Managing Information Privacy & Security in Healthcare

Case Study: Immunization Information Systems at University of Pennsylvania

National Immunization Program, Centers for Disease Control and Prevention

Information Security and Immunization Information Systems

rev. February 25, 1996
prepared by

Dr. Noam H. Arzt
Research Associate/Senior Fellow, Leonard Davis Institute of Health Economics
Suite 221A
3401 Walnut Street
Philadelphia, PA 19104
215/898-3029 (Voice)
215/898-9348 (FAX)
arzt@isc.upenn.edu
URL: http://nextb.dccs.upenn.edu/noam.html

Introduction

Many states, territories, and municipalities are developing an electronic registry for immunization information (Immunization Information System, or IIS). Part of the acquisition or development of these systems is a process of dealing with threats to information security and possible steps that can be taken to mitigate these threats. Information security is defined as " ... a set of technical and administrative procedures designed to protect data systems against unwarranted disclosure, modification, or destruction and to safeguard the system itself."[1] The specific goals of this effort are:

- Maintain the integrity of the data under the Program's stewardship
- Make the data available easily to legitimate users
- Ensure the privacy and appropriate use of patient data [2]

The notion of information security and ease of access are often tradeoffs of one another: ease of access can compromise information security if not done carefully, and too much security can make an application difficult or impossible to use even by valid users. Yet many information technology professionals do not consider information security that critical. Consider a recent Ernst & Young Security Survey: Almost 50 percent of respondents rated information security issues as "less than important."[3]

Methodology

This paper describes a six-step methodology:

1. Identify the information assets that need protecting

2. Describe the architecture of the information system to be deployed

3. Identify the threats to those information assets based on the architecture

4. Rank the threats on a high/medium/low scale and identify those that are the most serious

5. Develop solutions to mitigate the threats as much as possible

6. Make specific recommendations of solutions for deployment

Information Assets

Before one can secure information, one has to identify the information itself and the reasons why a certain level of security may be necessary. An IIS database is typically described in a design document, and usually contains at minimum the core data set as defined by the National Immunization Program at the CDC. The major groupings of information are typically:

Information about People
Includes patient biographical/demographic data, aliases of names, information about relatives and guardians, immunization provider information

Information about Patient Records
Focuses on the relationship between a patient and an immunization provider

Information about Immunizations
Includes immunizations administered, normative schedule information, vaccine vendor information

Information about Registry Output Patient/family outreach information

Information about Technical Aspects
Includes system user profiles and permissions, system access logs

Code tables

Various code tables for valid values of various database elements

Medical information systems containing data that can be linked to individual patients must take precautions to prevent the inappropriate disclosure of this information, and to protect the rights of the individuals whose information is contained in the system. Specifically, the United States Department of Health, Education and Welfare articulated these responsibilities in 1973 as follows (*note additional comments in italics*):[4]

- There must be no personal data record-keeping systems whose very existence is secret.

  Notice and disclosure: need to tell a patient the data system exists, and that their data may be in there.

- There must be a way for an individual to find our what information about him is in a record and how it is used.

- There must be a way for an individual to prevent information about him that was obtained for one purpose for being used or made available for other purposes without his consent.

  The agency building the system itself needs to know how information is being used. Often a public relations brochure is helpful. A disclosure log is probably wise.

- There must be a way for an individual to correct or amend a record of identifiable information about him.

  Just because the individual suggests a correction does not mean that the original data should be removed. The suggested correction can simply be noted.

- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data. An IIS certainly qualifies as a medical information system whose policies should be sensitive to these concerns. In 1980, a federal court of appeals ruling [5] added some additional insight into balancing various factors in determining an appropriate approach to information security:

  (1) the type of healthcare record and information it contains; (2) the potential harm from any unauthorized disclosure; (3) the injury from disclosure to the relationship in which the record was generated; (4) the adequacy of safeguards to prevent non-consensual disclosure; and (5) the degree of need for access.[6]

Immunization data is not the *most* sensitive of medical information, and the potential harm from unauthorized disclosure is likely minimal. Nevertheless, Projects have a responsibility to protect the integrity of the system from inappropriate damage, and to respect the privacy of the individuals whose data is entrusted to the Project's care. Since the risk of communicable disease may be high in a given population, access to immunization information as an aid to reducing this risk is critical.

