

---

## **Public Key Infrastructure Analysis**

### **Electronic Prescriptions for Controlled Substances Healthcare IT Infrastructure Analysis**

**Prepared for**

**Drug Enforcement Administration  
Office of Diversion Control  
600 Army Navy Drive  
Arlington, Virginia 22202**

**In response to  
Assist 5C-A-JMD-0072-DO-220**

**May 26, 2000**

**Prepared by  
PEC Solutions, Inc**

---

## Table of Contents

	<b>Page</b>
<b>Section 1 – Introduction.....</b>	<b>1–1</b>
1.1 Overview and Background .....	1–1
1.2 Mission of the Office Of Diversion Control.....	1–1
1.3 Document Organization.....	1–2
1.4 Description of Network Infrastructure Analysis.....	1–3
1.5 Analysis Methodology.....	1–4
1.5.1 Industry Stakeholder Groups Defined.....	1–4
<b>Section 2 – Industry Prescription IT Environment.....</b>	<b>2–1</b>
2.1 Current Prescription Process.....	2–1
2.1.1 Standards for Electronic Prescriptions.....	2–2
2.1.2 Insurance Checks and Prescription Claims Adjudication.....	2–2
2.2 Stakeholder Information Technology Services.....	2–3
2.2.1 Practitioner IT Environment .....	2–4
2.2.1.1 Practitioner System Architecture .....	2–5
2.2.1.2 Practitioner Network Architecture.....	2–6
2.2.1.3 Practitioner IT Management .....	2–7
2.2.1.4 Practitioner IT Safeguards .....	2–7
2.2.1.5 Practitioner Use of PKI.....	2–8
2.2.2 Pharmacy IT Environment.....	2–9
2.2.2.1 Pharmacy System Architecture.....	2–9
2.2.2.2 Pharmacy Network Architecture.....	2–12
2.2.2.3 Pharmacy IT Management .....	2–13
2.2.2.4 Pharmacy IT Safeguards .....	2–13
2.2.2.5 Pharmacy Use of PKI.....	2–15
2.2.3 Hospital IT Environment .....	2–15
2.2.3.1 Hospital System Architecture .....	2–16
2.2.3.2 Hospital Network Architecture.....	2–17
2.2.3.3 Hospital Organization Management .....	2–17
2.2.3.4 Hospital IT Safeguards .....	2–17
2.2.3.5 Hospital Use of PKI.....	2–19
2.3 Electronic Prescription Design.....	2–19
2.3.1 Internet Healthcare Portal .....	2-19
2.3.2 Closed System.....	2-19
2.3.3 Switched Service Network.....	2-20

<b>Section 3 – Analysis and Derived Requirements .....</b>	<b>3-1</b>
3.1 DEA High Level Design Requirements/Constraints .....	3-1
3.2 Controlled Substances Business Process Requirements .....	3-2
3.3 IT Infrastructure Requirements .....	3-4
3.3.1 Network Architecture Requirements .....	3-4
3.3.2 Systems Architecture Requirements .....	3-5
3.4 IT Organization, Administration and Technical Support Requirements .....	3-6
3.5 Information Technology Security Requirements .....	3-6
3.5.1 Physical Security and Disaster Recovery Requirements .....	3-6
3.5.2 Logical Information Technology Security Requirements .....	3-7
3.5.3 Information Technology Security Policy and Auditing Requirements .....	3-7
3.6 Current Use of PKI and Encryption Technologies .....	3-7
<b>Section 4 – Background and High Level Requirements Table .....</b>	<b>4-1</b>
<b>Appendix A – Requirements Interviews List.....</b>	<b>A-1</b>
<b>Appendix B – Documents Reviewed.....</b>	<b>B-1</b>
<b>Appendix C – Listing of Acronyms .....</b>	<b>C-1</b>
<b>Appendix D – Veterans Health Administration IT Environment .....</b>	<b>D-1</b>

## List of Exhibits

		<b>Page</b>
1-1	Prescription Dispensing Environment .....	1-2
2-1	Prescription Process.....	2-1
2-2	Typical Practitioner Systems Architecture .....	2-5
2-3	Practitioner Hardware/Platform Matrix .....	2-6
2-4	Practitioner IT Safeguards .....	2-7
2-5	Typical Pharmacy System Architecture.....	2-10
2-6	Pharmacy Hardware/Platform Matrix.....	2-11
2-7	Pharmacy Network Connections.....	2-12
2-8	Summary of Pharmacy Network Architectures .....	2-13
2-9	Pharmacy IT Safeguards .....	2-13
2-10	Typical Hospital System Architecture .....	2-15
2-11	Hospital Hardware/Platform Matrix .....	2-17
2-12	Hospital Safeguards .....	2-17
2-13	Switched Service Network Model for Electronic Prescriptions .....	2-20
4-1	High Level Business and System Requirements Table .....	4-2

## Section 1—Introduction

### 1.1 Overview and Background

The goal of this document is to capture the Information Technology (IT) environment of the prescription process stakeholders. This document identifies and evaluates existing facilities, hardware platforms, systems software, communications infrastructure, and software applications used by industry.

Under the authority of the Controlled Substances Act of 1970, the Drug Enforcement Administration (DEA), Office of Diversion Control (OD) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. *Title 21, Code of Federal Regulations, 1300 to the end*, sets forth in detail the authority and responsibilities of DEA in this area. It is further intended that their systems prevent the introduction of contraband controlled substances into the legal distribution channels.

The Government Paperwork Elimination Act of 1999 (Title XXII of Public Law 105-277) mandates that Federal agencies allow for the option of electronic submission of required records and for the use of electronic signatures when practicable.

The DEA plans to modify their regulations to permit the electronic transmission of controlled substance prescriptions between practitioners and pharmacies that employ Public Key Infrastructure (PKI) technology. This technology will bring to this process the following advantages: (1) reduce the amount of paper in the process (2) reduce errors due to illegible handwriting (3) speed transaction times (4) lower costs per transaction and (5) introduce security services into the process.

The security services include those inherent in any PKI: (a) *confidentiality of communications*- only authorized persons will be able to read encrypted communications; (b) *authentication of sending party*- the recipient will be able to positively identify the sender of a communication and subsequently to demonstrate to a third party, if required, that the sender was properly identified; (c) *integrity of communications*- it will be possible for the recipient of a message to determine if the message content was altered in transit; (d) *non-repudiation*- the originator of a message can not convincingly deny to a third party that the originator sent it.

### 1.2 Mission of the Office of Diversion Control

*Title 21, Code of Federal Regulations, 1300 to the end*, defines the registration, record keeping, inventory, order processing, prescribing, and miscellaneous activities as they relate to controlled substances. Persons who wish to participate in a controlled substance business activity, i.e. manufacturing, distributing, dispensing, research, narcotic treatment programs, import, export, are required to register with the DEA unless otherwise

exempted from registration described in §1301.22. Registrants fall into two categories, A-Type registrants and B-Type registrants.

The electronic prescription project focuses on specific A-Type registrants—retail pharmacy and practitioner. The project will review the relationships and processes as they pertain to controlled substance prescriptions. The project will ultimately determine how the DEA’s regulations can be modified to allow for the electronic transmission of controlled substance prescriptions through the use of a PKI. Exhibit 1-1 illustrates the current prescription dispensing environment.



**Exhibit 1-1. Prescription Dispensing Environment**

### 1.3 Document Organization

The document is organized into the following sections:

**Section 1-** The introduction provides a description of this task and provides an overview of the goals and objectives of the task.

**Section 2**—This section provides the data and findings produced by the interviews, meetings, seminars, document reviews and site visits.

**Section 3**—This section provides an analysis of the data and findings to derive the requirements for the electronic transmission of controlled substance prescriptions.

**Section 4**—This section provides a table of high level requirements.

**Appendix A**—Listing of Interviews, Site Visits, Meetings and Conferences

**Appendix B**—Listing of Documents Reviewed

**Appendix C**—Listing of Acronyms

**Appendix D**—Veterans Health Administration Information Technology Environment

## **1.4 Description of Network Infrastructure Analysis**

### **Infrastructure Analysis Task 2.2.2**

The goal of this document is to capture the Information Technology (IT) environment of the prescription process stakeholders. This document identifies and evaluates existing facilities, hardware platforms, systems software, communications infrastructure, and software applications used by industry. The DEA plans to modify their regulations to permit the electronic transmission of controlled substance prescriptions between practitioners and pharmacies by employing PKI technology. Stakeholders may employ complex and expensive IT infrastructures to gain advantages over competition, improve workflow, or improve profit margins. Any changes that are proposed to the current *Code of Federal Regulations* (CFR) would need to account for existing networks and technologies. This is crucial because acceptance of this technology by the stakeholders depends on a number of factors that can include perceived benefits, initial and recurring costs, ease of use, and the ability to leverage existing investments in these networks and technologies.

This analysis will identify the IT requirements based on the information that was collected through research and interviews with the stakeholders. These requirements along with security requirements will provide the basis to proposed changes to the CFR. As part of the DEA electronic prescription program, a Pilot will be constructed to evaluate the effectiveness of the proposed changes. The Pilot is planned to be performed at a Veterans Administration (VA) outpatient pharmacy environment.

This document provides an overview of the IT architectures industry is currently employing; and provides an understanding of VA technology that is representative at their hospital locations. To validate the effectiveness of the proposed regulation changes, this Pilot environment will need to be representative of the industry IT environment. Information contained within this document captures the current VA IT environment and provides a basis for the design of the VA pilot system. With this information, VA pilot

readiness can be determined, the systems that will be PKI enabled can be selected, and project critical path events can be identified.

## **1.5 Analysis Methodology**

The six-step methodology used for this analysis is listed below:

- (1) Interviews with selected DEA and industry representatives.
- (2) Review of documents recommended by DEA and industry.
- (3) Visit to VA medical center and review of VA IT infrastructure information.
- (4) Interviews with vendors.
- (5) Follow-up of leads and sources developed during (1-3) above.
- (6) Questionnaires submitted to selected industry representatives.

Appendix A of this document contains the listing of all interviews conducted, site visits made, and conferences and meetings attended in the preparation of this analysis. Appendix B contains a listing of all documents reviewed in preparation for this analysis.

### **1.5.1 Industry Stakeholder Groups Defined**

The dispensing activity—as defined in CFR §1300.01 and §1301.13—applies to retail pharmacies, hospital/clinics, practitioners, teaching institutions, and mid-level practitioners. Stakeholders for this project are parties that have an interest or share in the retail pharmacy prescription process. Specifically, this includes; 1) regulators, (DEA and state organizations), and 2) industry, which include practitioners and pharmacists.

#### **Pharmacists**

Pharmacy organizations—including chain pharmacies, community/independent pharmacies, pharmacy associations, and integrated health delivery systems—were contacted for interviews. Information collected included: current business policies and practices, information technology (IT) infrastructure, and IT security that are currently in place at pharmacies.

