Cybercrime, Cyberterrorism, and Cyberwarfare

Critical Issues in Data Protection for Health Services Information Systems

Technology and Health Services Delivery
Health Services Organization Unit (THS/OS)

Pan American Health Organization
Pan American Sanitary Bureau, Regional Office of the
World Health Organization

June 2003

PAHO Library Cataloguing-in-Publication Data

Ramsaroop, Peter
Cybercrime, Cyberwarfare, Terrorism, and Sabotage:
Critical Issues in Data Protection for Health Services Information
Pan American Health Organization.
Washington, D.C. : PAHO, © 2003. 85 pages

ISBN 92 75 12464 7

I. Title. II. Stull, Roger III. Rodrigues, Roberto J.
IV. Hernandez, Antonio

1. MEDICAL INFORMATICS
2. COMPUTER SECURITY
3. TECHNOLOGY CONTROL
4. HEALTH SYSTEMS
5. CONFIDENTIALITY
6. COMPUTER COMMUNICATION NETWORKS

NLM WA26.5.R178c

ISBN 92 75 12464 7

Peter Ramsaroop

Chairman and Chief Executive Officer,
EVOLVENT Technologies Inc., Falls Church VA, and
Adjunct Professor, Uniformed Services University of the Health Sciences
Bethesda MD, USA

Roger Stull

Chief Executive Officer, LRS Health Systems, Falls Church VA, and
Former Health Administrator, U.S. Air Force Medical Services

Roberto J. Rodrigues

Adjunct Professor, Science, Technology and International Affairs Program
School of Foreign Service, Georgetown University, Washington D.C and
Senior Consultant, The Institute for Technical Cooperation in Health Inc. (INTECH),
Potomac MD, USA

Antonio Hernandez

Regional Advisor, Clinical Engineering and Maintenance
Pan American Health Organization/World Health Organization
Washington D.C., USA

Contents

Foreword

"Our IT networks are an integral part of our critical infrastructure. They will become ever more critical as e-commerce becomes a more and more common way of doing business, and as more and more governments move to provide electronic access to services and programs."

Margaret Purdy

Associate Deputy Prime Minister
Office of Critical Infrastructure Protection
and Emergency Preparedness, National Defence
Canada

Health information and communication technologies (ICT) applications have been deployed with variable degree of expertise and success with the objective of improving health services operation, management, patient care, and knowledge management. Functions most widely supported include clinical and administrative messaging; material, financial, and human resource operation and administration; logistical management of health sector tasks and patient information; health education and promotion; epidemiological surveillance and health status monitoring; clinical decision assistance; access to knowledge; image, signal analysis, and modeling; and remote consultation and intervention.

Threats to health information data integrity, privacy, and security, to information technology (systems, networks and infrastructures), and to critical facilities infrastructure are becoming more prevalent, and come from a greater variety of sources than ever before. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, governance, banking and finance, transportation, health, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. Information technology and the necessity of improved efficiency have made these infrastructures increasingly automated and interlinked creating vulnerabilities due to equipment failures, human error, natural causes, and deliberate attacks.

Addressing these vulnerabilities will necessarily require flexible and adaptative approaches that span both the public and private sectors, and protect domestic and international security.

With the growing advances in information and medical technologies and logistical and management resources that use networked system, healthcare providers must stay alert and knowledgeable of the “informational” threats to patient and medical organizations and facilities, data, and supporting critical information technology and infrastructure that are critical to their ability to provide uninterrupted and safe services. Awareness of cybersecurity and physical security threats to medical information and patients; and a commitment to securing and protecting information and critical infrastructures must become embedded in the daily business practices and processes of healthcare facilities and agencies.

Based upon the global nature of the threats of cybercrime, cyberterrorism, and cyberwarfare, to healthcare organizations information and technology resources the issue has been in the agenda of numerous organizations and agencies worldwide. They recognized the need for introducing information, guidance, and standards into the healthcare industry to assist governments, agencies, organizations, providers, and patients with the call for medical information security and privacy. Among the most active international groups and organizations, are the G8 countries technical committees, the Organization for Economic Cooperation and Development, the United Nations, and the European Union.

As part of its technical knowledge dissemination mission, the Pan American Health Organization, Regional Office for the Americas of the World Health Organization, recognized the need prepare a publication direct to health professionals dealing with current issues related to systems security and data protection and privacy that are critical to healthcare organizations, agencies, providers and ultimately patients.

This publication purports to raise the awareness of health decision-makers in the public and private sectors in the Region of the Americas. Its scope focuses primarily on addressing the need to increase awareness of critical issues in data protection for Health

Services Information Systems related to cybersecurity requirements and concerns. This brief review is not intended to be an all-inclusive paper on every security issue and solution pertinent to healthcare governing organizations, agencies, facilities, and providers; however, it presents sufficient information to raise the awareness of key healthcare policy makers, managers and provider on the steps they must take toward information and privacy security assurance. Multiple sources of information related to the security and privacy of information and information technology were consulted. Of particular interest are documents that are referenced from U.S. and international organizations focused on the protection and privacy of personal information.

The Authors

1. Introduction

The use of information systems, electronic networks, and the entire information technology environment changed dramatically in last decade expanding and linking all social sectors. Those advances brought significant benefits to individual citizens and to the financial, industrial, business, academic, and service sectors. Yet, the **reliable and safe operation** of the myriad of technological solutions, information systems, and support infrastructure requires that far-reaching concerns about **security** issues are effectively addressed by governments, business concerns, organizations, and individual users who develop, own, provide, manage, service, and use those information systems, resources, and networks.

As the civil society, particularly in industrialized countries, became to a greater extent dependent on information technology and systems, the information infrastructure and the systems themselves turned into another area for illegal activity as criminals and criminal organizations learned to take advantage of **information technology for illegal purposes (Cybercrime)** and for **indiscriminate violence against civilians and civil institutions (Cyberterrorism)** with the purpose of causing confusion and unrest, and destroying their faith on leaders, policies, and institutions. Government agencies and military organizations have waged **electronic war operations against military institutions and well-defined targets of military tactical or strategic importance (Cyberwarfare)**.

1.1. Fighting Cybercrime, Cyberterrorism, and Cyberwarfare

The distinction between **cybercrime** on one side and **cyberterrorism and cyberwarfare** on the other is of significant import as the ways and means to detect and fight each are radically different. Equating a terrorist that bombs civilian targets with criminals and thus being on a par with smugglers, drug traffickers, Internet pornographers, and others, generally limits protective interventions to mostly reactive and defensive measures. As is the case with the determined and often

suicidal terrorist, his or her characterization as a “criminal” and the use of traditional law enforcement interventions is utterly inadequate to deal with individuals and organizations that are highly organized and trained paramilitary units conducting offensive campaigns against nations and civilian organizations and populations that they consider to be at war.

Nature, methods, and motives are quite different in criminals and terrorists. The criminalization of cyberterrorism and failure to acknowledge that they are the cyberspace equivalent of combatants restricts the nature, scope, and efficacy of required responses. In truth, international terrorism has always been what its perpetrators have indicated: a form of warfare -- that requires a different type of preparation and response, many times of pre-emptive nature [1].

The fight against national and international **cyberterrorism and cyberwarfare** requires a perspective different of the simplistic law enforcement and intelligence reactive type of response that is, in most cases, appropriate for the detection and apprehension of criminals. As in war, the response to cyberterrorism and cyberwarfare requires a concerted proactive involvement of the whole “society of users”, as a weak link in the security of the infrastructure can bring down significant portion of systems and cause severe and costly service disruption to all. No better examples of this have been the repeated incidents of **computer virus attacks** to public and private systems in the last years and the downright poor level of preparation of the society, organizations, and the international community to deal technically and legally with the perpetrators. Those attacks can rightly be considered as cases of cyberterrorism.

As it will be discussed later in this book, **effectively dealing with cyberterrorism and cyberwarfare** requires a raised level of awareness, shared responsibility, constant risk assessment and testing procedures, the management of identified risks, and finally the most difficult issue of implementing truly comprehensive and steadfast legal and enforcing mechanisms. Similar to what has occurred in understanding the “bomb terrorist” motives, mode of action, and categorization as a combatant, confusion and argument over terms and concepts, goals, and strategies, have hampered the **achievement of appropriate responses** against cyberterrorism. Among the most **controversial issues** has been those

related to the definition of terrorism as an immoral war against civilians independent of the justification for it; the encroachment on personal freedom and privacy, and on the sovereignty of states, when taking measures to reduce the vulnerability of systems to attack; and finally, the regulatory mechanisms and form, extend, and degree of the use of coercive power against attackers – or, as succinctly put by Thomas Hobbes in the XVII century, "covenants without the sword are but words, and of no strength to secure a man at all" [1].