It is important, however, to recognize secondary effects that can result from improper access to the IIS, and from its improper use. Several examples illustrate these concerns: A manufacturer recall of a vaccine lot may result in patients having received vaccine that may be harmful. Inadvertent disclosure of this information improperly may violate the privacy of the patient involved.

Certain adverse reactions, or pre-existing information (such as HIV infection), may violate the privacy of a patient if disclosed improperly. While it is not its intention, the IIS has the potential to store this information if a user enters it.

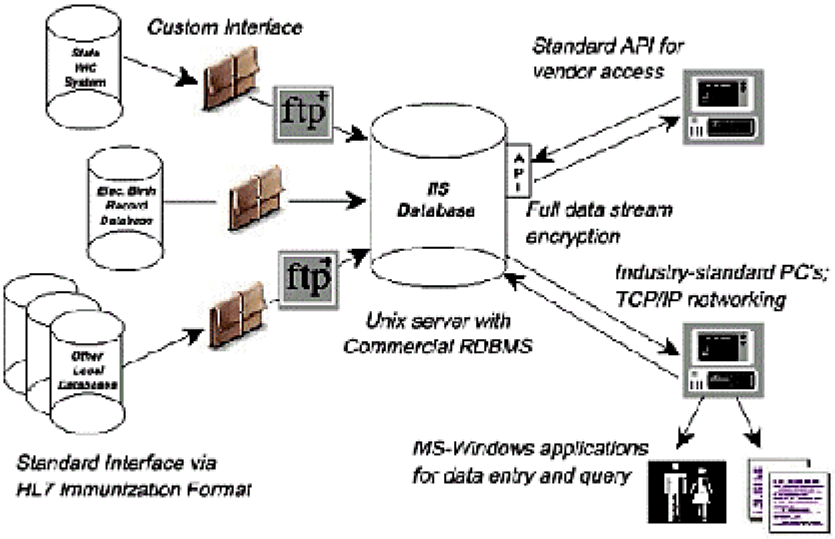
Address/contact information in the IIS could inadvertently be used to locate a parent or child improperly (e.g., cases of adoption, legal restraining order, etc.).

Policies developed for use with the IIS must address these issues. The IIS applications need to be created to support the objectives of these policies.

Individual state, territories, or municipalities may have local laws that relate to information security in general, or medical information in specific. It is important to research these local laws for applicability to the IIS project.

System Architecture

The IIS is usually deployed within a systems architecture that is often part of a larger technical architecture for the state, territory or municipality. A Technical Architecture is a blueprint for how future technology acquisitions and deployment will take place. It consists of standard, investment decisions, and product selections for hardware, software and communications. The Technical Architecture is developed first and foremost based on community direction and business requirements.



Additionally, principles are used rigorously to be sure the Technical Architecture is consistent with the community's information technology beliefs. The current (de facto) technical architecture is taken into consideration, as well as relevant industry and technology trends.

A typical systems architecture for an IIS is displayed in Figure 1.

Figure 1 - Sample IIS Systems Architecture

The major components of an architecture are:

Database
The database management system (e.g., Oracle 7) and the server upon which it runs.

Client Computers
The client computers (e.g., terminals, industry-standard personal computers) including hardware configuration and desktop operating system (if applicable).

Network Protocol
TCP/IP, SNA as appropriate.

Wide-area Network
Examples include proprietary networks, existing statewide network, the Internet.

Applications
Description of client applications, whether they are host-based or client/server - what tools are used to create them, and how they connect to the IIS database, if applicable.

Query Tools
Additional "off-the-shelf" or custom-developed/provided query tools are expected to be deployed, and their connectivity to the IIS database.

Data Collection
Methods by which data will enter the IIS, either by being "harvested" via electronic interface from a WIC system, an Electronic Birth System, or from other local data systems found in clinical provider locations.

Data Access
Eventually, an applications program interface (API) might be developed to allow vendors to write software that accesses data in the IIS for transfer to local data systems found in clinical provider locations.

User Access
Methods by which on-line users receive direct or indirect access to the IIS

Once an architecture is defined, it helps set the framework for how the information assets will be protected. It helps to identify the threats and risks that are defined in the sections that follow.

Detailed Threat Analysis [6]

A set of possible threats to an IIS have been developed. There are a number of potential threats to

Registry data. This table should be reviewed, and a ranking should be conducted of these threats on two scales:

Risk: The likelihood that the particular threat to the information identified above will take place, based on the technical architecture for the Project.