#### **Practitioners**

Registered practitioners (including registered mid-level practitioners) have the authority to prescribe controlled substances in the course of their professional practice. Practitioners interviewed included members of associations, private practices, hospital/clinic practitioners, and practitioners associated with integrated health delivery systems. Information collected included: current business policies and practices, IT infrastructure, and IT security.

## **Hospitals**

Hospitals and Integrated Delivery Networks (IDNs) usually have all of the health care components located in one facility. An example of an IDN is an HMO provider like Kaiser Permanente that also provides integrated health care services—typically in one location. The VA falls into this category. Hospital staff and representatives for IDNs were interviewed to document workflow and current technology employed.

## **State Regulatory Organizations**

State regulatory organizations such as State Controlled Substance Authorities, Diversion Control Units, and State Boards of Pharmacy play an important role in regulating pharmacy operations. State agencies were interviewed to gather information regarding current laws and regulations, business flow, diversion problems, along with any concerns and ideas regarding an electronic prescription system for controlled substances.

## **Drug Enforcement Administration (DEA)**

The OD's mission is to limit diversion while maintaining adequate supplies for medical purposes. The DEA enforces regulations that practitioners and pharmacies must adhere to when prescribing and dispensing controlled substances. DEA has the authority to conduct administrative and criminal investigations. DEA representatives were interviewed to collect information on DEA's mission in the Office of Diversion Control with regard to regulating, preventing diversion, investigating/auditing, and prosecution.

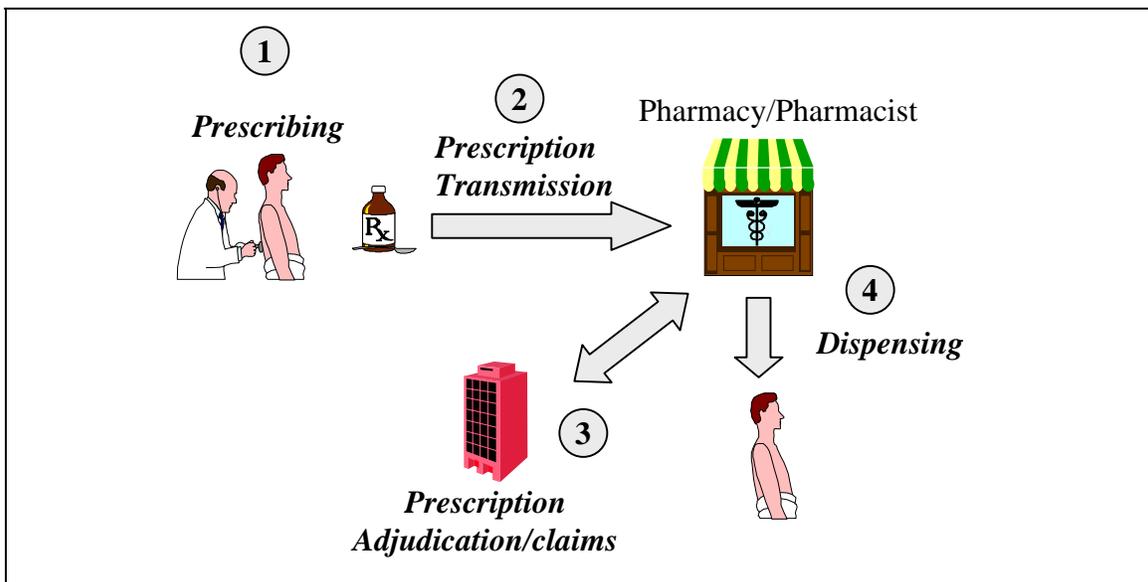
## Section 2—Industry Prescription IT Environment

This section provides information on relevant aspects of IT environments found in the healthcare industry that impact the DEA's electronic prescription project. This section will identify industry IT environments that electronic prescriptions must interoperate with including 1) practitioner, 2) pharmacy, and 3) hospitals/Integrated Delivery Networks (IDN). These three stakeholders will bear the impact of any changes to DEA regulations. This section focuses on their IT environment to ensure that the proposed regulations do not neglect their investment in or reliance on this IT infrastructure.

Section 2.1 provides a high level description of the existing controlled substance prescription business process. The remainder of Section 2 provides technical information about existing IT environments. Additional technical details on the VA's IT environment—as it impacts the Pilot—are provided in Appendix D.

### 2.1 Current Prescription Process

The fundamental elements of the prescription business process are shown in Exhibit 2–1.



**Exhibit 2–1. Prescription Process**

The following paragraphs provide more detail concerning this process.

**1) The practitioner prescribes medication**—An authorized practitioner prescribes the medication for the patient. Traditionally this is performed in a healthcare provider's office or hospital setting. Practitioners are beginning to adopt the use of desktop computers and portables as they slowly move away from the traditional method of hand-written

prescriptions.

**2) The patient presents the prescription to the pharmacy**—The patient presents the prescription to the pharmacy clerk or technician. Telephones and fax machines are used as alternate methods of transferring prescription data to the pharmacy. Electronically transmitted prescriptions are increasing in use, as more practitioners begin to use electronic systems within their practice—however their current use is limited to a small number of practitioners.

**3) The prescription is reviewed by the pharmacy**—The pharmacist is obligated by government regulations to verify the validity of the prescription. The pharmacist also performs a Drug Utilization Review (DUR) to ensure that the prescribed medication does not conflict with other medications the patient may be taking. If being paid for by a third party, the pharmacy adjudicates the prescription. During adjudication, prescription information is typically sent to a switch that forwards the request to the appropriate Pharmacy Benefits Manager (PBM). The PBM verifies the patient and prescription's eligibility (as explained in 2.12 below).

**4) The medication is dispensed to the patient**—Once the prescription is filled, the pharmacist presents the medication to the patient (or agent). It is now common for patients to receive medications through the mail—especially for maintenance drugs.

### **2.1.1 Standards for Electronic Prescriptions**

The National Council for Prescription Drug Programs' (NCPDP) SCRIPT standard was developed for the purpose of transmitting prescription information electronically between a practitioner and pharmacy. The American National Standards Institute (ANSI) recognizes NCPDP as an accredited standards organization. The SCRIPT standard adheres to Electronic Data Interchange For Administration Commerce And Transport (EDIFACT) and Accredited Standards Committee (ASC) X12 standards. EDIFACT and X12 are widely accepted by the healthcare industry for EDI transactions. The SCRIPT standard is currently in release 5, version 1—released in August 1999. The first version of the SCRIPT standard was published in April 1997.

### **2.1.2 Insurance Checks and Prescription Claims Adjudication**

Third parties maybe involved if a third party insurer is paying for a prescription. The third party participants that make up the prescription adjudication and medical claims network are not directly involved in the prescribing and dispensing of medication. They are important because they are common to both the pharmacy and the prescribing clinician. Prescriptions

- **PBM**—Before a pharmacy fills a prescription, the prescription must be adjudicated to ensure that it is payable under the patient's insurance plan. PBMs are paid by insurance companies to provide pharmacies with insurance

information including formulary, pricing, and eligibility information. These EDI transactions are submitted using the NCPDP TELCOM Standard.

- **Pre and Post edits (adjudication)**—Pre and post adjudication editing systems screen claims transactions before they are sent to a PBM in an effort to maximize profit and minimize data formatting errors.
- **Switch**—Switches maintain connections to all major PBMs and route pharmacy claims to the appropriate PBM for processing. Switches provide electronic capture, transmission and storage of time-sensitive data for the healthcare industry in both real-time and batch modes. Switches maintain large, robust data backbones that are able to support the tremendous volume of prescription transactions.

## 2.2 Stakeholder Information Technology Services

PEC interviewed doctors, pharmacists, and representatives of hospitals and IDNs to develop an understanding of their current IT architecture. The IT architecture can be described in terms of the following elements—bulleted below. Sections 2.2.1–2.2.3 summarize the IT infrastructures for each of the three industry groups studied.

- **System Architecture**—System Architecture defines the manner in which the application is designed. This includes the programming language used, the computing architecture such as client/server or mainframe-based, and the platforms that the application runs on.
- **Network Infrastructure**—The manner in which the systems are connected to communicate with one another is defined as the network architecture. Telecommunication links vary depending on the size and IT architecture of the organization. The network architecture will be described in terms of the Local Area Network (LAN) and Wide Area Network (WAN) technologies used.
- **Organization Information Technology Management Structure**—One of the key non-technical aspects of any IT environment is how that environment's day-to-day operations and maintenance are managed; and how change is brought about in the IT environment.
- **Security Safeguards (Policy & Practices)**—IT security safeguards are used to ensure the integrity and availability of IT resources and data. The following bullets describe existing IT safeguards deployed in the healthcare industry.
  - **Security Policy and Practices**—Healthcare security policies define the requirements for both physical and IT security. A security policy is a formal document. A security practice statement defines how these safeguards will be implemented within the organization.

- **Disaster Recovery Plan**—An IT disaster recovery plan defines the IT safeguards that will be employed to protect the availability of information resources within the organization. The plan is a formal document.
- **IT System Auditing**—Healthcare IT systems are audited to verify two things 1) proper day-to-day operations and maintenance of IT resources, and 2) the data stored and serviced by IT resources.
- **Existing PKI**—Each of the stakeholders was asked about their current use of PKI technology—for either encryption or digital signature—within their organization.

### 2.2.1 Practitioner IT Environment

Healthcare providers use IT to improve services to patients and customers. They are using the Internet to gather clinical and personal information. The Internet also gives healthcare providers the ability to advertise their unique skills on-line; helping to attract customers requiring specific skills. Many off-the-shelf applications provide practitioners with the ability to track patient information, automate billing, facilitate scheduling, and more. See Appendix B for a listing of these applications.

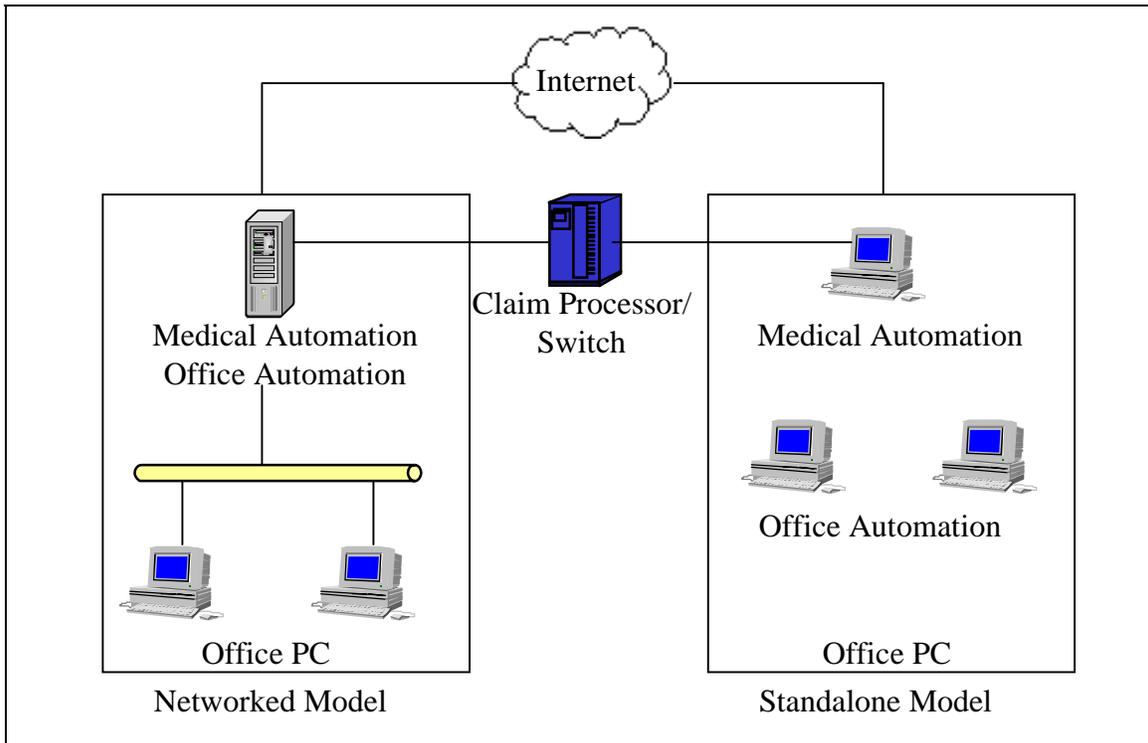
Practitioner IT environments vary based on the following three factors.