1.2. Information Systems in Health

The diffusion and use of information systems by the health sector and healthcare services is **growing dramatically**. A vast number of applications are used by all types of organizations in support of the logistics and operation of health programs and healthcare provision, in the management of resources, for communication among providers and other stakeholders, to search and retrieve data from knowledge bases, and as a central component of diagnostic and therapeutic interventions. Functions that were once thought to be the sole province of the professionally trained mind and only trusted to pen and paper are now routinely performed by systems considered to be highly accurate and reliable.

Patient information that was recorded on paper and most of the times available only at the site of care and during the course of an acute episode of illness, is now packaged, formatted, related and stored conveniently in computerized patient records and databases to be accessible from any place at any time in the future. Examples of this fact include automated clinical pathway systems, automated physician order entry with conflict alerts for pharmacy, dietary and laboratory, and massive databases and data warehouses used for case, disease, utilization management, and epidemiological studies.

The advances in computer science in the last decade as well as a growing acceptance of information systems as reliable tools in the health services community are creating a new and expanding connectivity between health services enterprises, systems and information. This growing connectivity is cutting through traditional

barriers and borders and opening the future to new levels of professional, scientific and national and international cooperation and collaboration. Introduction of the latest advancements in information technology capabilities -- hardware and software -- as well as information and knowledge management practices into healthcare facilities and supporting agencies, is rapidly improving the quality of healthcare provided worldwide. Introduction of information technology solutions; and information management processes has also significantly improved patients' accessibility to healthcare providers and facilities; as well as access to their patient care information on a daily basis. As more expert systems are introduced into traditional areas of healthcare the processes become more efficient and extend the reach and efficacy of the caregiver.

But those gains do not come without a price. In this context of widespread utilization and increasing dependency on information and communication technologies by the health sector, the **issues of security and privacy of healthcare information are a vital matter to health organizations and care providers**, who have become increasingly reliant upon such resources for the daily operation of their clinical, administrative, and business practice.

1.3. Security and Privacy: The Core Issues

In times past, patient information, clinical data, healthcare delivery data and financial data didn't hold much significance for anyone but those directly involved in the receipt or delivery of health services. Healthcare institutions were self-centered caregivers with information kept in supervised paper files. This was not very efficient, but tended to be very secure. Information in healthcare services were also pretty much compartmentalized within clinical or administrative areas and was limited to the local operation. In the few instances (e.g., malpractice litigants, personal interest, business or competitive interest) where unusual interest did exist, **access was very limited due to the difficulties in assembling relevant information from distributed sources**.

With information and telecommunication technologies, the processes of information-dependent activities gain in capacity, speed,

and quality. But those processes become also dependent upon the **reliability** and **availability** of the technical system and resources that provide the gains. The issue of reliability of the data that move in the system is particularly important in the health sector -- as the connectivity between information sources from various clinical areas such as pharmacy, laboratory, radiology, dietary and patient scheduling grows, more efficient and safer clinical pathways are enabled but, in doing so, the process becomes totally dependent upon the **integrity** and **accuracy** of the system. The new connectivity between health services data sources and advances in technology for collecting, classifying, grouping and search open possibilities for community, area and national health planners and policy makers never before considered. New capabilities in case, disease and utilization management become possible along with gains in the efficiency of epidemiological studies. Health planners are allowed a new perspective for health needs at the community and population level.

As our dependence to information technology and systems increase, **securing systems** to be consistently reliable and available and producing information that is accurate and protected against deliberate or accidental illegitimate modification becomes a major issue. In bringing together information and classifying data so that it can provide the gains mentioned, the **sensitivity of the information** grows and can impinge significantly on **personal privacy** aspects as well as growing in value to criminals, economic and political spies, and even for military intelligence. The health system as well as related social, cultural, and government processes become inextricably and highly dependent on the **confidentiality** of the system that contains the information in order to protect the privacy of individuals.

Security and privacy of information stored in systems and shared across networks and systems, an environment referred to as **cyberspace**, are of vital concern for managers at all levels of organizations as well as individuals. For those who grew up in gentler times, treasured honor and tradition, and only had to contend with world wars, revolutions, local criminals, the occasional plague, and the family doctor, the language and openness of the information society can be daunting. Who I am, what I am, what I do, and what I own is threatened in ways no one could have imagined just ten years ago.

1.4. Security Risks in Health Information Systems

Each day, huge amounts of sensitive data are exchanged within and between organizations' networks, many of those networks being public channels. As a result of **increasing interconnectivity**, information systems and networks are exposed to a growing number and a wider variety of **threats and vulnerabilities**. Threats to healthcare data and information systems can come from many sources. **Attacks by criminals, teenager hackers, terrorists, disgruntled employees, or agents of external organizations or other nations use the same tools and methods, exploit the same systems and organizational vulnerabilities, and cause similar damage. Most importantly, these attacks require the same defensive measures**.

Organizations must evolve their methodologies to address these changes and provide **information assurance that is effective, consistent, and continuous**. Because of this, organizations must develop security policies and guidelines for their information assets that apply to all systems and that actively support the need for greater awareness and understanding of security issues with the goal of developing a **"culture of security"**.

In this context, **cybersecurity** has to do with ensuring the safety of networked information systems. The following are **examples of common threats** that can result from cybercrime, sabotage, cyberterrorism, and cyberwarfare actions:

- **Malicious hackers**, those that break into computer systems without authorization, are especially troubling because their identity and purpose are unknown.

- **Malicious code**, such as viruses, computers worms, Trojan horses, and logic bombs, that can cause serious damage and disruptions of applications and computer networks and can be costly to remedy.

- **Employee sabotage or spying** can cause serious problems because the employee may have detailed

knowledge of systems operations and their physical and technical vulnerabilities.

- **Threats to personal privacy** are of concern because computers store vast amounts of electronic information about employees, patients, other beneficiaries, suppliers, business partners, and financial transactions.

1.5. Developing a "Culture of Security"

Individuals, as fitting to their professional roles, should be aware of the relevant security risks, required preventive measures, and assume responsibility and take steps to enhance the security of information systems and networks they deal with. **Each individual in an organization is important for ensuring an appropriate level of cybersecurity**.

Promotion of a culture of security requires both leadership and extensive participation and should result in a heightened priority for security planning and management, as well as an understanding of the need for security among all participants. Security issues should be topics of concern and responsibility at all levels of government and business and for all individual participants of the organization.

Information assurance means providing the right information to the right people at the right time. Although simplistic in concept, it involves much more than data security, i.e., the reliability, availability, integrity, accuracy, and confidentiality of data and more than protecting your computer information system from internal or external disruption. **Information assurance is the systematic approach to protecting an organization's intellectual property from all potential exposures, both intentional and accidental, and minimizing the consequent effects**. Information assurance assumes the responsibility of every individual in the organization, as well as every agency, firm, or company with which the organization interacts [2].

To assure the security and privacy of critical information (**information assurance**), systems, networks, and infrastructure including information and communication technologies and physical facilities, organizations at all levels and of all types need to establish security goals in order to:

- Raise **awareness** about security risks to information systems and networks; about the policies, practices, measures, and procedures available to address those risks; and the need for their adoption and implementation at all levels of an organization.

- Promote a **culture of security** among all members of their organization as a means of protecting information systems and networks.

- Foster greater **confidence** among all users of information systems and networks and the way in which they are provided and used.

- Create a general frame of reference that will help individuals **understand security issues and respect ethical values** in the development and implementation of coherent policies, practices, measures, and procedures for the security of information systems and networks.

- Promote **cooperation and information sharing**, as appropriate, among all organizational members in the development and implementation of security policies, practices, measures, and procedures.

- Promote the consideration **of security as an important objective** among all participants involved **in the development or implementation of standards**.

Emphasis on **information assurance**, **contingency and continuity of operations planning**, **emergency and disaster**

preparedness, training, and recovery must be put into place by organizational management to guarantee the security and protection of their vital information and the critical technology and infrastructure related to information systems.

Healthcare organizations must **assure the privacy and security** of information, and **insure continuation of quality patient care** in support of the credo to “to do no harm” in the midst of disaster and emergency situations; as well as in routine healthcare daily operations. **Emergency and disaster preparedness and recovery are primary duties of healthcare providers and other first responders and must be carefully taken into consideration when planning an information system operational capabilities**.

2. Nine Principles for the Security of Information Systems and Networks

The following nine guiding principles were developed by the Organization for Economic Cooperation and Development Working Party on Information Security and Privacy (WPISP) and transcribed with minimal editing from a 2002 publication [3], pursuant to a mandate from the Committee for Information, Computer and Communications Policy (ICCP).