Harm: The severity of the harm if the threat in fact occurred.

In other words, just because a threat is likely does not mean its impact is severe. And just because the impact of a threat may be severe it does not mean it is likely.

Risk and Harm should be assessed for each threat below on a High (H)/Medium (M)/Low (L) scale. When the analysis is complete, the search for solutions should focus on those threats where the likelihood of the risk occurring, and the harm that might be incurred should the risk occur, are reasonably high.

Threats are divided into three categories:

Desktop: Those threats that relate to the desktop, whether it be a terminal or personal computer.

Server: Those threats that relate to the IIS server and its integrity.

Network: Those threats that relate to the network that connects users desktops to the IIS server.

Each description is followed by a rationale that describes a typical rating for each threat. The rationale for a particular IIS project may be different. The sample rationales most closely follow those of a client/server deployment.

A. DESKTOP THREATS

THREAT A-1: Unauthorized access to someone’s desktop resulting in disclosure of sensitive data that has been stored on the desktop.

RATIONALE: Sensitive data is likely either to be stored on the desktop, or visible as the IIS application is on a user’s screen. It is the deployment site’s responsibility to control physical access to desktop computers within their facilities by preventing inappropriate access to desktop computers, and by ensuring that the IIS application is not left on a computer screen unattended.

THREAT A-2: Someone finds sensitive data stored on a workstation and alters or destroys the data.

RATIONALE: Unauthorized access to medical systems is possible, and risk of alteration is present.

THREAT A-3: Someone alters the application code on the desktop making it possible to use the modified code to change data on the database server or access sensitive data on the server.

RATIONALE: The RISK is typically LOW because it is usually be very difficult to modify object modules in a way the application would still function and also access and modify data on the server. The HARM might be rated HIGH because serious damage could be done to the data on the server, and potentially go undetected.

THREAT A-4: Someone violates a software license by running unlicensed copies of software.

RATIONALE: The RISK is usually LOW because it is unlikely that an unlicensed use of software would be detected. The HARM might be rated HIGH because a commercial vendor would have legal means to significantly penalize the Project (if applicable).

THREAT A-5: The user of a desktop accidentally deletes an important local file.

RATIONALE: The RISK is often rated HIGH in client/server systems because it is easy to delete files accidentally on a workstation. The HARM is usually rated MEDIUM because while local data files are not the Project's concern, local Project software could be rendered inoperable.

THREAT A-6: Someone accidentally or intentionally infects a desktop with a virus.

RATIONALE: The RISK is usually rated MEDIUM because viruses are most prevalent on workstations and are easily transmitted via floppy disks. It is believed that a substantial number of users do not run virus protection software. The HARM is usually rated LOW because it should be possible to recover the workstation from the damage that most viruses cause.

THREAT A-7: Physical damage or destruction to a desktop (fire, broken water pipes, riot, etc.)

RATIONALE: The RISK is usually rated LOW because the occurrence of events that damage workstations is low. The HARM was rated MEDIUM because, in the event that there was destruction of a workstation, lack of off site backups and other recovery information would make it difficult to recover the data lost on the machine.

B. SERVER THREATS

THREAT B-1: Someone accesses the server and uses a program to guess passwords, or some similar tool, to find IDs and passwords that they can use to get on the system and read or alter data.

RATIONALE: The RISK varies depending on how accessible the server is. The HARM is usually rated HIGH because if someone ever did break into the server damage could be done.

THREAT B-2: Special accounts that have the authority to damage the system if not used properly, such as the root or system account, are compromised by an intruder and the intruder alters the system, sometimes with the intent of making subsequent access easier.

RATIONALE: The RISK is usually rated MEDIUM because most individuals trying to break into a system are likely to go after the special accounts. The HARM is usually rated HIGH because severe damage can be done from a special account.

THREAT B-3: System administrators with root authority (most privileged user status) use the account to make changes to the system that are not part of their responsibilities, or give themselves additional authority for future breaches of security.

RATIONALE: The RISK is usually rated LOW because it is not likely that the responsible individuals given that authority would abuse it. The HARM is usually rated HIGH because if they did abuse it, severe damage could be done.

THREAT B-4: Vulnerable accounts (dormant accounts, retired accounts, accounts without passwords, accounts with weak passwords, etc.) are used to gain access to data or set up future access to the system.