- **Degree of dependency on IT systems**—Practitioner use of IT fall into the following categories:
  - **Office Automation**—The use of computers for scheduling patient appointments and for financial purposes.
  - **Electronic Medical Records**—Electronic Medical Records (EMR) technology allows a practitioner to record medical data that was either entered electronically or transcribed from a written record. Additional uses of EMR include the transmission of medical records including laboratory results, professional communications, and communications with the patient.
- **Size**— The size and number of users a practitioner IT system needs to support contributes to the design of the IT system.
- **Location**—The number of office locations also effects the type of IT environment.

#### 2.2.1.1 Practitioner System Architecture

Practitioner systems are typically independent of other healthcare systems. Practitioner systems are typically made up of Intel processor based hardware running the Windows

operating system. Exhibit 2–2 shows typical practitioner system architectures.



**Exhibit 2–2. Typical Practitioner Systems Architecture**

As a result of the interviews, PEC identified two system architecture models in prescribing clinician organizations.

- 1) **Networked model**—The networked model has multiple workstations that connect to a central server.
- 2) **Standalone model**—The standalone model consists of one or more single systems running independent applications.

Both models use the following system applications.

- **Medical Automation Systems**—While some practitioners still rely on the paper-based approach to storing and retrieving patient information, many medical practices in the United States use computers to run Practice Management Software for billing and scheduling. They may also use EMR, lab/test results, and claims processing. EMR technology is found in larger practitioner settings. Small practitioner settings are slowly beginning to adopt EMR technology. Only 4% of the 88,000 members of American Academy of Family Physicians are currently using EMR. Two examples of such software are:

- DenTec provides health care assistants the ability to chart patient information, automate accounting procedures and provides scheduling capabilities.
- Medical Manager is a desktop application which addresses: financial, administrative, clinical, and practice management needs of the healthcare professional.
- **Office Automation**–Office automation includes applications that support day to day clerical, office tasks, financial, and billing.
- **Internet Services**–Internet services includes web access and Internet e-mail. The method of connecting to this service is described in section 2.2.1.2.

Exhibit 2–3 summarizes typical practitioner system architecture specifications.

Category	Server	Client
<b>Operating System</b>	UNIX, AIX, Windows NT/98/95, Novell Netware, Aix, HP-UX, Open VMS,	Windows 95/98/NT, DOS, Macintosh
<b>Hardware</b>	DEC Alpha, Intel Pentium, HP 9000, DEC VAX,	PC, dumb terminals, Macintosh, IBM RS/6000
<b>System Software</b>	EMR Vendors (ie. Soapware.com, Logician, Practicepartner Epicsystems)	

\*The server column is only applicable for the network model

### Exhibit 2–3. Practitioner Hardware/Platform Matrix

#### 2.2.1.2 Practitioner Network Architecture

Network architectures vary with the size of the practice. A survey of EMR systems shows that these products are designed to work in networked environments and can support a significant number of users. These products are network independent and usually run over TCP/IP. The following bullets describe influences on practitioners’ network architecture.

- **Connectivity to the Internet**– A few of the practitioners that were surveyed did have access to the Internet. The methods for connecting to the Internet include dial-up and dedicated connections. There was not an overwhelming bias towards one method of connecting to the Internet.
- **Healthcare Electronic Commerce Services**– Commercial companies such as Medical Manager Health Systems and CareInsite provide healthcare network services. This network is used for the confidential exchange of clinical, administrative and financial data between physicians and their affiliated insurance payers, patients, providers and suppliers. The network enables the medical community to electronically submit claims to payers (i.e. Medicare, Medicaid, Blue Cross/Blue Shield, and commercial carriers) using EDI.

- **Computer Automation**—EMR vendors have indicated that less than 5% of practitioners use EMR. Practitioners who use EMR are “early adopters” of this technology. These early adopters do not have a common network architecture. EMR vendors and other medical automation vendors design their products to work in different network architectures.

### 2.2.1.3 Practitioner IT Management

None of the practitioners surveyed maintained an in-house IT support staff. Since their systems tend to be off-the-shelf products, technical support is generally purchased from the respective software vendor. The vendor typically provides installation, training, maintenance, and telephone technical support services. Warranty support for system failures is also included.

### 2.2.1.4 Practitioner IT Safeguards

Through the interviews, PEC identified the following IT security safeguards in practitioner organizations as shown in Exhibit 2–4.

Security Aspect	Safeguards in Place
Physical Security	<ul style="list-style-type: none"><li>• Gated/locked with limited access to areas—Practitioner resources are placed in areas that are either locked or limited to authorized staff.</li><li>• Security Guard—Security guards are found in large practitioner environments such as clinics.</li><li>• Alarms and Surveillance sensors— Alarms are used to secure practitioner facilities during none operating hours. Keypads and Smart/swipe cards are used to activate and deactivate alarms or to gain entry into to the facility.</li><li>• Badges— Badges are used to identify the practitioner and his/her staff to the public and to one another.</li></ul>

**Exhibit 2–4. Practitioner IT Safeguards**

Security Aspect	Safeguards in Place
<b>Logical Security Controls</b>	<ul style="list-style-type: none"><li>• Log out before leaving computer</li><li>• Don't share passwords</li><li>• Individual username/password</li><li>• Password selection criteria– Some password selection criteria are: minimum password length, must contain a upper and lower case letter, must contain one digit and non-alphanumeric, and must not be a dictionary word.</li><li>• Application level, role based access security with access control lists</li><li>• Initials and passwords– Some practitioner systems are configured to accept initials to verify actions.</li></ul>
<b>Information Technology System Auditing</b>	<ul style="list-style-type: none"><li>• Audits are done to verify data and the accessing of that data. Federal laws and state medical boards generally require these types of audits. The practitioners commonly conduct spot audits in the duty of providing quality care to patients.</li><li>• Practitioners typically conduct internal audits of their systems to ensure adherence to organizational policies and practices. Larger practitioner settings contract with external auditors to conduct third party audits. The frequency of the audit for mission critical and data sensitive systems varies with the type of audit and depth of the audit.</li></ul>

#### **Exhibit 2–4. Practitioner IT Safeguards (Concluded)**

##### **2.2.1.5 Practitioner Use of PKI**

None of the practitioners that PEC interviewed currently use PKI technology to either encrypt or digitally sign information. The AMA is working to establish their own Certification Authority for issuing digital certificates to doctors. This activity may increase the use of PKI within this stakeholder group.

## 2.2.2 Pharmacy IT Environment

Most pharmacies have incorporated information technology as part of the normal workflow of counseling and dispensing medication to patients. Pharmacies use IT to automate tasks such as labeling, packaging, Drug Utilization Reviews (DUR), formulary checking, EMR, and billing and claims processing.

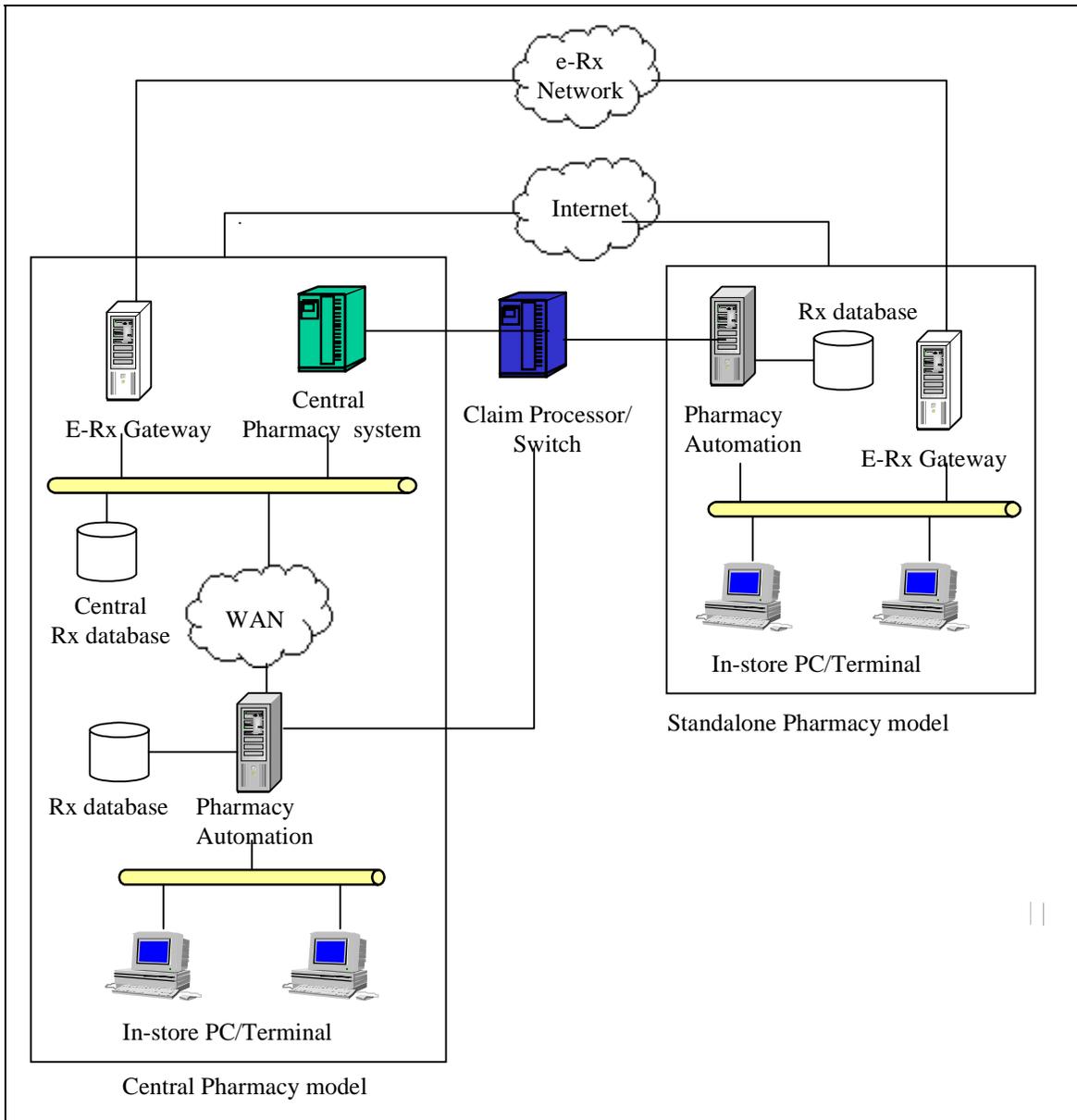
There are a wide range of pharmacy IT environments. The type of pharmacy system generally depends on a number of factors; 1) the size of the pharmacy, 2) whether the pharmacy is independent or part of a chain, and 3) the extent to which the ownership embraces new technology.