They concern developer, users, and stakeholders at all levels, including policy and operational personnel (participants). Under these principles, the responsibilities of participants vary according to their roles.

All participants will be aided by **awareness, education, information sharing, and training** that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be **consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy**.

2.1. Awareness

- All participants must be aware of the **need for security** of information systems and networks and what they can do to enhance security.

- **Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks**.

- Information systems and networks can be affected by both **internal and external risks**.

- Participants should understand that **security failures may significantly harm systems and networks** under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency.

- Participants should be aware of the configuration of, and available updates for, their system, its place within networks, **good practices that they can implement to enhance security**, and the needs of other participants.

2.2. Responsibility

- **All participants are responsible for the security** of information systems and networks. Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. **They should be accountable in a manner appropriate to their individual roles**.

- Participants should **review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate** to their environment.

- **Those who develop, design, and supply products and services should address system and network security** and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

2.3. Response

- Participants should **act in a timely and cooperative manner** to prevent, detect, and respond to security incidents.

- Recognizing the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should **address security incidents and share information about threats and vulnerabilities and implement procedures for rapid and effective cooperation** to prevent, detect, and respond to security incidents. Where permissible, this may involve cross-border information sharing and cooperation.

2.4. Ethics

- Participants should **respect the legitimate interests of others**. Given the pervasiveness of information systems and networks in our societies, **participants need to recognize that their action or inaction may harm others**.

- Ethical conduct is therefore crucial and participants should strive to develop and **adopt best practices** and to promote conduct that recognizes security needs and interests of other individuals.

2.5. Democracy

- The security of information systems and networks should be **compatible with the essential values of democratic societies**.

- Security should be implemented in a manner consistent with the values recognized by those societies including

the **freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness, and transparency**.

2.6. Risk Assessment

- Risk assessment identifies threats and vulnerabilities and should be **sufficiently broad-based** to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications.

- Risk assessment will allow **determination of the acceptable level of risk and assist the selection of appropriate controls** to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected.

- Because of the growing interconnectivity of information systems, risk assessment **should include consideration of the potential harm that may originate from others or be caused to others**.

2.7. Security Design and Implementation

- Participants should **incorporate security as an essential element of information systems and networks**.

- Systems, networks and policies need to be properly designed, implemented, and coordinated to **optimize security**. A major, but not exclusive, focus of this effort is the **design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities**.

- Both technical and non-technical safeguards and solutions are required and **should be proportionate to the value of the information on the organization's systems and networks**.

- Security should be a **fundamental element of all products, services, systems and networks**, and an integral part of system design and architecture.

- For **end-users**, security design and implementation consists largely of selecting and configuring products and services for their system.

2.8. Security Management

- Participants should adopt a **comprehensive approach to security management**. Security management should be **based on risk assessment and should be dynamic**, encompassing all levels of participants' activities and all aspects of their operations.

- Should **include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review, and audit. Information system and network security policies, practices, measures and procedures**. All such components should be coordinated and integrated to create a coherent system of security.

- The **requirements of security management** depend upon the level of involvement, the role of the participant, the risk involved, and system requirements.

2.9. Reassessment

- Participants should **review and reassess** the security of information systems and networks, and **make appropriate modifications to security policies, practices, measures and procedures**.

- **New and changing threats and vulnerabilities are continuously discovered**. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

3. Cyberspace Security Threats

Risk and threats to critical healthcare information and information technology supporting healthcare organizations can come from **natural or man-made emergencies and disasters** (fire, flood, storms, etc.) or they can result from the **action of individuals**, both **intentional** (e.g., criminal or unlawful activities, disgruntled employee sabotage, terrorism) and **unintentional** (e.g., lack of training on proper routines and procedures, human error, laziness, disregard for procedures).

3.1. The Scope of the Problem: Examples of Recent Threats

A few examples highlight the **variety of threats, sources, and the international dimension of the problem of cybersecurity**:

- In 1998, at a time of increased international tension, U.S. military logistics, administrative, and accounting systems were **penetrated by what appeared as a major cyber attack by a hostile nation**. The source of the attack was traced to the United Arab Emirates. As it turned out, three teenager hackers from California and Israel had organized the attacks using software tools readily available on the Internet and tried to hide their involvement by routing their attacks through servers in different countries.

- In February 2000, servers hosting several large commercial websites on the Internet were **flooded with connection requests overwhelming the networks and systems** – a so-called distributed denial of service attack. It was found out that a young Canadian hacker was responsible for the slowdowns and service outages that cost more than 1 billion U.S. dollars in economic losses worldwide.

- In May 4, 2000, the “I love you” virus released by a computer science student in the Philippines. The **virus swept the globe and infected nearly 60 million computers and caused an estimated 13 billion U.S. dollars in damage**. The student could neither be charged nor punished because that country criminal code at the time did not explicitly outlaw such actions.

- On November 2002, a series of **simultaneous distributed denial of service attacks were directed at thirteen Internet root servers** – the main computers that manage global Web traffic.

- On January 25, 2003, a **self-propagating worm dubbed Slammer, Sapphire and SQL Hell, demonstrated the vulnerability of systems and the problem of not using available protective measures**. Although a known flaw in Microsoft’s widely-used SQL database had a corrective patch available, a large number of system’s administrators failed to update their systems. The negligence resulted in thousands of systems infected and widespread disruption of networks.

- There have been **many cases of electronic patient records stolen and published on the Internet**. The records were obtained from unsecured systems and were related to a personal grievance by a healthcare organization employee.

- At the end of 2002, an employee of a major U.S. credit rating agency **stole identification data from thousands of citizens with the objective to sell them to a gang of criminals involved in the growing area of “identity theft”** used to defraud credit card companies and retail businesses.

3.2. Lessons Learned

From the large number of recorded security incidents the following **relevant conclusions** can be drawn [4]:

- **Technical Resources are Widely Available** – the tools used to conduct the attacks are easily and anonymously available to any individual or group regardless of their motivation.

- **Common Patterns** – because tools and methods of attack are so similar across the threat spectrum – from hackers, to criminals and terrorists – many of the technical methods to combat such attacks are also similar.

- **Impact** – due to the highly complex interdependence of global infrastructures, there is no good understanding or way to measure the impact of cyber attacks. Purely in terms of economic impact some of those incidents involved billions of dollars in losses. However, one must think not only in economic terms but also from a national security perspective as cascading failures can be significant enough to have national security implications.

- **National Boundaries** – cyberspace attacks do not respect national boundaries. In fact, perpetrators are likely to purposely route attacks through different countries to decrease the probability of detection or prosecution.

- **Shared Responsibility** – the interconnectedness of global users suggests that the security of all depend on the responsibility of individual system administrators. Least secure countries or sites pose a security risk to all. Good systems security practices implemented by all make successful attacks more difficult.

- **Constant Learning** - Organizations must understand the issues of securing information systems in an ever-evolving and increasingly complex environment. Healthcare organizations and supporting agencies must provide an approach that captures and leverages lessons learned from past experiences and ensures continuity and growth of their security and information technology team's expertise and knowledge of the tasks.

- **International Cooperation** – attempts to track and capture perpetrators requires international cooperation on a significant scale. International cooperation is easier to achieve in controlling cybercrime than in dealing with cyberterrorism.

- **Public-Private Partnership** – because most of the information infrastructure used by the public and private sectors are in the hands of the private sector, security cannot be a government-only responsibility.

- **Cyberterrorism and Cyberwarfare Require Specific Responses** – as indicated in the introductory section, cyberterrorism and cyberwarfare must be equated to military operations requiring a different set of responses than the ones that would be used to counteract cybercrime – for instance, an armed response including pre-emptive strikes, may be required to neutralize threat sources that are embedded in enemy countries or protected by terrorism-supporting states.

3.3. Dealing with Security Threats: The Information Assurance Four-Phase Life Cycle Approach

A dependable **information assurance process** provides the organization with:

- **Method and Road Map** - a solid life-cycle methodology and approach

- **Problem Definition** - identification of risks and vulnerabilities
- **Required Responses** - analysis of current or planned implementations against requirements
- **Solutions** - the next steps that must be taken to support requirements
- **Strategy** - planning including detailed recommendations that are collaboratively derived.

Based upon many years of experience in information assurance in the public and private sector healthcare and non-healthcare organizations, and information assurance, the issue of security and **privacy is best approached by considering a four-phase cycle** [2]. This approach encompasses a continuum of actions that sequentially consider the following phases:

- **Assess**
- **Address**
- **Test**
- **Monitor, Plan, and Improve**.