RATIONALE: The RISK is usually rated MEDIUM because people trying to break into an account also target carelessly managed accounts. The HARM is usually rated MEDIUM because these accounts typically don't have the authority to damage the system.

THREAT B-5: Someone obtains an ID with authorization beyond what they should have been granted and uses it to read or delete files or to make changes to allow future access to the system.

RATIONALE: The RISK is usually rated LOW because there would be sufficient administrative policies in place to prevent such a request from being made with out the proper authorization. The HARM is usually rated MEDIUM because the account still would not be a special account and the potential for damage is not high.

THREAT B-6: An intruder gains access to a machine and has been detected. The system administrator is unable to determine what damage was done, and so cannot recover from the damage.

RATIONALE: The RISK is usually rated MEDIUM because there are a number of people attempting to break into systems, and there is a good chance the intrusion could change something that would go undetected. The HARM is usually rated LOW because most break-ins are not made with the intent of damaging the system and the account that would be compromised is not likely to be a special account.

THREAT B-7: Someone who has access to the system as part of their job responsibilities uses that access to destroy data or programs.

RATIONALE: The RISK is usually rated LOW because there are usually a small number of people with direct (i.e., logon access) to the system. The HARM is usually rated LOW because they don't usually have the authority or knowledge to find programs or files that they shouldn't have access to.

THREAT B-8: Someone who has access to the system as part of their job responsibilities uses that access to find and modify source code in order to execute it to make changes or read data they were not authorized to access.

RATIONALE: The RISK is usually rated LOW because it is unlikely that the user would be able to locate or change code to work as the planned. The HARM is usually rated HIGH because if they were successful, they could do severe, undetected damage to the integrity of the data.

THREAT B-9 Someone exploits weaknesses of network mounted file systems or NIS IDs or passwords and modifies or reads data not intended for them.

RATIONALE: The RISK is usually rated LOW because these services are not usually activated on an IIS server. The HARM is usually rated MEDIUM because it is unlikely valuable data will be NFS mounted or that an ID compromised would be a special account.

THREAT B-10: A user accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated LOW because the amount of damage an individual user can actually do to IIS data is usually fairly limited. The HARM is usually rated LOW because it should be possible to restore most files from a system backup.

THREAT B-11: A user with System Administrator responsibilities accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that *some* errors will be made at some point in maintaining or deleting files. The HARM is usually rated HIGH because deleted files could impact the Project while waiting for it to be restored or rebuilt or if it couldn’t be rebuilt.

THREAT B-12 A Production Control employee accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that *some* errors will be made at some point in maintaining or deleting files. The HARM is usually rated HIGH because deleted files could impact the Project while waiting for it to be restored or rebuilt or if it couldn’t be rebuilt.

THREAT B-13: A data base administrator)/system administrator accidentally deletes or corrupts data or software in performing their job responsibilities.

RATIONALE: The RISK is usually rated MEDIUM because it is likely that errors will be made in maintaining or deleting files. The HARM is rated HIGH because deleted files could affect the Project while waiting for it to be restored or rebuilt or if it couldn’t be rebuilt.

THREAT B-14: A virus is accidentally placed on the system by someone performing their job responsibilities.

RATIONALE: The RISK is usually rated LOW because server viruses are rare in most multi-user operating systems, and the ability to introduce them to the environment is limited (no floppy disks used, FTP is limited). The HARM is usually rated LOW because most viruses are not written to destroy data, and it is unlikely that the virus would do more than cause a minimal outage.

THREAT B-15: The server is destroyed or incapacitated by riots, flood, burst pipes, fire, power failure/surge, etc.

RATIONALE: The RISK is usually rated as MEDIUM because experience shows that problems such as leaking pipes and power failures are not exceedingly rare. The HARM is usually rated as HIGH because many services rely heavily on a few key servers.

C. NETWORK THREATS

THREAT C-1: Someone spoofs network addresses to gain access to servers, and uses that access to read/alter data or set up future access. Network spoofing involves someone having their host computer "impersonate" a trusted computer, thereby improperly gaining special permissions that only the trusted computer should have.

RATIONALE: RISK is usually rated LOW because it data, when stored in a commercial RDBMS, is not easily interpreted. HARM is usually rated HIGH since if the data were acquired and disseminated, it could pose a serious legal threat or harm to the Project.

THREAT C-2: Someone uses a packet sniffing tool (a software package which allows a computer connected to the network to view data intended for another host computer) to read sensitive medical data being transmitted over the network.