### 2.2.2.1 Pharmacy System Architecture

Pharmacy IT systems across the industry are used for Electronic Medical Records (EMR), product inventory/ordering, financial, and messaging applications. Pharmacy system architectures provide the following services:

- **Pharmacy Automation Systems**—Pharmacy automation applications include DUR, formulary checking, EMR, billing, claims processing, and inventory controls. Pharmacy organizations with a large number of pharmacy locations tend to develop proprietary pharmacy automation systems.
- **Electronic prescriptions**—Pharmacies that accept electronic prescriptions maintain a gateway system that interconnects their centralized headquarters computer system with one or more electronic prescription switching vendors' network. Prescriptions that are received over this network are formatted and converted if necessary into a format that the pharmacy system can interpret—not all pharmacies support the SCRIPT standard. The use of SCRIPT varied among the pharmacies that were interviewed.
- **Internet Services**—Connectivity to Internet services varied among the pharmacies interviewed. Pharmacy organizations with multiple pharmacy locations may have a corporate Intranet. Pharmacies often use computers that are separate from the pharmacy automation systems for web browsing and email.

Exhibit 2–5 shows typical Pharmacy system architectures.



**Exhibit 2–5. Typical Pharmacy System Architecture**

- **Standalone pharmacy model**—Independent pharmacies tend to have standalone systems with modem connections to a switch and the Internet. This model is typical of small independent pharmacies.
- **Central pharmacy model**—This model is not as rigid as the standalone model. The locality of applications varies among pharmacy organizations—some are run locally while others are performed at a central site. Central systems are commonly used for data backup, financial records, and inventory ordering and

tracking. The central pharmacy model may differ in regards to the way 1) prescription adjudication is handled, and 2) prescription data is handled.

- **Prescription Adjudication**
  - *Scenario I:* Prescription adjudication is conducted for the local system by the central system. The central system typically has a high bandwidth connection to a switch.
  - *Scenario II:* Prescription adjudication is conducted directly by the local pharmacy system. This is typically a dial-up on demand connection to a switch.
  
- **Prescription Data**
  - *Scenario I:* Prescription data is stored centrally after being entered at the local pharmacy system. The prescription data is then available to be retrieved by any local pharmacy system.
  - *Scenario II:* Prescription data is entered and stored locally. In some cases the prescription data is transmitted to the central system on a scheduled basis. Systems with central prescription adjudication typically follow this scenario.

Most commercial pharmacy software can operate in both pharmacy system architectures. Pharmacy systems typically run on Intel processor based hardware platforms. Industry interviews showed that the server Operating System is typically SCO UNIX. The clients are typically terminals or PCs running Microsoft Windows operating system. Exhibit 2–6 summarizes typical pharmacy system hardware and software specifications.

Category	Server	Client
Operating System	SCO-UNIX, Windows NT, Novell NetWare,	Window 95/98/NT workstation,
Hardware Platform supported	PC compatible	Dumb terminals, PCs
Application Software*	Proxymed, NDC software system, PDX, MedImpact (PBM), Citrix	

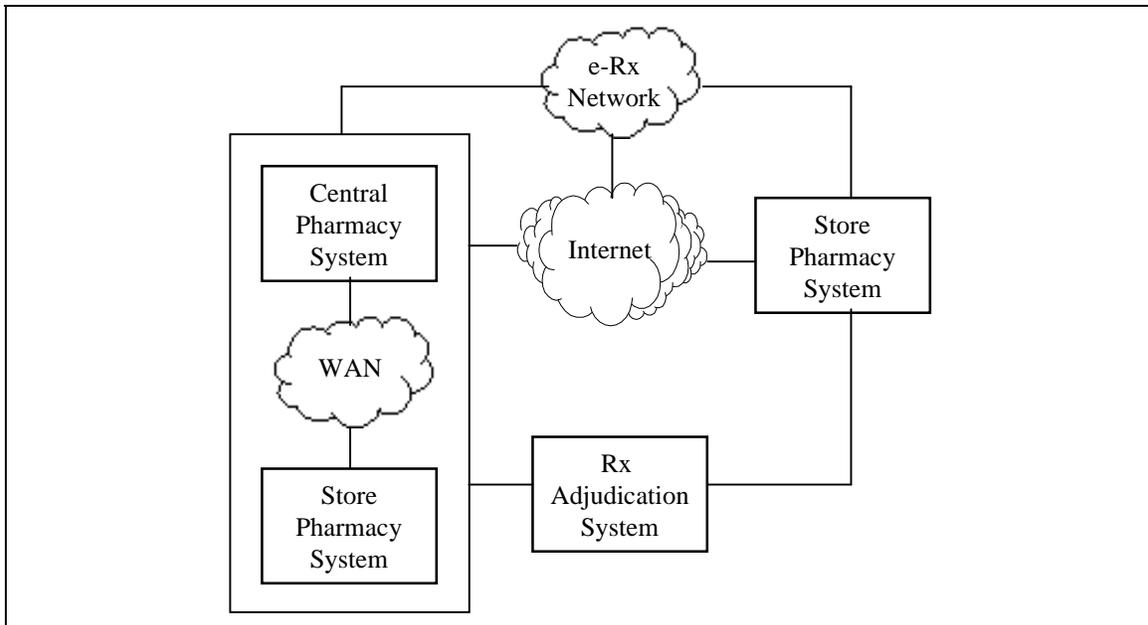
**Exhibit 2–6. Pharmacy Hardware/Platform Matrix**

### 2.2.2.2 Pharmacy Network Architecture

Pharmacy systems were found to have the following network connections.

- **Corporate WAN**—Chain pharmacies or those with multiple pharmacy locations typically use a WAN for data communications between individual pharmacies and centralized computing facilities. Leased lines are generally used for this purpose.
- **Switch/PBM Services**—Pharmacies typically maintain a connection to a switch for claims adjudication. The switch then forwards the transaction to the proper PBM for processing (See Section 2.5). Depending on the volume of prescriptions at the location, the link can either be dedicated or dial-up on demand.
- **Internet**— A few pharmacies maintain a connection to the Internet.

Exhibit 2–7 shows the typical network links employed by pharmacies.



**Exhibit 2–7. Pharmacy Network Connections**

Exhibit 2–8 provides a summary of current pharmacy network connectivity.

Category	Connectivity to HQ (Chains only)	Connectivity to Switch	Internet Connectivity
Small	Dial-up on demand	Dial-up on demand	Yes, from standalone PC with a dial-up
Medium	Dial-up on demand	Dial-up on demand	Yes, from standalone PC with a dial-up
Large	Dedicated high speed WAN	Dedicated frame relay	Yes, via cooperate WAN

#### Exhibit 2–8. Summary of Pharmacy Network Architectures

LAN technology supports a single server and typically two to three clients. Pharmacy systems with LAN technology typically use 10 Mbps Ethernet.

#### 2.2.2.3 Pharmacy IT Management

Pharmacy chains provide support, training, and administration to their pharmacists and support staff. Help desk personnel answer typical day-to-day operational issues during business hours of the pharmacy. High-level problems are supported 24 hours a day and 7 days a week (24x7). COTS software vendors typically provide 24x7 technical support for their software products. The manufacturers and/or distributors of hardware products typically provide support for hardware breakage and failure. Pharmacy chains that support multiple pharmacy locations have full time technical support staff.

#### 2.2.2.4 Pharmacy IT Safeguards

Physical security typically is not in place for the sole purpose of protecting IT resources. Security is in place to ensure the well being of the occupants and the pharmaceutical equipment inside. The following physical security safeguards can be found in pharmacy organizations. Exhibit 2–9 identifies the IT safeguards that pharmacies employ.

Security Aspect	Safeguards in Place
<b>Physical Security</b>	<ul style="list-style-type: none"> <li>• Gated/locked with limited access to areas– Pharmacy resources are placed in areas that are either locked or limited to authorized staff.</li> <li>• Security Guard– Security guards are found in large pharmacy environments and are dependent on the location of the pharmacy.</li> <li>• Alarms and Surveillance sensors– Alarms are used to secure pharmacy facilities during non-operating hours. Keypads and Smart/swipe cards are used to activate and deactivate alarms or for gaining entry into the facility.</li> <li>• Badges</li> <li>• Closed community– Pharmacy staff tend to be under 10 people therefore unauthorized physical access to pharmacy IT resource is minimized.</li> </ul>

#### Exhibit 2–9. Pharmacy IT Safeguards

Security Aspect	Safeguards in Place
<p><b>Logical Security Controls</b></p>	<ul style="list-style-type: none"> <li>• Log out before leaving computer</li> <li>• Don't share passwords</li> <li>• Individual username/password</li> <li>• Password uniqueness requirements</li> <li>• Application level, role based access security with access control lists</li> <li>• Transactions require Initials /passwords</li> <li>• Firewalls</li> <li>• Access logging/System Auditing</li> <li>• Inactivity timer</li> <li>• Shared/Role-based user account w/password</li> <li>• Central broadcast of password adjunct code PINs</li> <li>• Mandatory computer keycard placement</li> <li>• Mandatory password formats and changes</li> <li>• Restricted use of floppies—pharmacy systems typically are not equipped with floppies.</li> </ul>
<p><b>Disaster Recovery Plan</b></p>	<ul style="list-style-type: none"> <li>• On and off site tape backups and tape rotations</li> <li>• Perform backup verification</li> <li>• Redundant data center for central resources</li> <li>• Data stored at central resource</li> <li>• Auxiliary power sources for critical IT resources</li> <li>• Redundant data links to central IT resources</li> <li>• 24 hours 7 days a week disaster response personnel</li> <li>• Procedures for continued operation during disaster</li> </ul>
<p><b>Information Technology System Auditing</b></p>	<ul style="list-style-type: none"> <li>• Typically audits are done to verify data and the accessing of that data. Pharmacies commonly conduct spot audits in the duty of providing quality care to patients. A majority of the audits are to verify inventory and sales records. Since a bulk of the inventory and sales records are kept electronically. The IT systems that contain the electronic data is checked and verified as a result of the inventory and sales audit.</li> <li>• Pharmacies typically perform internal audits of their systems to ensure adherence to organizational policies and practices. Larger pharmacy organizations contract with external auditors to conduct third party audits. The frequency of the audit for mission critical and data sensitive systems varies with the type of audit and depth of the audit.</li> </ul>