The methodology defines the **activities, services, technology, and project management components** needed to assess the specific requirements of an information assurance environment and provide a blueprint for tailored successful solutions. Overall this approach maps directly to the accepted standards of U.S. Government agencies within the Department of Defense (DITSCAP, NIACAP, and VAITSCAP)[1], other federal agencies, and commercial organizations (Figure 1).

[1] - DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process)
- NIACAP (National Information Assurance Certification and Accreditation Process)

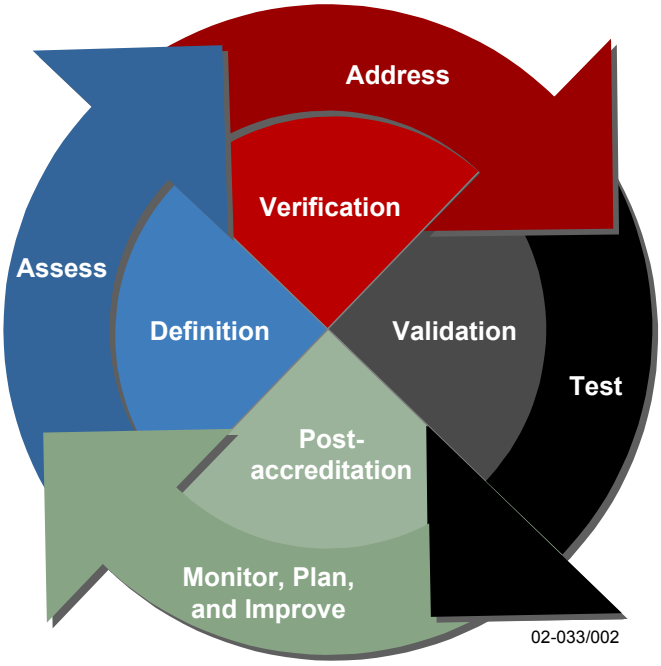

Figure 1. The 4-Phase Security Life Cycle Approach

Assess

The organization must develop an in-depth **understanding of the design and readiness** of their:

(a) Environment (systems and networks)
(b) Processes
(c) Standards
(d) Education
(e) Related risks

VAITSCAP (Veterans Affairs Information Technology Security Certification and Accreditation Process)

This includes a detailed **evaluation of the organization's infrastructure** to ensure an accurate understanding of the current security posture.

Address

The organization must **identify weaknesses and vulnerabilities** including policies, plans, evidentiary documentation, and training implementation of countermeasures and architectures that address the exposures and fortify the client's security posture and information management.

Test

Thorough testing systems for verification and validation must be executed in accordance with requirements and the organization's priorities. Verification and validation evaluations **should be performed typically by an "unbiased third party"** to ensure the protective measures effectively perform as they were intended.

Monitor, Plan, and Improve

Organizations must be capable of providing **critical near- and long-term guidance** along with enhancement of processes and workflows, which will reduce risk effectively and within budget. They should also provide **post accreditation system management and operation** to ensure that an acceptable level of residual risk is attained.

Experts must **continually tailor processes and procedures** to incorporate their recent experience to improve effectiveness and efficiency. **Sharing of information between "trusted partners" and organizations** on lesson learned and processes and procedures for securing information and their supporting technology infrastructure is essential. Utilizing the **expertise of security consultant companies**, as required, is an approach that provides organizations with the benefits from the lessons learned by their and other security teams. Those strategies are mutually enhancing toward assuring the security and privacy of their patients' information and their own organizational

business information and technology. The Table 1 summarizes **key foundations for cybersecurity for organizations whether public or private organizations** [3].

Table 1. Cybersecurity Foundation and Corresponding Areas

Key Foundations for Cybersecurity	Areas of Effort to Develop Foundation
Securing shared systems	Securing the resources of the Internet Supervisory control and data acquisition systems Research on threats and vulnerabilities Highly secure and trustworthy computing Securing emerging systems Vulnerability remediation
Fostering a reinforcing economic and social framework	Awareness Training and education Certification Information sharing Study of crime-related opportunities and means Market forces Privacy and personal data protection
Developing national (and organizational) plans and policy	Analysis and warning requirements Continuity of operations, reconstitution, and recovery from disaster or attack National and organizational security Interdependency of physical security

The strategic goal for **securing the mechanisms for public networks (Internet)** is to foster the development of secure and robust mechanisms that will enable the support of users needs now and in the future. Securing the mechanisms includes:

- **Software** - improving the security and resilience of key Internet protocols
- **Physical Systems** - increasing router security
- **Standards** - adopting best security standards, practices and criteria – “code of good conduct”; and

- **Cooperation** - establishing a public-private partnership to identify and address fundamental technology needs for the Internet

4. Risk Management

The Figure 2 presents a model for **threat and risk assessment (TRA) management** advocated by the Canadian Government and used throughout the world to deal with risk management. As depicted, **risk management is an activity that must begin with the very first steps in developing an information system and that continues throughout the life cycle of the system**. It involves:

Planning

- Aim (Goals)
- Scope
- Gathering Information
- System Description
- Target Risk and Required Certainty

Threat and Risk Assessment

- Preparation
- Analysis
- Recommendations

Requirements Definition

Safeguard Selection

- Administrative
- Personal
- Physical
- Technical
- Economic

Life Cycle Evolution

Activity that must begin with the very first steps in developing an information system and continues throughout the life cycle of the system

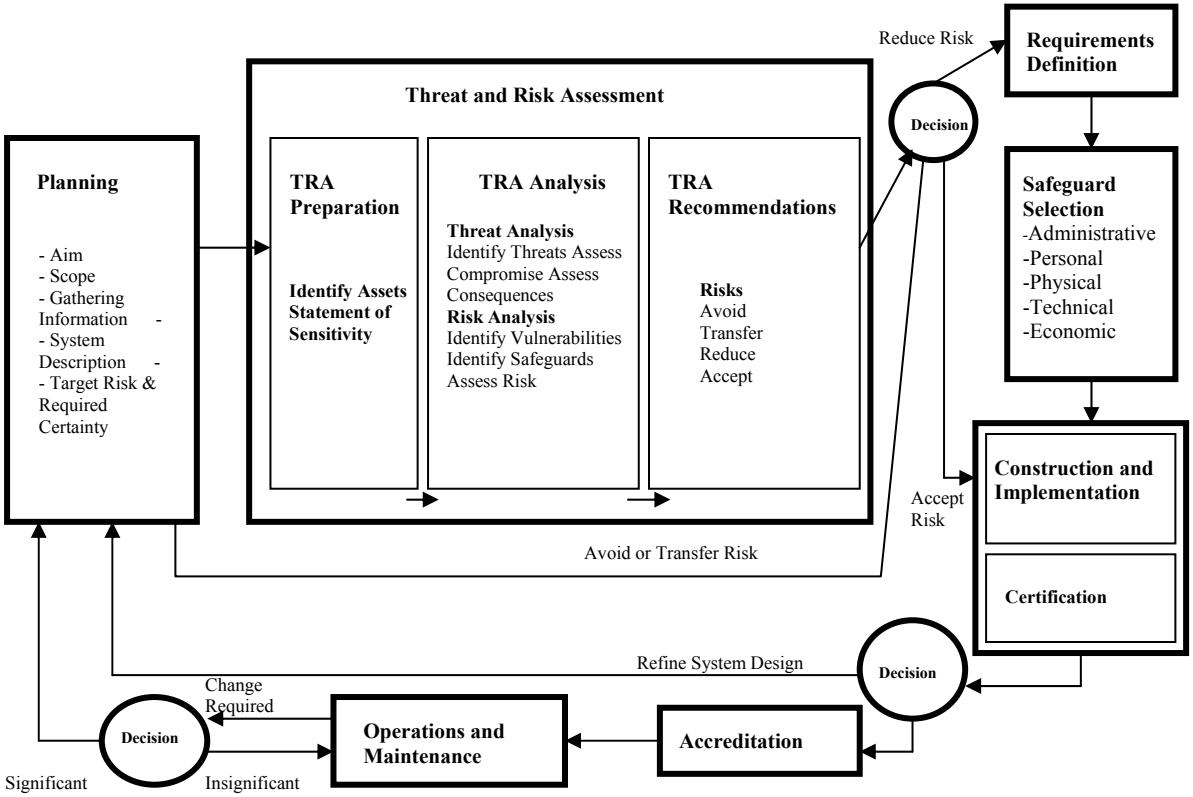

Figure 2. Risk Management Model

4.1. How Much Security Is Enough?

Security in any system should be commensurate with its risks. However, the process to determine which **security controls** are appropriate and cost-effective is quite often a **complex and sometimes by far a subjective matter**. One of the prime functions of security risk analysis is to put this process onto a more objective basis. **A risk assessment produces an estimate of risk to an information system at a given point in time**. It answers the following questions:

- What is at risk?
- What can go wrong?
- How bad could it be?
- How likely is it to occur?
- What is an acceptable amount of risk versus the cost of risk avoidance/information assurance for the organization?