RATIONALE: The RISK is usually rated only MEDIUM because even in the most promiscuous of networks, the difficulty of interpreting data as it travels the network mitigated the likelihood that someone would attempt this. The HARM is usually rated HIGH because of the legal ramifications of disclosing sensitive data.

THREAT C-3: Someone uses a packet sniffing tool to capture accounts and passwords to gain access to host systems containing sensitive medical data.

RATIONALE: The RISK is usually rated HIGH because the Computer Emergency Response Team reported in the Spring of 1994 that there was a high incidence of such attacks on networks, and that the accounts compromised numbered between the tens of thousands and hundreds of thousands. It is significantly easier to "sniff" for account access information than for actual transactions. The HARM is usually rated HIGH because of the extensive harm that someone could do by gaining access to numerous users'or system administrators' accounts.

THREAT C-4: Intentional denial of network service. Denial of network service is defined as interference with the availability of any part of the network or its services. This threat considers denial of service only by logical means through the network (for example by flooding a network with messages). Physical denial of service attacks (physical harm to network infrastructure) are considered separately in Threat C-8.

RATIONALE: The RISK is usually rated LOW because it is thought to be relatively unlikely that anyone could intentionally deny widespread network services through logical means. The HARM is usually rated as HIGH because it was thought that if anyone could actually inflict a widespread network outage, many services on a functioning network.

THREAT C-5: Break-in through the dial-up modem pool. This threat considers the possibility of an intruder somehow gaining unauthorized access to the network by coming in through the dial-in modem pool. This might be accomplished by guessing a Network Authentication System ID and password, by an authorized user sharing his or her network password, or by an authorized user writing down his or her network password and having it disclosed.

RATIONALE: The RISK is usually rated as MEDIUM because it is often common for account holders to share their password. The HARM is usually rated as LOW since further access to network connected hosts is required before actual harm can be inflicted.

THREAT C-6: Unauthorized access through an insecure modem pool. It is possible that there may be modems or modem pools providing network access without requiring a password.

RATIONALE: The RISK is usually rated as LOW because if there are any such unauthenticated modems, it is not likely that their use is widespread, or widely known. The HARM is usually rated as LOW because further access to network-connected hosts is required before actual harm can be inflicted.

THREAT C-7: Accidental denial of network service. This threat considers a denial of service only by logical means (e.g. incorrect configuration of network components.). Denial of service by physical means is considered in threat C-8.

RATIONALE: The RISK is usually rated as MEDIUM because experience has indicated that network outages can sometimes be caused by such errors. The HARM is usually rated as LOW again because experience has indicated that generally such outages are brief in duration, and easily remedied.

THREAT C-8: Accidental or intentional denial of network service by physical means (e.g. riots, flood, burst pipes, fire, power outages, etc.).

RATIONALE: The RISK is usually rated as MEDIUM because experience shows that problems such as leaking pipes and power failures are not exceedingly rare. The HARM is usually rated as HIGH because a Project usually relies heavily on a functioning network.

Summary of Important Threats with Possible Solutions

Once the most serious threats are identified in the analysis above, some possible solutions are developed to mitigate these threats wherever possible. Here is a typical set of serious threats and possible solutions developed for one State IIS project deployed in a client/server architecture:

1. **Data in inappropriately disclosed or altered based on access to the IIS software** (Threats A-1 and

A-2): Inappropriate access to a "live" IIS client inherently brings potential for disclosure or alteration of data.

Solutions

Develop an information security policy that addresses these concerns, and includes descriptions of appropriate behavior and sanctions for inappropriate behavior.

Develop the IIS application security with security profiles to only allow a given user to access and/or modify data appropriate to his or her role in the organization.

Promote awareness and good behavior to reduce the occurrence of IIS applications being left unattended in clinical settings.

2. **An important local file is deleted** (Threat A-5): Since client/server systems, especially those deployed over wide-area networks, will require some software to be located on the client desktop computer, there is reasonable risk that critical files could be lost or damaged at the provider site. Desktop computers at provider sites are the *least* controlled part of a client/server architecture.

Solutions:

Develop an information security policy that requires regular data backups and compliance to participate in the Project.

Purchase and install software (or hardware) to secure Project files on provider site desktops. Encourage sites to install Project software on local file servers that are likely better maintained and backed-up than individual desktops.

