, Inc.).

- "A complete firewall product may cost between $100,00 at the high end and free at the low end. The free option, of doing some fancy configuring on a Cisco or similar router will cost nothing but staff time and cups of coffee. Implementing a high end firewall from scratch might cost several man -months which may equate to 30,000 worth of salary and benefits" (Firewall FAQ, 1-2).

Encryption

Definition and Explanation

"Encryption uses mathematical formulas to scramble information like credit card numbers to make then unreadable to computer users who lack a software key that can decode encrypted data" (Bard, 3). Normally, encryption system uses some kind of "key" or "pass phrase" to "unlock" or "decrypt" the scrambled message.

In this system, two different keys are used to encrypt a message and another to decrypt the message. Then, the encryption key can be (and usually is) widely distributed, so anyone who obtains it can send an encrypted message to the person who distributed his public key. (Ultimate Privacy Corp., Order Information).

Functions

- Encryption makes it difficult for possible attackers to determine the exact length of your original message.

- Encryption protects data from both internal and external user.

Cost Data

- " A pack of 5 keys pads (which allow comm w/up to 5 people is only $49. Ultimate Privacy Personal Edition with Program Disk Manuals, 5 keypads and a year of technical support only $99. Shipping fees $9.95, good for up to five items. (Ultimate Privacy Corp., Order Information)

IV. Systemic Methodology of Implementing a Data Security Plan for CPR

In implementing a data security plan for a CPR, it is important not only to address the technology involved, but the key legislative policies that monitor the security and freedom of information access and retrieval, in addition to planning for human error in a healthcare organization.

There are numerous information acts that affect the electronic communication of patient data. These are:

- The Privacy Act of 1974
- The Emergency Medical Treatment and Active Labor Act
- The Patient Self-Determination Act
- The Freedom of Information Act
- Individual organization-wide confidentiality and security policies

Understanding the occurrence of human error in the dissemination of vital CPR data involves knowing the policies and procedures of external access to internal, confidential patient information. It is important to recognize that certain individuals and agencies seek such information to make money from using it for various unauthorized ventures. Last, there must be organizational policy in place to monitor employee disclosure of personal patient information obtained in the CPR. Strict regulation helps to prevent both accidental and purposely harmful leaks of confidential patient information to parties other than the patient and his/her designated healthcare providers. This is perhaps the larger of the two problems in assuring completely confidential CPR information.

The systems development lifecycle maps out a thorough methodology to use when implementing an information security plan for CPR in the healthcare organization. The major interactive steps of the cycle include: project planning, problem analysis, solution design, solution implementation and product support.

For a confidentiality technology project, it is important to understand the governmental and organizational laws presiding over CPR data security. There must be organization-specific documentation of information security policies, standards and procedures, accessible to all employees in the healthcare organization.

In the analysis stage, individuals involved with the project need to review the current and proposed security network architecture, assess existing security technology and document current problems. Next, the various human factors concerning security should be identified and documented. To obtain physician support, they should also be interviewed for suggestions in creating a security model based on best practices.

In the design stage, project participants develop and model the proposed security architecture with a variety of technology and organization-specific diagrams of information flow. Here, it is important to match institution-wide patient record security policies to the proposed security model. Project managers and user also need to evaluate third-party CPR security tools and develop user training for the new technology. In addition, there should be security awareness training in the client healthcare organization. Other steps to consider are developing CPR information security roles and responsibilities and standards for technology usage and upgrades.

In the implementation stage, the plan is put into action. An employee in the healthcare organization needs to designate the implementation and project management leaders. In this process, there must be constant physician involvement with the CPR security plan implementation. In order to see results, there must be previously established plan guidelines and a time line in place. Pilot tests should be run to test the security technology and to gain input regarding any changes in the organization's security policies. Organization-wide user manuals and employee training should be designed for mastery of the new technologies to secure patient CPR data. Finally, someone needs to conduct an implementation review of the project, which includes input from all clinical and administrative system users.

The last stage in the process is support, maintenance and education. Dismissing the following steps will cause the best of any technology implementation plan to fail. To begin, it is important to re-visit and evaluate the final implementation checklist. Healthcare management needs to schedule and support an ongoing CPR security awareness training program. In addition, they should designate a CPR security compliance review board, which will produce quarterly (or other time interval) progress reports. Last, human resources personnel need to review current healthcare data security personnel responsibility descriptions and update them to reflect the new secure and confidentiality plan.

In sum, all five stages of the secure plan implementation process are pertinent to its ultimate success. In essence, healthcare providers need to assure their patients of confidentiality, while utilizing the best technologies available to provide the fastest, highest quality care possible. Our systems-oriented plan addresses both human factors and technology issues for the healthcare organization planning to update its current CPR information security framework. While we found no cost data for such a specific plan, we review the estimated costs in several requests for proposal to implement an information secure plan for an organization name Proprietary Rubbish Information Systems. While customers in this business cannot suffer the embarrassment and shame of divulged personal healthcare data, the two industries share some of the basic security problems:

- Few IT security-related policies
- Poor general security awareness
- Unknown security threats

The costs of a systemic information security plan are included in the document cost.xls. ~~document cost.xls~~.

V. Conclusions and Recommendations

In following along with the systems development lifecycle, there are several take-home points:

- It is necessary to integrate CPR data security policies with the emerging, proposed security technology.
- Team involvement between physicians, other clinical staff and the system administrators is pertinent to implementing the security plan for CPR information systems.
- The security group must plan for disaster recovery of CPR data across the organization.
- Security leaders need to clarify security policies to internal and external organizations that exchange CPR data with the healthcare entity.
- Pilot tests must takes place to simulate internal and external security attacks.

- The healthcare organization leaders need to clarify and document the consequences for CPR security attacks and violations in the organizational data security policy.

Finally, while high technology devices may aid in the prevention of security attacks to CPRs, it is the responsibility of those who monitor the records to ensure confidentiality of patient information and to closely monitor and record internal behavior. In essence, "Most security problems are people problems," claims Kathleen Frawley, director of the Washington, DC office of American Health Information Management Association (Bard, 2).

"Even with the smartest technology, medical information systems can always be foiled by human behavior. If an office worker lends her password to a colleague, the principle of authentication has been violated and a security breech has occurred" (Bard, 2).

In close, those care administer the care have the most control over the confidentiality of the CPR. We may use technology as a tool to automate security controls, but we must first understand the primary principle behind our roles in implementing such devices to secure patients' CPR data: **keep it confidential**.