The resulting **measure of risk** is also referred to as a risk assessment. There are a number of distinct approaches to risk analysis; however, these essentially break down into two types: **quantitative and qualitative**.

4.2. Quantitative or Qualitative Risk Analysis?

A quantitative measure of risk can be developed in some cases. The **quantitative analysis** approach employs two fundamental elements; the **probability** of an event occurring and the **cost** should it occur. Cost can be expressed in many forms but financial controls quantitative risk analysis makes use of a single figure produced from these elements. They define measurements called the **Annual Loss Expectancy (ALE)** or the **Estimated Annual Cost (EAC)**. This is

calculated for an event by simply multiplying the potential loss by the probability.

It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this. ALE and EAC often provide a good starting point for the auditor in developing a quantitative risk model. But, **the term "quantitative" can give a false sense of confidence since the estimation of impact and assignment of probability are as subjective as most qualitative methods**. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability is only an estimate and can, in some cases, promote complacency. While quantitative analysis has sometimes proved to be useful for risk analysis of internal financial controls or classification based on well defined factors, it has not often been used meaningfully in information systems security risk analysis. For information technology systems, however, there is often a high level of uncertainty in many risk variables, in which case qualitative risk measures are the most reasonable choice.

Qualitative risk analysis is by far the most widely used approach to information systems risk analysis. Quantitative probability data is not required and only estimated potential loss is used. It relies on a community body of knowledge and incorporates actual experience. The basic elements to be considered in a qualitative analysis approach are:

- **Threats** - these are things that can go wrong or that can "attack" the system. Examples might include flood, fraud, or hacking. Threats are ever present for every system.

- **Vulnerabilities - t**hese make a system more prone to attack by a threat or make an attack more likely to have some degree of success or impact. For example, related to a flood threat, a possible vulnerability would be the site presence near a river.

- **Countermeasures -** There are four types of countermeasures for vulnerabilities: ***Deterrent controls*** reduce the likelihood of a deliberate attack; ***Preventative***

- ***controls*** protect vulnerabilities and make an attack unsuccessful or reduce its impact; ***Corrective controls*** reduce the effect of an attack; and ***Detective controls*** discover attacks and trigger preventative or corrective controls.

These elements can be illustrated by a simple relational model (Figure 3):

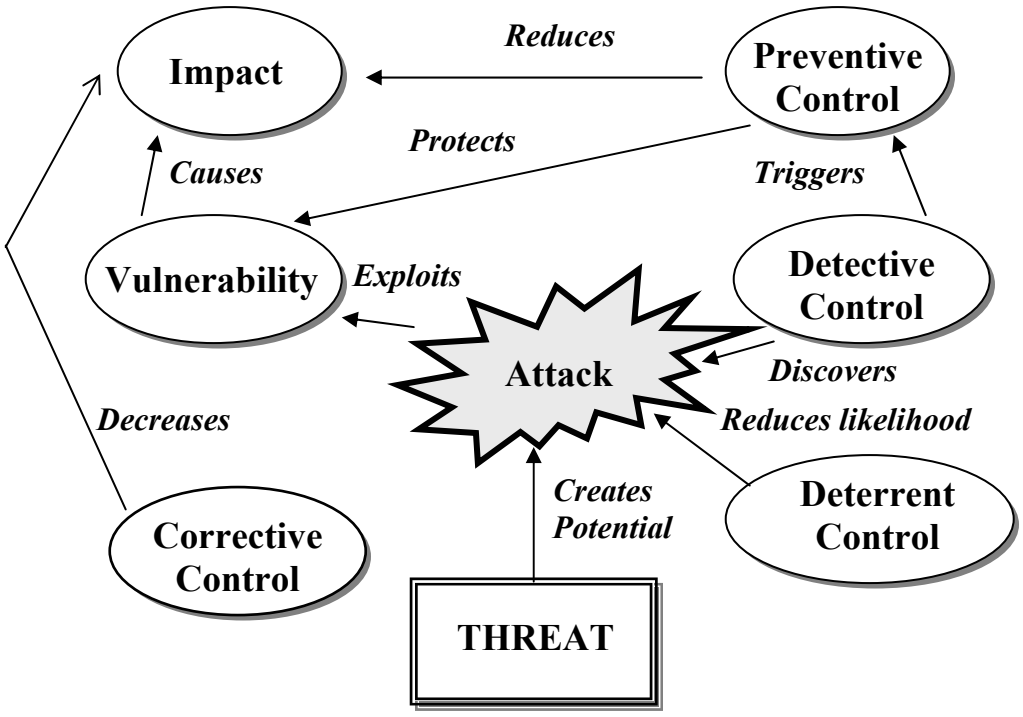

Figure 3. What Could Go Wrong?

4.3. Threat Assessments

The Figure 4 provides a relational view of the elements and relationships involved in the understanding of relevant threats.

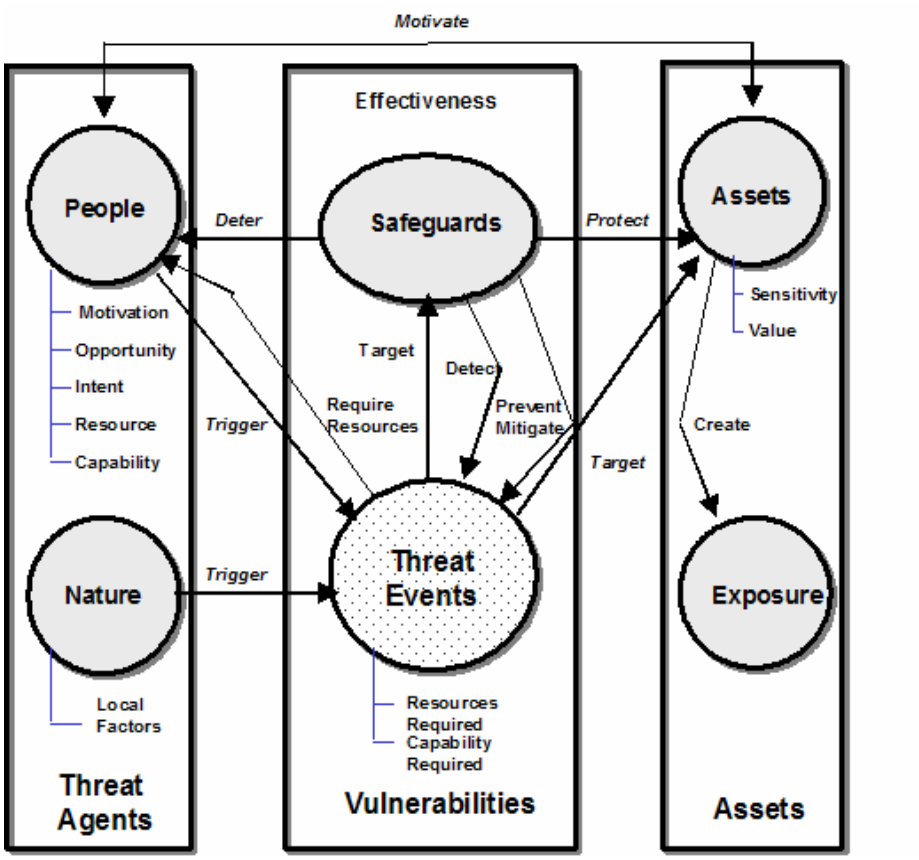

Figure 4. Threat Assessment - Elements and Relationships Involved in the Understanding of Relevant Threats

It is not enough to just consider listings of known threats. An effective **threat assessment must consider agents, vulnerabilities, and assets that could potentially come under attack and business exposure**. The goal is to develop a comprehensive understanding of risk based on the relationship of all four elements. All known threats must be

considered, but they must also be filtered so that system applicable threats may be **focused on for practical safeguard requirements**.

4.4. Taxonomy of a Threat

Threat agents include both **environmental agents** that can cause harm but have no objective and **human agents**, which have particular objectives and may or may not produce harm.