3. **Attack on the server via the Internet** (Threats B-1 and B-2): Servers on the Internet are an attractive target for some individuals whose goal it is to read or alter data inappropriately or find an undetected location from which to perpetrate other exploits.

Solutions:

Restrict the number of network services that are co-existing with the database server as much as possible.

Install the most secure version of the basic operating system as possible, and keep all security patches up-to-date. Specifically, use "secure" versions of operating systems (including shadow password files), one-time passwords (via smart card) [e.g., SecureID] or software [e.g., S/Key or Kerberos])

Install utilities that require frequent password changes, that enforce rules against easily-guessable passwords, and that scan the system for easily-guessable passwords.

Restrict access to the database server from certain network locations (either by inclusion or exclusion).

Deploy a network firewall to best protect the server from attack.

4. Inadequate System Administration (Threats B-11, B-12, and B-13): Multi-user operating systems and commercial RDBMS software packages are difficult products to learn, master, and maintain properly. Unless managed very carefully, data can be corrupted or inappropriately disclosed due to administrator or operator error or ignorance.

Solutions: I

Invest in necessary training for all systems staff.

Be sure necessary staff are cross-trained to provide sufficient backup for critical skills.

5. Physical threats to server or network (Threats B-15 and C-8): Environmental threats are always a concern, especially in a wide-area implementation with a diverse set of sites.

Solutions

Locate server in a secure machine room.

Provide upgraded environmental conditions wherever the server is located, including uninterrupted power supply, redundant network connections, and redundant systems in different locations. Implement a proper backup procedure, including off-site storage of backup media, to facilitate recovery from a catastrophic failure or accident.

6. Promiscuous monitoring of network traffic (Threats C-2 and C-3): Unscrupulous individuals may choose to monitor network traffic with the hopes of either capturing usernames and passwords to be used to attack systems, or to capture sensitive medical data inappropriately.

Solutions:

Encrypt all data as it passes across the network.

Restrict database access from the public Internet by providing connectivity between the server and clients *behind* a firewall.

Recommendations

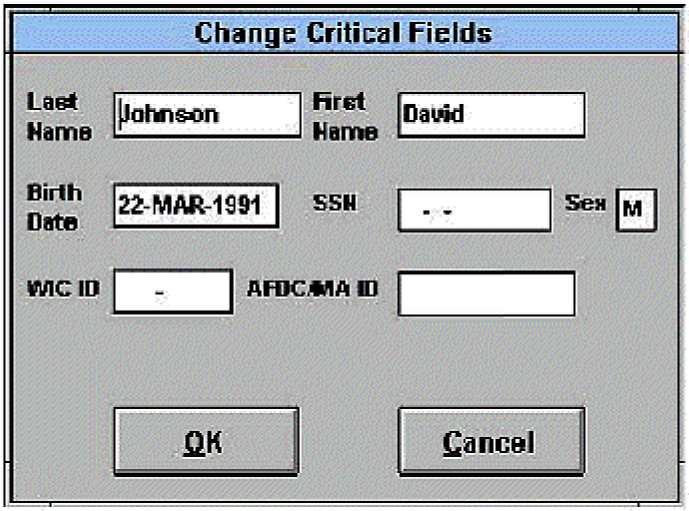
The set of possible solutions needs to be examined and analyzed. Specific recommendations then need to be made based on the technical, political, and financial constraints of the Project.

Here is a typical set of serious threats and possible solutions developed for one state IIS project deployed in a client/server architecture based on the possible solutions the Project developed above: Policy: Develop an information security policy that delineates the roles and responsibilities of the Project staff and participants with respect to the IIS and its data. Include appropriate procedures to ensure local site data and software are properly managed.

Create Security Levels for Applications: At least three security levels should be created:

- *General Reader:* Can view data on children but cannot add or modify data; limited access to standard reports; no access to outreach processes.
- *General User:* Can view and modify data on children *except* for "critical fields"; cannot add new children; limited access to standard reports and outreach processes.
- *Site Manager:* Can view and modify all data on children, including "critical field"; can add children; full access to all standard reports and outreach processes.