**Exhibit 2–9. Pharmacy IT Safeguards (concluded)**

### 2.2.2.5 Pharmacy Use of PKI

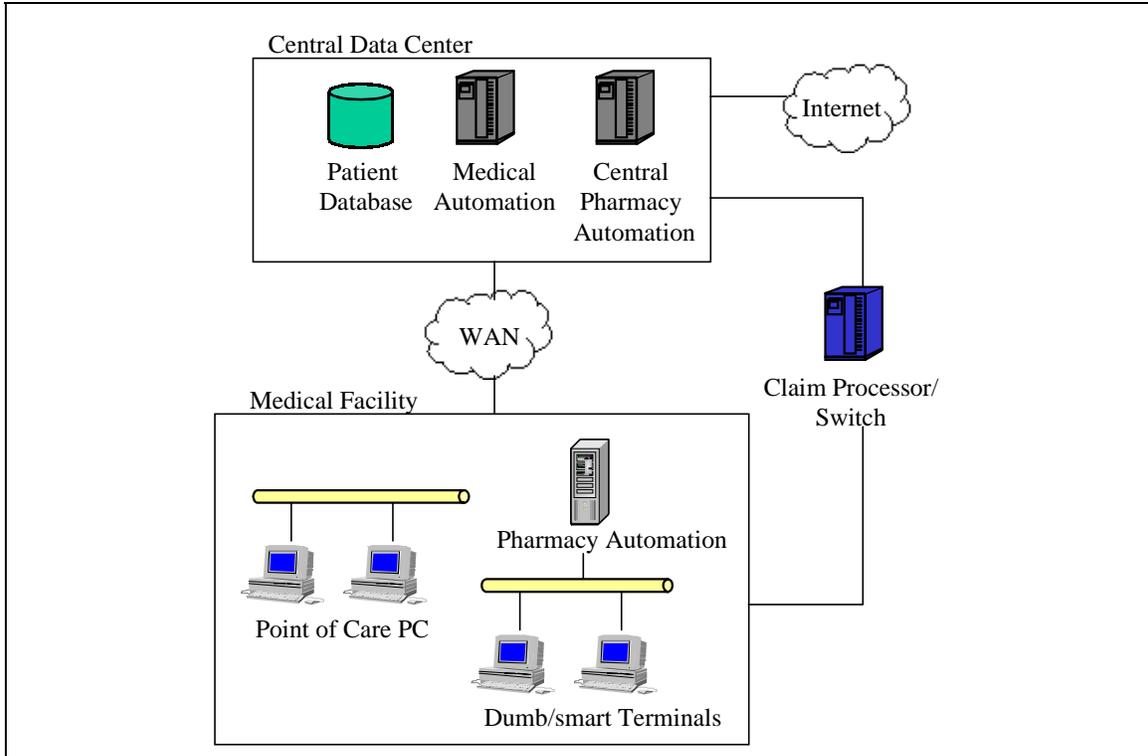
None of the pharmacies that PEC interviewed currently use PKI technology to either encrypt or digitally sign information in a production environment. There have been several pilots to test the effectiveness of secure remote log-in and digital signatures.

### 2.2.3 Hospital IT Environment

A hospital system delivers complete healthcare to a patient. Examples of such systems are the VHA, DOD Consolidated Health Care System (CHCS), Kaiser healthcare, and hospital organizations.

Hospitals are undergoing major changes from a centralized minicomputer and mainframe system toward distributed, client/server systems. One example Brigham Women's Hospital is migrating to a LAN-based, distributed, client/server, and desktop environment. This structure allows physicians from remote offices access to information stored on the main hospital campus.

The client/server architecture provides physicians the ability to utilize applications such as Patient Accounting, Results Retrieval and Physician Order Entry. Brigham Hospital utilizes the Massachusetts General Hospital Utility Multi-Programming System (MUMPS) as its coding language to build its various applications.



**Exhibit 2–10. Typical Hospital System Architecture**

Two types of hospital organizations exist, 1) multiple geographical locations, and 2) single geographical location. A hospital organization with multiple geographical locations typically has an IT environment as depicted in exhibit 2–10. A hospital organization with a single geographical location will house the data center at the single location with the pharmacy automation system consolidated into a single system.

### 2.2.3.1 Hospital System Architecture

System architectures for most hospital organizations are highly diverse and have many different architectures in place, depending on the geography, system, application, available technology, and budget. In a large organization there simply is no one “architecture.” The degree of interoperability and data sharing among healthcare systems varies among hospital organizations. This trend is beginning to change with the increasing reliance on data systems. The following items describe the typical system architecture as depicted in exhibit 2–10.

- **Pharmacy Automation Systems**—Pharmacy automation applications include DUR, formulary checking, EMR, billing, claims processing, and inventory controls. Pharmacy systems operating in a hospital are similar to those operated in retail pharmacies. The pharmacy system is typically self contained at the medical facility. Data is copied to a central pharmacy system to be shared among other medical facilities and applications.
- **Medical Automation Systems**—Hospital medical automation systems include applications such as EMR, lab results, patient scheduling, and claims processing.
- **Office Automation**— Office automation includes applications that support day to day clerical, office tasks, financial, and billing.
- **Web Services**—Internet services include Internet access, Intranet, and Internet e-mail. Web services are also offered to patients for order placement and payment.
- **Prescription adjudication**—Prescription adjudication and claims processing are handled differently. If the hospital is the insurer, the prescription adjudication process occurs internally. In some circumstances a switch is used to process the prescription adjudication back to the hospital/insurer organization when the pharmacy is outsourced. Alternatively, if the hospital is not the insurer prescription adjudication must take place with the aid of a switch.

Exhibit 2–11 summarizes typical hospital system hardware and software specifications.

Category	Server	Client
Operating System	SCO-UNIX, UNIX, Windows NT, Novell NetWare,	Windows
Hardware	Mainframe, PC Compatible, UNIX hardware	PC workstations, mainframe terminals, laptops, palm tops, personal internet access, devices, wireless devices
Software	NDC	

**Exhibit 2–11. Hospital Hardware/Platform Matrix**

### 2.2.3.2 Hospital Network Architecture

Hospital network architectures are typically using large LANs to interconnect computing resources in IDN/Hospital facilities. WANs are used to interconnect sites with centralized computing facilities.

### 2.2.3.3 Hospital Organization Management

Hospital organizations provide support, training and administration for their facilities. Help desk personnel answer typical day to day operational issues during operational hours of the pharmacy. High level problems are supported 24 hours a day and 7 days a week. COTS software vendors typically provide technical support 24 hours a day and 7 days a week for their software products. The manufacture or distributors of hardware products typically provide support for hardware breakage and failure.

### 2.2.3.4 Hospital IT Safeguards

Exhibit 2–12 lists the hospital IT safeguards that were identified in the interviews.

Security Aspect	Safeguards in Place
Physical Security	<ul style="list-style-type: none"> <li>• Gated/locked with limited access to areas– IDN/hospital resources are placed in areas that are either locked or limited to authorized staff. IDNs/hospitals typically house servers in dedicated computer rooms.</li> <li>• Security Guards</li> <li>• Alarms and Surveillance sensors– Alarms are used to secure practitioner facilities during none operating hours. Keypads and Smart/swipe cards are used to activate and deactivate alarms or for gaining entry into the facility.</li> <li>• Badges</li> </ul>

**Exhibit 2–12. Hospital Safeguards**

Security Aspect	Safeguards in Place
<b>Logical Security Controls</b>	<ul style="list-style-type: none"> <li>• Log out before leaving computer</li> <li>• Don't share passwords</li> <li>• Individual username/password</li> <li>• Shared/Role-based user account w/password</li> <li>• Password selection criteria– Some password selection criteria are; minimum password length, must contain an upper and lower case letter, must contain one digit and non-alphanumeric, and must not be a dictionary word.</li> <li>• Central broadcast of password adjunct code PINs</li> <li>• Mandatory password format and change</li> <li>• Initials and passwords—Some practitioner systems are configured to accept initials to verify actions.</li> <li>• Application level role based access security with access control lists</li> <li>• Multilevel security access/function menus</li> <li>• Mandatory password or second password entry for certain functions</li> <li>• Central broadcast password adjunct</li> <li>• Automatic linkage with personnel systems</li> <li>• Inactivity timer</li> <li>• 24 * 7 Security monitoring Access logging and System Auditing</li> <li>• Restricted dual access</li> <li>• Firewalls</li> </ul>
<b>Disaster recovery Plan</b>	<ul style="list-style-type: none"> <li>• On and off site tape backups tape rotations</li> <li>• Perform backup verification</li> <li>• Redundant data center for central resources</li> <li>• Data stored at central resource</li> <li>• Auxiliary power sources for critical IT resources</li> <li>• Redundant data links to central IT resources</li> <li>• 24 hours 7 days a week disaster response personnel</li> <li>• Procedures for continued operation during disaster</li> </ul>
<b>Information Technology System Auditing</b>	<ul style="list-style-type: none"> <li>• Typically audits are done to verify data and the accessing of that data. IDNs/hospitals commonly conduct spot audits in the duty of providing quality care to patients. A majority of the audits are to verify inventory and sales records. Since a bulk of the inventory and sales records are kept electronically.</li> <li>• IDNs/hospitals typically perform internal audits of their systems to ensure adherence to organizational policies and practices. IDNs/hospitals use external auditors as a requirement by state and federal laws. The frequency of the audit for mission critical and data sensitive systems varies with the type of audit and depth of the audit.</li> </ul>

**Exhibit 2–12. Hospital Safeguards (Concluded)**

### **2.2.3.5 Hospital Use of PKI**

A lack of standards, high costs, and implementation difficulties have caused US hospital systems to shy away from PKI. Hospitals are required to share patient medical records with other institutions and patient confidentiality is a major concern. Health care conglomerates such as Kaiser Permanente, Catholic Healthcare West and PacifiCare Health Systems Inc. are looking for ways to adopt PKI. Catholic Healthcare West has standardized on a Worldtalk product to provide its businesses with secure electronic e-mail.

## **2.3 Electronic Prescription Design**

The following section provides a look at existing electronic prescription design concepts that are being developed. The electronic prescription market is too immature at this point to determine which electronic prescription model will dominate the market. Currently many systems send prescriptions to the pharmacy via facsimile.

### **2.3.1 Internet Healthcare Portal**

With this model, both the practitioner and pharmacy connect to a central healthcare web site via the Internet using a standard web browser. This model leverages the Internet as a transport medium for many types of healthcare transactions. Portals are becoming popular because they offer a very low cost of entry for their users—a simple web browser and a connection to the Internet is all that is needed. Security is provided via Secure Sockets Layer (SSL) protocol, which provides an encrypted tunnel between the Portal server and the client workstation.