4.4.1. Threat Agent Motivation

Motivations
1. Personal financial gain *Blackmail, competitive advantage, lawsuit, career advancement, corruption of clinical trials or research results, divert valuable assets*
2. Revenge *Denied advancement, perceived wrong, ideological redress (common occurrences from a potentially disgruntled employee; higher probability then most other sources of threat to an agencies information, information technology infrastructure, and/or physical facilities)*
3. Curiosity and thrill seeking *Non-malicious hacker, desire to be an insider, "how does it work" reasons, gain access*
4. Intellectual challenge, learning, need for acceptance and respect *Malicious and non-malicious hackers, destroy data bases, take control*
5. Personal evidence *Cover a crime, cover a mistake, insider and external information destruction*
6. Institutional evidence *Cover crime, cover bad decisions, cover misadventures, change clinical trials or research results, intimidate personnel*
7. Perceived moral or idealism purpose *Religious, cultural and philosophical radicals, demonstrate ideological or religious causes, labor unrest, domestic and foreign cultural agitation, "Robin Hood" motives*
8. Military and national intelligence *Information on readiness, composition and disposition of units, status and intent of forces, impact readiness through destruction of capability*
9.Political and economic intelligence *Gain information on individuals, gain advantage in international negotiations, obtain research and other valuable technical information that would be too expensive to develop by oneself or in failing economies*
10. Business intelligence *Competitive advantage, trade secrets entrusted to government, illegally obtain product specifications or research content and results, illegally obtain data to conduct research*
11. Terror *Create life threatening situations, destroy care capability, weaken culture and values*
12. Ignorance *Intruders may be unaware that actions are illegal and punishable, consultants obtaining unauthorized password block, keys, etc.*

4.4.2. Threat Agent Limitations and Restraints

For a threat agent to be effective, the agent must have **motivation**, **intent or commitment**, **opportunity**, **resources**, and **capability**. Any event or factor that can limit or eliminate one or more of these elements also limits or eliminates the threat.

For the purpose of this paper, limitations and restraints can be summarized into the following general categories:

Threat Limitations and Restraints	
Effectiveness Factor	***Limiting Factors***
1. Motivation	a. Interest b. Perceived probability of success c. Probability of detection
2. Intent/commitment	a. Culture and moral values b. Image c. Perceived probability of punishment d. Perceived value of success
3. Opportunity	a. Awareness b. Access
4. Resources	a. Finances b. Available technology c. Time d. Information
5. Capability	a. Skill b. Knowledge c. Training

4.4.3. Potential Threat Agents

Classes of agents considered potentially threatening to the health services enterprise are numerous. The potential **external** and **internal threat agents** are directly related to motivations and limiting factors as detailed before. **The methodology of coupling agent classes with motivation and limitations will allow the analyst to improve the granularity of the analytical process**.

A. Potential External Threat Agents	
Potential Agents	Defining Risk Factors
1. Foreign Intelligence	Allied, neutral and enemy. Hostilities and peacetime, unpredictable constant threat. Somewhat influenced by agent limitations and constraints in relation to value.
2. Foreign Military	Allied, neutral and enemy. Direct military action in hostilities and intelligence in peacetime. Predictable in hostilities, unpredictable in peacetime. Significant agent limitations and constraints in peacetime, Limited or no constraints in hostilities
3. Terrorist	All times, all causes, all places, direct action and intelligence. Unpredictable, limited or constrained only by opportunity, ability and value to terrorist objectives.
4. Criminal	Direct opportunity, Direct value, derivative value (support of other crimes), and evidence. Unpredictable, somewhat significant limitations and constraints
5. Political	Issue impact, election impact, news impact, unpredictable, changes with time and issues. Very significant limitations and constraints
6. Ideological	Generally related and confined to ideological principles. Unpredictable, significant limitations and constraints.
7. Economic	Developing economies, ease of misappropriation compared to development costs, relatively predictable, significant limitations and constraints.
8. Educational/ Research	Presence of information critical to projects. Unpredictable, very significant limitations and constraints
9. Business	Presence of competitive or economic value. Unpredictable, very significant limitations and constraints.
10. Opportunity Hackers	Unpredictable motivation, Probability 100% that system will be attacked. Threat is 24x7x365. Limited and constrained only by opportunity and ability.
B. Potential Internal Threat Agents	
11. Unintentional	Unpredictable, limited only by access, training, knowledge and personal responsibility

12. Intentional Personal Gain	Personally defined value. Unpredictable, significant limitations and constraints
13. Intentional Personal Harm	Personally defined grievance. Unpredictable, somewhat limited and constrained
14. Intentional Personal Concealment	Related to an event or pattern of behavior that would be susceptible to forensics. Unpredictable, limited only by opportunity and ability.
15. Intentional Institutional Concealment	Presence of financial or operational misconduct. Can be individual or conspiracy somewhat limited and constrained, somewhat predictable with information from other business processes (audit, oversight)
16. Intentional Institutional Harm	Personal grievance, labor unrest, cultural conflict. Somewhat predictable, significant limitations and constraints
17. Industrial Espionage	Potential presence of intellectual property, trade secrets or competitive information. Unpredictable, significant limitations and constraints
C. Environment or Natural Threat Agents	
18. Power	Certainty of occurrence of interruptions, somewhat predictable as to when
19. Water	Somewhat predictable
20. Commercial Communications	Certainty of occurrence of interruptions, somewhat predictable as to when
21. ICT Equipment Failure	Certainty of occurrence of interruptions, unpredictable as to when
22. Environmental Controls	Certainty of occurrence of interruptions, unpredictable as to when
23. Environmental Accident	Unpredictable
24. Physical Security Failure	Presence of value that requires physical presence to realize. Unpredictable, significant limitations and constraints
25. Flood	Presence of geographical and topological factors. Somewhat predictable
26. Fire	Unpredictable
27. Tornado	Geographical factors, somewhat predictable
28. Hurricane	Geographical and seasonal factors, Predictable in the short term
29. Lightning	Unpredictable
30. Ice Storm	Geographical factors, somewhat predictable
31. Earthquake	Geographical factors, predictable as to long term likelihood, unpredictable as to when
32. Volcano	Geographical factors, predictable likelihood
33. Corrosive Chemicals	Predictable, preventable

4.4.4. Assets and Vulnerabilities

Threat agents target assets. A threat can only cause harm when an asset is vulnerable and the vulnerability is exploited. **Assets must be identified to discover applicable threats**. Classes of assets and their potential vulnerabilities are listed below:

System Assets and Vulnerabilities	
Asset	**Potential Vulnerabilities**
1. Personnel	Death or injury, Compromise, Mistakes, Training, Grievance, Accident, Skill Level
2. Facilities	Lax physical security, Limitations in or inappropriate site selection, Inappropriate construction, Contingency and continuity of operations
3. Network Hardware	Susceptible physical configuration, Radiation/Emanations, Physical access controls, Personal controls, Administrative controls, Security policy, Power interruption, Physical damage, Equipment mean time to failure (MTF), Contingency and continuity planning, Corrosion and materials fatigue/failure
4. Network Software/Files	Vendor passwords, Trust files, Default configuration, Guest log-in, plaintext passwords and privileges in tables, Susceptible interfaces, Protocols, Logical access controls, Root files and directories, Trust symmetry (mutual trust between two hosts), Trust transitivity (Mutual trust between two hosts is exploited to use the trust symmetry of the second to a third), Session hijacking, “Spoofing”
5. Peripheral Devices	Location, Physical security, Power interruption, Local modifications, Poor personal security, security policy, Local practices, Security training, Unauthorized connection, Phantom connections (network that is connected to another network through an unauthorized modem or other device)
6. Host Hardware	Mean Time to Failure (MTF), Power backup, Corrosive protection, Environmental controls, Corrosion Facility weaknesses, Physical security, Configuration, Logical access
7. Storage Devices	Equipment failure, Residual data, Configuration, Disposal of equipment, particularly of data storage devices I

8. Host Operating System	Vendor passwords, Design Flaws, Outdated Security Features, Protocols, Languages, Compromised specifications, Releases and updates, Configuration management
9. System Level Software	Vendor passwords, Updates and releases, Configuration management
10. Application Level Software	Releases and updates, Development environment, Access control
11. Operational Data	Back up and recovery, contingency planning, deliberate and non-deliberate corruption
12. Historical Data	Media aging and destruction, Recovery procedures, Storage facility environment
13. System Security Features	Insider system break-in, Deliberate attacks
14. System Security Files	Insider intentional and unintentional corruption and modification
15. Power supply and distribution systems	Design, Corrosion, Power surge or current instability, Capacity planning
16. Environmental systems	Design, Capacity planning, Corrosion, Maintenance
17. Telecommunications systems	Tapping, Intercept, Hacking, Disaster, Service interruption

4.5. How Bad Could It Be and How Likely Is It to Occur

It is necessary to provide guidance to systems developers and managers to work out safeguards into the system that focus on the greatest threats to the system and its data. For new systems the process of assessing the probability of a risk is a theoretical exercise. For systems already in operations, the safeguards already in place must be carefully inventoried and assessed for effectiveness.