In this example, "critical fields" are defined as those fields required to establish the uniqueness of a record in the IIS. An IIS application might have a restricted screen or panel for addition/update of these fields:

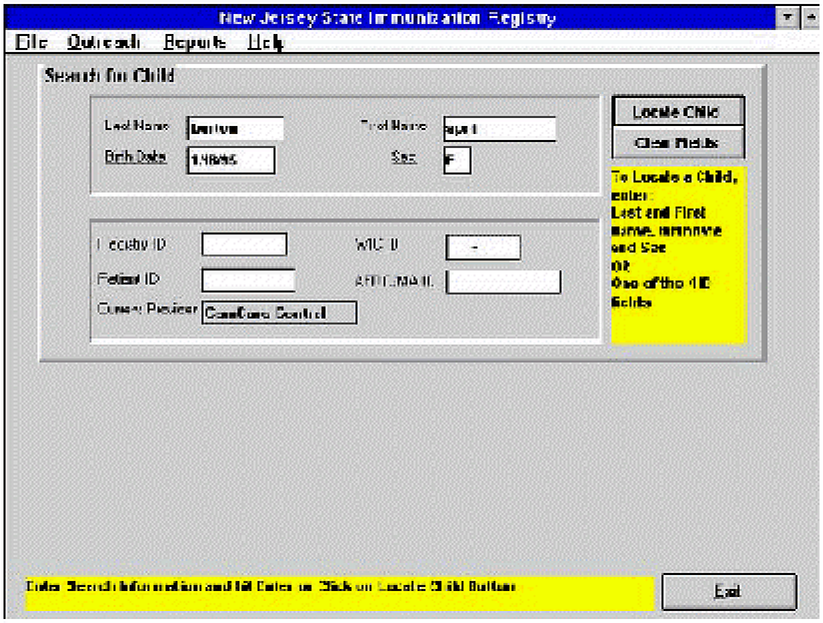


Change Critical Fields

Last Name: Johnson
First Name: David
Birth Date: 22-MAR-1991
SSN: - -
Sex: M
WIC ID: -
AFDC/MA ID:

figure 2

Similarly, a look-up screen for an IIS record might restrict simple, free browsing to ensure confidentiality of records:



Last Name: [illegible]
First Name: [illegible]
Birth Date: [illegible]
Sex: F
Registry ID:
WIC ID: -
Patient ID:
AFDC/MA ID:
Current Provider: [illegible]

To Locate a Child, enter: Last and First name, birthdate and Sex OR One of the 4 ID fields

Enter Search Information and hit Enter or Click on Locate Child Button

figure 3

Note that on this application screen, a user must know specific information about the record being requested, and will not be shown any identifying information by the application that the user did not provide once a record is found.

Harden Server Against Network Attack: Several steps can be taken to harden the server against attack from the Internet:

- Keep operating system version current with all necessary security patches
- Install the "trusted" version of the operating system on the database server
- Remove any unnecessary services
- Implement frequent password aging and enforce non-guessable passwords
- Deny file transfer access to all accounts that do not require it
- Frequently audit system for security exposures
- Audit system services and access, and review audit logs for questionable events
- Purchase SQL<>Secure to provide user-changeable database passwords
- Purchase one-time password generator and smart cards for Project staff who require terminal-to-host connections for administrative functions.

Train Staff Appropriately: Appropriate systems and operations training needs to be provided for staff, including backup personnel. Consulting assistance needs to be provided when necessary.

Physically Secure the Server: The database server should be kept in a locked facility, alarmed whenever left unattended. Uninterrupted power should be provided. Data backups (including off-site storage of backup media) should be in place and functioning. Restoration from backups should be periodically tested.

Prevent Promiscuous Access to Data: Implement products to encrypt the full client/server data stream to prevent even accidental disclosure of data by promiscuous capture on the network.

Summary and Conclusions

Information security is a serious topic and requires serious consideration at all stages of a Project's planning and implementation. The structured methodology described in this paper is not the only approach, but it does try to balance the need for a secure system with the realities of Project pressures and cost.

1 Lawrence O. Gostin *et al.*, "Privacy and Security of Personal Information in a New Health Care System," *Journal of the American Medical Association*, 270(20), Nov. 24, 1993, p 2487.

2 *Idem.*

3 Ernst & Young/Information Week, "2nd Annual Information Security Survey," Sept. 1994.

4 Based on a presentation by Dr. Christine Harbs, All Kids Count National Program Meeting, Atlanta, GA, March 3, 1995.

5 *United States v Westinghouse Electric Corp,* 638 F2d 570 (3rd Cir 1980). 6 Gostin, *et al.*, p. 2489.

6 Based on a framework developed at the University of Pennsylvania in the fall of 1994.