The process works in three steps; the practitioner connects to the web site, authenticates to the system, and creates the prescription. Prescriptions can reach the pharmacy either electronically using the NCPD SCRIPT EDI standard or via fax. Healthcare portals offer a number of services beyond electronic prescriptions including:

- Electronic prescriptions, Drug Utilization Review (DUR)
- Research data
- Practice management tools
- Lab Tests And Results

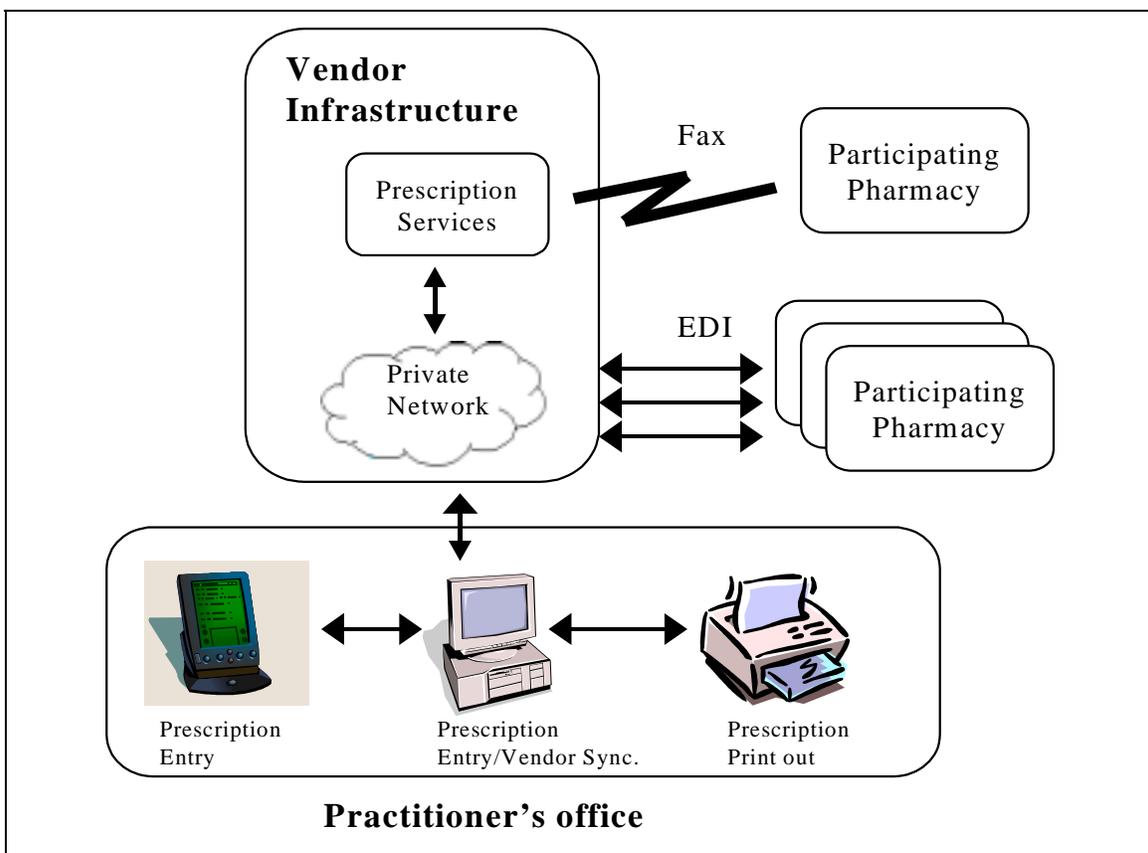
### **2.3.2 Closed System**

Hospitals and other self contained healthcare organizations use a single system—composed of many individual applications. All aspects of a closed system are controlled and owned by a single entity. The pharmacy and the practitioner are employees of the same healthcare organization. This model supports two applications; 1) order entry, and 2) prescriptions. The process for these two applications are very similar. The practitioner creates the outpatient medication order (prescription) that is then sent to the centralized

computer platform. The order is held on the system, awaiting processing by a pharmacist who will complete the prescription transaction.

### 2.3.3 Switched Service Network

This model consists of a set of healthcare services provided by a single vendor. Vendors market their services to practitioners and establish connectivity relationships with pharmacies. Private communication lines are used as the medium between the vendor and the participating pharmacies. Practitioners typically conduct transactions locally—these transactions are then forwarded to the vendor's prescription server system via a dialup connection. The practitioner can enter the prescription in two ways; 1) the prescription can be input on a standard computer using vendor supplied software, or 2) the practitioner can employ a portable handheld computer—again using vendor supplied software—that synchronizes with the desktop system either via a direct connect or with wireless technology. A third alternative allows the practitioner to print the prescription out if it happens to be for a controlled substance, or if the patient so desires. Once the electronically transmitted prescription reaches the vendor's system, it is forwarded to the destination pharmacy either via fax or by using the SCRIPT EDI protocol over a private network.



**Exhibit 2–13. Switched Service Network Model for Electronic Prescriptions.**

## Section 3—Analysis and Derived Requirements

Through the interview and industry research process, IT infrastructures currently employed by stakeholders were captured to form typical models used by industry. Adoption of electronic prescription transmission would have an impact on two stakeholders, Practitioners and Pharmacies. The established business processes of both practitioners and the pharmacists need to be accounted for when analyzing and deriving requirements based upon their existing IT infrastructure.

While some stakeholders have shown great interest in this technology, other stakeholders have shown a “wait and see” attitude. Some stakeholders—small practitioner offices and independent pharmacies—may have interest in an electronic option, but are not in a situation where a change from the paper system is vital to business growth. The business and IT requirements are derived directly from PEC’s industry research and from stakeholders contacted about this program. These business and IT requirements, along with the information security requirements presented in the Certificate Policy Requirements Analysis provide the framework for the selection of appropriate technologies. Integration of this technology into current workflow is critical. The requirements derived from the stakeholders’ IT environment—discussed in Section 2—are addressed in this section.

### 3.1 DEA High Level Design Requirements/Constraints

- PKI-enabled, electronically transmitted prescriptions must meet or exceed the current level of security for the existing paper-based system.
- PKI-enabled, electronically transmitted prescriptions will be an alternative to the existing manual process—participants will not be required to employ electronic prescriptions.
- PKI-enabled electronically transmitted prescriptions will need to provide the DEA with the ability to take action against improper use of this technology.
- The DEA will need to inform Industry CAs of any changes in a registrant’s status.
- The CA will be required to inform the DEA of any non-registrants who are issued certificates (pharmacists and agent practitioners).
- The continued evolution of security technology and computing platforms must be considered to ensure that regulations are written in a manner that specifies the desired end-result rather than focusing on a specific implementation.

### 3.2 Controlled Substances Business Process Requirements

Information technology plays a vital role towards ensuring the success of industry organizations. It is often the sole factor in their ability to distinguish themselves in the marketplace and gain a competitive advantage. Industry stakeholders have substantial investments in their business processes and the technology infrastructures that support those processes. This is especially evident in hospitals and institutions that may have centralized computer record systems, and pharmacies and pharmacists that regularly fill high volumes of prescriptions.

The IT business process requirements for electronically transmitted prescriptions for controlled substances are listed below.

**REQUIREMENT: Ability to generate prescriptions quickly, easily, efficiently and accurately.**

Acceptance of an electronic prescription system is based on a number of factors. One factor is the ability of electronic prescription technology to improve workflow by providing prescription transactions that can be processed quickly, easily, efficiently, and accurately.

Pharmacists and practitioners interviewed have each expressed that they experience severe time limitations/constraints in their daily routines. For practitioners, current workflow in the typical office setting has one practitioner scheduled to see multiple patients within a concurrent time slot. Most of the practitioner's time is spent seeing to patients — administrative duties are delegated to assistants and office staff. For pharmacies, the numbers of prescription transactions vary, with some of the larger pharmacies filling an average of 1000 prescriptions a day. Transaction volumes are very high and will continue to increase due to market factors such as the aging population and new products being brought to market.

The ability to handle large and increasing transaction volumes is critical to providing improved service levels to customers. Electronically transmitted prescriptions will have to take current stakeholder business processes into account so that fast and efficient prescription filling can be achieved.

**REQUIREMENT: Must not place additional burdens of time or technical difficulty on users of the system.**

Stakeholders have specialized, technical training—however not usually in computer science technologies. The stakeholders have stated that their daily workload does not provide an abundance of time during the day to learn new material outside of their specialty. The introduction of electronically transmitted prescriptions should provide workflow enhancements, and require little or no training. Understanding and using PKI-enabled electronic prescriptions should not be technically burdensome—computer novices should be able to use it with minimum technical support from vendors.

Pharmacists expressed that they found the ability to perform automatic certificate checking very appealing and that this feature would enhance workflow without decreasing workflow efficiency.

**REQUIREMENT: Flexibility to leverage existing processes and in-place systems to the fullest extent.**

Pharmacies currently use very sophisticated prescription management software to direct the process of prescription tracking, prescription filling, and patient information. Therefore, any new system must be able to interact with the features and business logic of their current prescription management systems. The ability to leverage current prescription processes and business logic is a key factor to acceptance of any new system.

Typical pharmacies utilize public and private networks, or dial up access to resolve insurance adjudication/acceptance. This is accomplished through 1) a connection to a switch that facilitates the processing of insurance information/adjudication or 2) a connection to the pharmacy chain headquarters who then passes information to the switch. Current electronic prescription providers may act as a switch for these pharmacies using expensive IT infrastructures. This is usually achieved by the integration of this technology into current pharmacy software. Current processes, software and hardware, and network connectivity must be leveraged to the fullest extent.

**REQUIREMENT: Must be able to verify the status of program participants.**

Pharmacists have a corresponding liability, equal to the liability of a prescribing practitioner, to ensure that the proper substance, at the right dosage, reaches the intended patient for a legitimate medical purpose. The stakeholders that were interviewed expressed confidence that PKI-enabled, electronically transmitted prescriptions will provide the necessary security to ensure the integrity of transactions between practitioners and pharmacists. However, there was concern from some pharmacists that it would be difficult to determine the validity of a prescription especially for participants that do not have a high degree of knowledge in computers. If an open architecture is adopted for this technology, tools would be needed to ensure identities of the prescription originators.

**REQUIREMENT: Technology must not exclude any potential participants and must be equally viable to all participants large and small.**

Introduction of the electronic prescription transmission technology will require an outlay of resources to include hardware, software, and computer communications access. Viable solutions may range from very complex architectures that can be integrated into existing prescription management software to more simple configurations that would be stand-alone and involve a web browser. Electronic prescriptions for controlled substances must employ security levels that meet or exceed current levels for paper prescriptions. However, adoption of this technology will be curtailed with the demands of complex and costly implementation requirements.

Interviewees expressed concern over the potential costs of electronic prescription systems. Individual and small practice practitioners typically have a limited amount of resources allocated to IT due to the limited return on investment (ROI) from the technology. Currently, a majority of private-practice practitioners maintain hand-written schedules and patient records. Typically, small pharmacies have limited resources to spend on IT outlays and may find the use of electronic prescriptions cost-prohibitive.