4.5.1. Exposure

Business exposures are the **areas of potential harm** where an enterprise is or may be left unprotected and therefore exposed to risks through the **combined effects of threat agents and vulnerabilities and the characteristics and degree of the organization's dependency of the information asset in use**.

Enterprise Exposure
A. Financial Significance
1.Material effect on financial statements *Financial data used in the preparation of strategic planning, department budgets, and financial statement documents*
2. Loss of Intellectual Property *Trade secrets and proprietary information entrusted to public or regulatory agencies. Research and clinical trials. Theft of intellectual property*
3. Fraud and Abuse *Provider, health groups, insurance plans, eligibility and coverage, contract, pharmaceutical, billing, reimbursement*
4. Criminal, civil, and administrative findings *Use of system for sexual harassment, defamation and other illegal or proscribed purposes or actions*
5. Downstream liability. *One party fails to secure its systems and they are used to attack other systems causing loss to third parties*
6. Repudiation *Denial that an event, action or agreement took place*
B. Indirect Value Significance
7. Unusual interest *Personal or command information that would be of unusual interest to employees and others*
8. Effect of disclosure on enterprise *Adverse effect on employee moral, loss of productivity, or embarrassment to the management or employees*
9. Loss of reputation *Loss of ability to carry out mission, impairment of mission, unauthorized disclosure*
C. Intelligence, Confidentiality, and Privacy Significance
10. Privacy considerations *Disclosure or misuse of private information. Information that is sensitive in nature to an individual or entity. Regulatory, criminal, and civil transgressions*
11. Regulatory intervention *Disclosure or misuse of information protected by regulation or a prime candidate for regulatory protection*
12. Harm to the Health System, Society, or Government *Disclosure of sensitive information of national value*

4.5.2. System Harms

In order to identify the impact of threats, it is necessary to examine the **various ways in which a system may be harmed, or the organization or healthcare mission may be harmed through the system**. The list of harms must address the various components of the system, including its data, software, hardware, network infrastructure, facility, and support organizations. The list of potential harms to or through health services systems has been summarized as follows:

Harm
a. Unauthorized disclosure of sensitive information
b. Unauthorized modification of integrity-critical information
c. Impeding the availability of system services.
d. Unauthorized use of system resources
e. Destruction of system hardware, software or data
f. Death or injury to personnel

4.6. Vulnerability Analysis Tables

Vulnerability analysis has the objective of **testing for conditions or weakness in, or the absence of, security procedures, technical controls, physical controls, or other controls that could be exploited by a threat**. System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system.

Security management, physical facilities, personnel, procedures, the use of commercial or in-house services (such as networking services), and contingency planning are examples of areas that affect the security of the entire system, but may have been specified outside of the systems development or acquisition cycle [5]. Follows a listing of

types of tests recommendations for ongoing **vulnerability and security assessments**:

Vulnerability Testing		
Test	**Strengths**	**Weaknesses**
Network Mapping (using port scanner)	- Fast - Efficiently scans a large number of hosts - Excellent freeware tools available - Highly automated - Low cost	- Does not directly identify known vulnerabilities - Generally used as prelude to other testing - Requires significant expertise to interpret results
Vulnerability testing (using vulnerability scanner)	- Fairly fast - Efficiently scans large number of hosts - Some freeware tools available - Highly automated - Identifies known vulnerabilities from data base - Often provides advice on mitigating vulnerabilities discovered - High cost (commercial scanners) to low (freeware) - Easy to run on regular basis	- High false positive rate - Generates large amount of network traffic - Not stealthy – easily detected - Can be dangerous in the hands of a novice - Can miss latest vulnerabilities - Identifies only surface vulnerabilities
Penetration (attack) testing	- Tests networks and hosts using methodologies that hacker use - Verifies vulnerabilities - Goes beyond surface vulnerabilities (show how interaction of surface vulnerabilities can be used to gain greater access) - Demonstrates reality of vulnerabilities (as opposed to theoretical) - Provides the realism and evidence needed to addressed security issues - Can test the human as well as the technical elements of security	- Requires great expertise - Labor intensive - Slow - Dangerous when done by inexperienced testers - Certain tools may be banned by host organization - Expensive - Can be disruptive - Legal requirements

Security Testing and Evaluation	- Does not have to be invasive or risky - Includes policies and procedures - Generally requires less security expertise - Addresses physical security	- Does not verify vulnerabilities - Generally, does not identify newly discovered vulnerabilities - Labor intensive - Expensive
Password cracking	- Quickly identifies weak passwords - Provides clear demonstration of password strength or weakness - Easily implemented - Low cost	- Potential for abuse - Certain organizations restrict use - Needs the full processing resources of a powerful computer
Log reviews	- Provides excellent information - Only data source that provides historical information	- Cumbersome to review - Automated tools available are not perfect and filter out important information
File integrity checkers	- Reliable method for determining if a host has been compromised - Highly automated - Low cost	- Does not detect any compromise prior to installation - Checksums have to be updated whenever a change is made to the system
Virus detectors	- Excellent at detecting and repairing viruses - Low/medium cost	- Requires constant updates to be effective - Server based versions may have significant impact on performance - False positive issues - Ability to react to new, fast replicating viruses is often limited
Dialing attack	- Effective way to identify unauthorized modems	- Legal and regulatory issues especially if using public switched networks - Slow

The following table depicts **testing intervals** that may be tailored to fit system requirements as necessary.

Testing Intervals					
Test	**Cat 1[(a)]**	**Cat 2[(b)]**	**Complexity**	**Level of effort**	**Risk**
Network mapping	Quarterly	Annually	Medium	Medium	Medium
Vulnerability testing	Quarterly or bi-monthly	Annually	High	High	Medium
Penetration testing	Annually	Annually	High	High	High
Security Testing and Evaluation	Every three years or significant changes	Every three years	High	High	High
Password cracking	Monthly	Yearly	Low	Low	Low
Log Reviews	Weekly	Weekly	Medium	Medium	Low
File integrity checkers	Monthly/incident	Monthly	Low	Low	Low
Virus detectors	Continually	Continually	Low	Low	Low
Dialing attack	Annually	Annually	Low	Low	Medium

(a) Category 1 systems are those sensitive systems that provide security for the organization or other important functions: Firewalls, routers, perimeter defense systems such as intrusion detection; public access systems such as WEB and e-mail servers; DNS and directory servers; other internal systems that would be likely targets of intruders.

(b) Category 2 systems are all other systems and components.

4.7. Safeguards

Legal and policy issues are confronting law enforcement agencies and the Internet community - providers and users alike as societies attempt to strike the right balance among the legitimate needs of enforcement, consumer protection and privacy, and obligations imposed on Internet Service Providers (ISP). The basic starting point for any discussion on cybercrime legislation is the need for a **harmonized legal approach** to prevent a patchwork of laws that will make a hash of the global Internet.

Legal safeguards are very important. Existing statutes and precedence from common law can act as a deterrent to attackers and therefore can be considered a safeguard. Regulations have been enacted in many countries that support information assurance, data protection, and privacy. Legal safeguards are only effective if a firm policy of prosecution exists and an effective incident response plan is in place to protect forensic evidence in support of prosecution. Also, certain **data protection rights** accrue to those who use computer systems and one who violates these rights may be subject to civil and perhaps criminal proceedings. These rights can include protection against intellectual property violations, copyright, and defamation of character, sexual harassment, and invasion of privacy. An extensive review of the regulatory and legal aspects of person identifiable data protection was published by the Pan American Health Organization [6].

Categories of safeguards include the **control of personnel** that has access to the system, **mechanisms to ensure integrity, authentication, confidentiality of data**, and the establishment of an **audit trail** throughout the data capture, processing, and utilization workflow. There are technical and cost issues associated with legislative measures and the state of existing technology is such that the oft-desired surveillance of ISP traffic will not be substantially effective.

Among the problems related to the fight against cybercrime, cyberterrorism, and cyberwarfare the issue of **interception of communications** has been identified as one of the most complex.