### **3.3 IT Infrastructure Requirements**

#### **3.3.1 Network Architecture Requirements**

**REQUIREMENT: Ability to operate in a variety of network topologies and use multiple communication topologies and protocols.**

The existing network architectures currently used by the stakeholder groups within their organizations are varied and highly customized. There is no typical or standard configuration that is employed by the stakeholders due to diverse business size, geographic location, cost allocation, and demand. All forms of network architectures, protocols and transmission methods are used. Individual practitioner offices might utilize stand-alone or LAN configurations that commonly use MS Windows platforms. PKI-enabled, electronically transmitted prescription technology would need to be able to interoperate with these topologies and protocols.

Electronic communication between the stakeholder groups is generally accomplished through dial-up connections or direct lines to external entities for claims adjudication and insurance processing. Typically, pharmacies employ client/server architectures at individual stores with a variety of topologies and operating systems that connect to central facilities. Larger retail and chain pharmacies are employing web-based business solutions to sell products and to allow for the fill/refill of prescriptions. This is usually done through the pharmacy chains' central office with information forwarded to the individual store through the corporate data connection. Stakeholders usually have some type of connection to a switch for insurance/claim adjudication. To make electronic prescription transmission viable for all potential participants, all protocols and access methods should be considered including Internet access.

### 3.3.2 Systems Architecture Requirements

The following factors will influence the regulations:

**REQUIREMENT: Regulations should allow electronic prescription adopters to flexibly implement compliant systems. Implementations should be compatible with existing central server platforms, end user personal computers, workstations, terminals and laptops.**

The stakeholder groups use various network configurations and employ a number of different computing platforms to operate their businesses. Pharmacy IT services are typically provided by a central server—accessed via terminals located at the pharmacy. These platforms might employ either the use of COTS or proprietary software packages.

**REQUIREMENT: Ability to utilize existing business process management software as the application to be PKI enabled.**

The stakeholder groups (practitioners and pharmacies) currently use sophisticated software that is designed for their specific business needs. These software packages have been either developed internally as propriety software or purchased from a software vendor as COTS packages. These software packages usually serve as the central workflow application—multiple processes are run from the application. Electronic prescriptions in industry are typically being performed through the use of stand-alone applications. In a few cases, proprietary and COTS software packages currently have or are slated to integrate electronic prescription transmission capabilities.

**REQUIREMENT: Existing standards should be used to ensure interoperability.**

Existing technical standards should be adopted where appropriate in the area of EDI, PKI specifications, security policy, and network architectures. There are a number of small to medium-sized organizations that have entered the EDI arena, however practitioner and pharmacy IT systems are not tightly integrated. Therefore, support for recognized industry standards is the key to practitioners and pharmacies successfully collaborating and transmitting controlled substance prescriptions.

Electronic prescription providers seem to be moving towards supporting the NCPDP SCRIPT standard for the electronic transmission of prescriptions from a practitioner to a pharmacy. The SCRIPT standard adheres to the EDIFACT syntax requirements and utilizes standard EDIFACT and ASC X12 data tables. PKI services should support industry standards for public-key cryptography, FIPS 140-1 validation, X.509 certificate designations, and other relevant standards as much as possible. A standards-based environment will ensure interoperability between all program participants.

### **3.4 IT Organization, Administration and Technical Support Requirements**

Industry stakeholders universally depend on their IT assets to operate their businesses. This requires that the internal groups responsible for the IT operations be fully accountable for those operations. Typically large pharmacies, IDNs/hospitals and HMOs have very large and sophisticated IT organizations that are centrally managed. This type of organization creates a single point of contact for handling system malfunctions and failures. This is generally accomplished by a Help Desk that is available 24 hours a day 7 days a week that can either remotely diagnose and remedy the problem, or dispatch someone to the site. Smaller organizations—like small practitioner offices or independent pharmacies—typically have to maintain this knowledge in-house or employ contractors.

**REQUIREMENT: The DEA PKI Certification Authority (CA) will need to be centrally managed. Industry CAs will provide direct support to subscribers.**

To ensure that DEA has the ability to regulate and enforce the electronic prescription transmission process, the DEA will establish the root CA. This CA will in turn give authority to industry CAs that will provide digital certificates to subscribers. There is the potential that more than one million DEA registrants could use electronically transmitted prescriptions for controlled substances. Therefore, industry CAs will provide the needed support to users pertaining to enrollment, training, certificate management, and hardware and software problems.

### **3.5 Information Technology Security Requirements**

Both the DEA and industry stakeholder groups take information security very seriously. They exercise prudent care and take measures to insure that information assets and resources are secure and available when needed.

#### **3.5.1 Physical Security and Disaster Recovery Requirements**

**REQUIREMENT: The PKI-based electronic transmission of controlled substance prescriptions—and any associated applications using the PKI—must be available to subscribers and relying parties on a 24 hour by 7 days a week basis.**

DEA and industry stakeholder groups have made substantial investments in on-site physical security, backup measures and disaster recovery. As electronic prescription transmission becomes more popular, the set of measures taken to protect the DEA electronic prescription PKI must be as strong or stronger than those measures used to protect current information assets and resources. Security measures must ensure that an acceptable level of infrastructure availability be achieved to guarantee acceptable service to users.

### 3.5.2 Logical Information Technology Security Requirements

DEA and industry stakeholder groups currently use very sophisticated logical system methods to provide access control, confidentiality, and integrity of information assets and resources.

**REQUIREMENT: Ability to limit and restrict access based upon roles and functions down to the row level and log all actions taken on the system.**

DEA and industry stakeholder groups utilize numerous security safeguards in their businesses. These include access control lists, authorization servers, firewalls, and password-based access control to application functions and system information. They also audit/archive all actions taken on an order—down to the authorized user level. The electronic prescription PKI must be interoperable with these safeguards.

### 3.5.3 Information Technology Security Policy and Auditing Requirements

**REQUIREMENT: Provide registrants with written Security Policy for PKI CAs and scheduled system auditing procedures.**

Stakeholder groups largely expect some type of formal PKI policy from the DEA for the electronic prescription of controlled substances. Stakeholder groups indicated that they would incorporate that formal policy into their existing IT Security Policies. The policy will affect the parties that will act as industry Certification Authorities; as well the subscribers (practitioners and pharmacists) that will use this system. Auditing procedures must be developed that provide a mechanism for ensuring compliance with the written security policy.

## 3.6 Current Use of PKI and Encryption Technologies

**REQUIREMENT: The PKI will have the ability to support prescriptions for non-controlled substances.**

None of the practitioners that were surveyed exclusively prescribed controlled substances. Most practitioners surveyed said that these prescriptions accounted for ten percent of their total prescriptions. The DEA's electronic prescription framework should allow participating DEA registered practitioners to electronically prescribe non-controlled substances. Since the DEA registration-based certificate is structured to certify the holder's registration status to the other party for the prescription transaction, healthcare professionals not registered to handle controlled substances will not be authorized to obtain DEA sanctioned digital certificates for the purpose of certifying their identities to third parties.

## **Section 4—Background and High Level Requirements Table**

In addition to the requirements for the services provided in a PKI, there are requirements for business processes, both DEA and Industry, and system requirements. The requirements listed here represent a combination and compilation of high level existing network infrastructure elements gained through interviews, meetings and documentation of the stakeholders both in industry and DEA.

These high level requirements will provide the guidance necessary to produce the Concept of Operations for the electronic prescription PKI to leverage the existing business processes and systems to the maximum extent. It is recognized that it may not be possible to meet all requirements listed here in a single, universal design. As individual designs for the Concept of Operations are developed, the inclusion of these requirements will be measured against their ability to provide the maximum user acceptance. It should also be noted that these requirements need to be reviewed periodically to maintain their validity.

In conclusion, there is commonality among the stakeholders in the methods of operation surrounding the handling and documenting of controlled substances. There is a substantial variance though, in the types of networks, hardware, software and management of technology being used among the various stakeholders. Therefore the design standards brought forward in the Concept of Operations will need to cover and extend to a variety of different technology choices. This design “elasticity” will help to promote the maximum degree of stakeholder acceptance, and assure a faster implementation within the stakeholder community.

	<b>Business Process and System Requirements</b>
<b>REQUIREMENT</b>	Ability to generate prescriptions quickly, easily, efficiently and accurately.
<b>REQUIREMENT</b>	Must not place additional burdens of time or technical difficulty on users of the system.
<b>REQUIREMENT</b>	Flexibility to leverage existing processes and in-place systems to the fullest extent.
<b>REQUIREMENT</b>	Must be able to verify the status of program participants.
<b>REQUIREMENT</b>	Technology must not exclude any potential participants and must be equally viable to all participants large and small.
<b>REQUIREMENT</b>	Ability to operate in a variety of network topologies and use multiple communication topologies and protocols.
<b>REQUIREMENT</b>	Regulations should allow electronic prescription adopters to flexibly implement compliant systems. Implementations should be compatible with existing central server platforms, end user personal computers, workstations, terminals and laptops.
<b>REQUIREMENT</b>	Ability to utilize existing business process management software as the application to be PKI enabled.
<b>REQUIREMENT</b>	Existing standards should be used as appropriate.
<b>REQUIREMENT</b>	The DEA PKI Certification Authority (CA) will need to be centrally managed. Industry CAs will provide direct support to subscribers.
<b>REQUIREMENT</b>	The PKI-based electronic transmission of controlled substance prescriptions—and any associated applications using the PKI—must be available to subscribers and relying parties on a 24 hour by 7 days a week basis.
<b>REQUIREMENT</b>	Ability to limit and restrict access based upon roles and functions down to the row level and log all actions taken on the system.
<b>REQUIREMENT</b>	Provide registrants with written Security Policy for PKI CAs and scheduled system auditing procedures.
<b>REQUIREMENT</b>	The PKI will have the ability to support prescriptions for non-controlled substances.

**Exhibit 4-1. High Level Business and System Requirements Table**

## Appendix A –Requirements Interviews List

### A.1 DEA Representatives

DEA Representatives	Title	Location	Interview Date
Patricia Good	Chief Liaison and Policy Section	DEA HQ	12/6/99
Michael Mapes	Deputy Chief Liaison and Policy Section	DEA HQ	9/28/99
Jim Pacella	Chief Registration and Program Support Section	DEA HQ	10/12/99
Terry Woodworth	Deputy Director Office of Diversion Control	DEA HQ	12/6/99
Sharon K. Partlo	Chief Policy Unit	DEA HQ	12/6/99
Denise Curry	Chief Liaison Unit	DEA HQ	10/28/99
Janet Gardner	Staff Coordinator	DEA HQ	10/8/99
Vicky Seeger	Pharmacist, Policy Unit		11/19/99
Elizabeth Willis	Deputy Chief, Drug Operations Section	DEA HQ	10/14/99
Tom Crow	Diversion Program Mgr.	Chicago, IL	10/14/99
Jim Tillman	Diversion Program Mgr.	St. Louis, Mo	9/29/99
Scott Collier	Group Supervisor, Denver	DEA HQ	9/28/99
Larry W. Lockhart	Group Supervisor, Birmingham		
Gale Jones	Diversion Investigator		
Donna Dombourian	Diversion Investigator		
Barbara Health	Diversion Investigator		
Alan Clesi	Diversion Investigator		
Craig Riley	Diversion Investigator		

**A.2 Department of Veterans Affairs**

Department of Veterans Affairs	Location	Contact Person	Interview Date
Dr. Roy Altman	Florida	Dr. Roy Altman	11/10/99
Practitioner	Maryland	Practitioner	11/28/99
Dr. Van Horn	Maryland	Dr. Van Horn	11/26/99
Dr. Shillingford	Maryland	Dr. Shillingford	11/26/99
Dr. Marshall	Maryland	Dr Marshall	11/30/99
Frederick P. Soette	Maryland	Frederick P. Soette	11/29/99
Maarten Calon	Maryland	Maarten Calon	11/29/99

**A.3 Pharmacies**

Pharmacy Chains	Location	Contact Person	Interview Date
Walgreens	Deerfield,IL	Audrey Neely, Mike Jonas, and Neil Penco	11/4/99
Eckerd	Clearwater, FL	Laurie Toenjes	11/23/99
Rite Aid	Harrisburg, PA	Jim Krahulec	11/11/99
Publix Super Markets	Lakeland, FL	Ron Miller	10/18/99
Giant of Maryland	Landover, MD	Sheldon Pelovitz	11/8/99
Ukrops	Richmond based company with 18 pharmacies	John Beckner Dave Ylitalo	11/17/99
Wegmans Food Markets, Inc.,	Rochester, NY. Wegmans w/ 57 pharmacies	Mark Valesano	11/19 /99

**A.4 Practitioners**

Practitioners	Location	Contact Person	Date/Time
Dr. Melvin Sterling	CA	Dr. Melvin Sterling	12/20/99
Dr. Nancy Nielsen	NY	Dr. Nancy Nielsen	11/30/99
Dr. John Schneider	ILL	Dr. John Schneider	11/21/99

**A.5 Industry Associations**

Associations	Location	Contact Person	Date/Time
American Academy of Family Physicians (AAFP)	Washington D.C.	Susan Rehm	11/22 /99
Academy of Managed Care Pharmacy (AMCP)	Alexandria, VA	Richard Fry	11/9/99
American Society of Health System Pharmacists (ASHP)	Bethesda, Md.	Dr. Gary Stein	11/11/99
Food Marketing Institute (FMI)	Washington, DC	Ty Kelley	11/16/99
National Association of Boards of Pharmacy (NABP)	Park Ridge, ILL	Carmen Catizone	11/8 /99
National Association of Chain Drug Stores (NACDS)	Alexandria, VA	Mary Ann Wagner	10/27/99
American Academy of Physician Assistants (AAPA)	Alexandria, VA	Ann Davis	11/18/99
American Pharmaceutical Assoc. (APhA)		Susan Winkler	11/10/99
Pharmaceutical Care Management Assoc. (PCMA)		Lyle Piper	11/23/99
National Community Pharmacists Assoc. (NCPA)	Alexandria, Va	John Rector Doug Hoey	11/8/99
American Academy of Pain Medicine	Glenview, IL	Jeffrey Engle Executive Director	11/15/99
Federation of State Medical Boards	Ft. Worth Texas	Dr. James Winn Executive Vice Pres.	11/29/99

**A.6 State Authorities**

State Authorities	Location	Contact Person	Interview Date
Missouri Bureau of Narcotics and Dangerous Drugs	Jefferson City, MO	Dan Crider	11/19/99
Maryland State Board of Pharmacy	Baltimore MD	Melvin Rubin	11/15/99
State of California Bureau of Narcotic Enforcement	Sacramento, CA	Chris Bucher	11/17/99
Ohio Board of Pharmacy	OH	Tim Benedict	11/12/99
Massachusetts Board of Pharmacy	Massachusetts	Chuck Young	11/19/99
Nevada State Board of Pharmacy	Reno, NV	Joanee Quirk	11/10/99
New York Department of Health	Troy NY	James Giglio	11/17/99
New York Board of Pharmacy	Albany, NY	Lawrence H. Mokhiber	Fax

**A.7 Others**

Others	Location	Contact Person	Date/Time
Kaiser Permanente	CA	Steven Gray	11/23/99
St. Elizabeth's Med. Center	Ky	Don Ruwe	11/15/99
Proxymed	FL	Phillip Giordano	11/8/99

## Appendix B—Documents Reviewed

### B.1 Associations

The National Association of State Controlled Substances Authorities (NASCSA)

American Society for Automation in Pharmacy (ASAP)

National Council for Prescription Drug Programs (NCPDP)

### B.2 Documents Reviewed

Author	Title	Date	Source
Adams C. Farrell S.	Internet X.509 Public Key Infrastructure; Certificate Management Protocols	March 1999	<a href="http://www.ietf.org/rfc/rfc2510.txt">http://www.ietf.org/rfc/rfc2510.txt</a>
Arsenault A. Turner S.	Internet X.509 Public Key Infrastructure PKIX; Roadmap	October 22, 1999	<a href="http://search.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-04.txt">http://search.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-04.txt</a>
Chokhani S. Ford W.	Internet X.509 Public Key Infrastructure; Certificate Policy and Certificate Practices Framework	March 1999	<a href="http://www.ietf.org/rfc/rfc2527.txt">http://www.ietf.org/rfc/rfc2527.txt</a>
DEA's Office of Diversion Control	Pharmacist's Manual 8 <sup>th</sup> Edition	March 12, 1999	Controlled Substances Act of 1970
DEA's Office of Diversion Control	Prescription Accountability Resource Guide	September 1998	Prescription Programs Resource Guide
DEA's Office of Diversion Control	Technological Advances to Enhance Diversion Programs	January 1995	DEA
Department of Veterans Affairs and Cygnacom Solutions	VA PKI: Certificate Policy, Draft	June 14, 1999	Department of Veterans Affairs

Ford W. Housley R. Polk W. Solo D.	Certificate and CRL profile; Internet X.509 Public Key Infrastructure	October 22, 1999	<a href="http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-00.txt">http://www.ietf.org/internet-drafts/draft-ietf-pkix-new-part1-00.txt</a>
Management of Federal Information	Office of Management and Budget	March 5, 1999	Federal Register
Muirhea, Greg	New program reveals whether the patient filled the Rx	June 26, 1995	Drug Topics
Shirey R.	Security Glossary	October 17, 1999	<a href="http://search.ietf.org/internet-drafts/draft-shirey-security-glossary-01.txt">http://search.ietf.org/internet-drafts/draft-shirey-security-glossary-01.txt</a>
Stieghorst, Tom	Prescriptions can be written on-line	July 31, 1995	Sun-Sentinel
Treasury Board of Canada Secretariat	Digital Signature and Confidentiality; Certificate Policies	April 1999	GOC PKI Certificate Policies Version 3.02
Tunitas Group	Healthcare Model Certificate Policy, Tunitas, Draft model policy from 10/15/99	October 15, 1999	<a href="http://www.tunitas.com/pages/PKI/pki.htm">http://www.tunitas.com/pages/PKI/pki.htm</a>
Unknown	Electronic Prescriptions	November 19, 1998	NACDS
Unknown	ProxyMed Expands its Electronic Scripts Reach	Unknown	Health Data Network News

### B.3 Internet Resources

The Federation of State Medical Boards of the United States, Inc (1999). URL <http://www.fsmb.org/>

American Academy of Family Physicians (1999). URL <http://www.aafp.org/>

Academy Managed Care Pharmacy (1999). URL <http://www.amcp.org/>

American Society of Consultant Pharmacists. URL <http://www.ascp.net/>

American Society of Health-Care Pharmacists. URL <http://www.ashp.org/>

National Community Pharmacists Association. URL <http://www.ncpanet.org/>

### B.4 Regulatory Bodies, Laws, Regulations and Proposed Legislation

Drug Enforcement Administration (DEA)

Controlled Substance Act (CSA) of 1970

Code of Federal Regulations (21 CFR, Parts 1300 to end)

Government Paperwork Elimination Act (GPEA)

FDA, HHS 21 CFR Part 11

National Conference of Commissioners on Uniform State Law (NCCUSL)

Health Care Financial Administration (HCFA) Internet Security Policy

*Health Insurance Portability and Accountability Act of 1996 (HIPAA):* Security and Electronic Signature Standard (45 CFR Part 142), National Standard Health Care Provider Identifier (NPI), National Standard Employer Identifier, Standards for Electronic Transactions and Code Sets, National Standard for Identifiers of Health Plans, National Standard for Health Claim Attachments, Standards for Privacy of Individually Identifiable Health Information

National Archives and Records Administration (NARA)

## **B.5 Conferences and Seminars**

Public Key Infrastructure Analysis, DEVA PKI Pilot Program Plan, August 6, 1999, Author: PEC, DEA Office of Diversion Control.

**Appendix C—Listing of Acronyms**

ACF	Access Control Facility
ASAP	American Society for Automation in Pharmacy
ATM	Asynchronous Transfer Mode
CA	Certification Authority
CFR	Code of Federal Regulations
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
DEA	Drug Enforcement Administration
DEVA	DEA-Department of Veterans Affairs
DN	Distinguished Name
DUR	Drug Utilization Review
EDI	Electronic Data Interchange
EDT	Electronic Data Transmission
EMR	Electronic Medical Records
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure

GOC	Government Of Canada
GPEA	Government Paper Elimination Act
HCFA	Health Care Fraud Alert
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMO	Healthcare Maintenance Act
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRM	Information Resource Management
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LE	Law Enforcement
LEA	Law Enforcement Agency
LTCF	Long Term Care Facility
MADI	Manufacturers and Distributors
MCP	Multiple Copy Prescriptions
NABP	National Association of Boards of Pharmacy
NARA	National Archives and Records Administration
NASCSA	National Association of State Controlled Substances Authorities
NCCUSL	National Conference of Commissioners on Uniform State Law
NCPDP	National Council for Prescription Drug Programs

NIST	National Institute of Standards & Technology
NPI	National Standard Health Care Provider Identifier
NPRM	Notice of Proposed Rule Making
NPS	National Provider Service
NTP	Narcotic Treatment Programs
OD	Office of Diversion Control
OMA	Operations Management Authority
OMB	Office of Management and Budget
PBM	Pharmacy Benefit Management
PEC	Performance Engineering Corporation
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMA	Policy Management Authority
POC	Proof Of Concept
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, & Adleman
Rx	Prescription
TCP/IP	Transmission Control Protocol / Internet Protocol
UCF	Universal Claims Form
UCITA	Uniform Computer Information Transaction Act
UETA	Uniform Electronic Transaction Act
UID	Unique Identifier

VA	Veterans Affairs
VPN	Virtual Private Network
X.500	The standard for directory services
X.509	The standard for PKI certificates
XML	Extensible Markup Language

## **Appendix D—Veterans Health Administration IT Environment**

Appendix D omitted, please contact DEA for further information.