Generic Safeguard Categories		
Security Services	**Example**	**Threat addressed**
Access Control Ensuring that only authorized personnel are granted rights, attributes, and permissions associated with the request.	- Assigning rights and privileges to an account user - Ensuring that sensitive equipment and terminals are in a physically secure location	- Unauthorized access to system capabilities - Unauthorized access to sensitive hardware and peripherals
Identification and authentication Establishing the claimed identity of a user	- User ID and password	- Unauthorized access to network - Unauthorized access to system
Data integrity Ensuring that the data has not been modified, added, or deleted during its transit or entry, and that it is complete, whole, and valid	- Performing a checksum operation - Periodically comparing attributes of critical files to original footprints - Digital signature for updates or changes to critical files - Protection of audit files	- Modifying, adding or deleting
Data Confidentiality Ensuring the protection and non-disclosure of sensitive data	- Encrypting sensitive data - Use of digital signature - Proper notice on data - Proper disclaimers - Rights and privileges - Policy	- Unauthorized access to sensitive data - Interception of data - Inappropriate use of data (such as Web publishing)
Non-repudiation Providing the integrity and origin of data in an un-forgeable relationship that is verifiable by an independent third party. Proof of delivery	- Public Key Cryptography - Digital notary - Digital signature	- Denial that an order was entered or changed
Audit Ensuring the existence of adequate audit trails for all system user activity Audit trails must also confirm the integrity of the audit capability itself	- Audit logging of all access to system and data - Appropriate review schedule for all audit files	- Lack of forensics in prosecution - Lack of data for security analysis - Undetected incidents

Traditional interception capabilities were developed to apply to the opening of letters and tapping of telephones. With the diffusion of telecommunications and particularly the **Internet**, which is designed and implemented with a layered architecture of protocols, depending on the desired information, **successful interception may require capture and interpretation of multiple layers of protocol**.

Except when close to the source or sink of traffic, the flows in the network are dynamically routed so that the **interception must occur close to either source or destination to have a chance of capturing all that might be of interest**. Interception in the middle of the network is unlikely to produce the desired result. Furthermore, **there are substantial differences between the interception of stored e-mail and the interception of communications in raw data streams**. Although interception of incoming e-mail that is stored and forwarded by an ISP is straightforward assuming that the email service computer is accessible, senders can easily falsify return addresses and it is frequently impossible to prove who sent the e-mail. Apart from the technical uncertainties associated with Internet surveillance, the cost burden of complex search and seizure requirements could put smaller ISPs at substantial financial risk as they would also additionally incur the opportunity cost of having to divert resources and technical expertise from further development and improvement of services. Nationally developed standards for interception of communications have not proven to be satisfactory in today's global communications environment.

Due process for end users and immunity for intermediaries that follow the instructions of law enforcement is another complicated matter and the protection of industry and fundamental human rights are uniquely linked in this instance. **Service providers** have a stake in assisting law enforcement to keep the Internet a secure place to conduct business. However, without the pertinent detail and authority of a clear court order, Internet **users** would be subjected to surveillance of their communications based upon varying levels of substantiation, further eroding consumer confidence in the Internet. Network data reveals more than the conceptual equivalent of a telephone number and, without the detail and authority of a court order, service providers would expose themselves to potential liability for the results of interception requests, whether legitimate or not. It is for this

reason that policy makers in the U.S. have taken particular care to debate the quality and specificity of substantiation necessary for an intercept order in an Internet environment. The conflict with privacy principles is onerous, the stakes high, and the debate on the many facets of the topic continues, despite a concerted effort last year by U.S. law enforcement agencies to apply surveillance tools to the Internet [7].

5. Integrated Management of Risk

In addition to cyberspace security issues that must be addressed by healthcare organizations and supporting agencies new information technology continues to be a risky proposition. The size of the risk, which can run into the tens of millions of dollars for new systems or into hundreds of millions for potential disruption to the organization or to its customers, calls for aggressive and systematic risk management to ensure success. **Risk management must be seen as a comprehensive undertaking that goes beyond just security risk and must be directed to the integrated handling of four major risk categories**:

- **Security risk** - will systems and information be secure?
- **Technical risk** - will the system work?)
- **Organizational risk** - will the organization use the system?
- **Business risk** - will the system produce desired results?

Unfortunately, integrated risk management is a tall order for many of today's organizations that focus on technical issue resolution alone while leaving security, organizational, and business risks to chance. Today's message is very clear -- plan to **assess and mitigate all four kinds of risks effectively as moving ahead without managing all risks is a certain recipe for organizational disruption and even disaster**.

Documented failures of large system implementations rarely point to a single cause. Too often the mentioned causes go beyond what we might call technical glitches to problems with botched training, excessive resistance to change, lack of user interest and support, failures to communicate, etc. The failure record clearly calls for

proactive formal risk management programs that integrate all types of risks mitigation efforts.

5.1. Managing Security Risks

Security risks and threats to information, information technology systems and networks, and to physical facilities critical infrastructure must be thoroughly and aggressively assessed and managed to assure (Information Assurance) they are not damaged or compromised from internal or external sources in any manner. Other sections of this document deal specifically with security information assurance and assessment of risk.

5.2. Managing Technical Risks

Companies and technical vendors have been doing high quality technical risk management for a couple of decades. But most of the risks that have been managed are related to the technical risks of project implementation. Technical risk is associated with the critical questions – **will the system work, will it work on time, and will it come in on budget?** This kind of technical risk, while occasionally mismanaged, is usually handled quite well by a combination of the organization's or outsourced information systems professionals and the vendors. The primary approaches for mitigating technical risk fall into three general categories:

- **Development of a sound project** - that will focus on the delivery of the technical system only. The scope of the project should be minimized to ensure technical delivery.

- **Rigorous project management** - must be done to ensure that the technical delivery of the system comes in on target, on time, and on budget.

- **Use of systematic processes to keep users informed and in the loop** - organizations must understand where technical

- implementation is at all times so that they can adequately prepare to use the new system

5.3. Managing Organizational Risks

By organizational risk, we mean the chance the organization will not fully use the new system. Failure to use the new system could be caused by a number of factors – one of the most common and deadly being workforce resistance. The primary approach to mitigating organizational risk is the systematic and comprehensive use of **change management** to ensure that the organization will be positioned to use the new system after technical installation.

Change management is the body of knowledge that is used to ensure that a complex change, like that associated with a large or complex system, gets the right results, in the right timeframe, at the right costs. Change management is, therefore, a disciplined approach applied to the organizational units that will operate the new systems to ensure their acceptance and readiness to use the new system effectively. The primary approaches for mitigating organizational risk fall into three general categories:

- **User preparation by rigorous project management** - that will ensure that user organizations have done all their required groundwork to adjust business processes as necessary to align with the technical system soon to be delivered.

- **Comprehensive communication to all employees** - covering the business objectives of the new systems, the reason for change to the new systems, including answer to the question “what’s in it for me”, and the vision for the organization using the new system.

- **Performance management system** – the user organization will need to be altered to include a performance management mechanism to monitor role

- and job descriptions that require the use of the new system.

5.4. Managing Business Risks

By business risk, we mean the possibility that the costly-to-implement system will not pay off in terms of "dollars and sense" results for the implementing organization. Failure to gain a business outcome can result from number of factors -- one of the most commonly found factors of failure is lack of alignment between imbedded processes and the organization's business objectives and priorities. The primary approaches for mitigating Business Risk fall into three general categories:

- **System selection** - must be done so that the system selected has not only the integrating efficiencies needed by the company but has the imbedded processes that the organization will be able to use to get results over the long term in their specific business environment.

- **Business process documentation** - must be done so that the overall work of the organization as it uses the new system is logical, understandable, and doable by the workforce.

- **User training** - so that the users will not only be able to operate the new system but will be able to use it rationally.

5.5. Security and Data Protection: A Collaborative Endeavor

In the U.S., cooperation between the federal government, universities, and private industries, recognized as vital, have addressed cyberspace security concerns [8]. Many government and private healthcare agencies have been leaders in the field of **data protection and systems security regulation** including the United States

Department of Health and Human Services (USDHHS) and the Healthcare Financing Administration (HCFA).

The National Security Agency (NSA), the National Information Assurance Partnership (NIAP), the Federal Emergency Management Agency (FEMA), the Department of Justice (DoJ), the Defense Information Systems Agency (DISA), the Department of Defense (DoD), the Department of Veterans Affairs (VA), and the Department of Health and Human Services (HHS) are just some of the U.S. public and private sector agencies that have worked to develop and implement extensive guidance and requirements related to insuring the **protection, security, and privacy of healthcare information, information technology (hardware and software) and critical infrastructures**.

Guidelines and requirements have been developed and promoted by such organizations as the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), the National Committee for Quality Assurance (NCQA), and many others. The National Institute of Standards and Technology (NIST) conducts **education** and **research** efforts, and is an agency that develops **security standards** for civilian agencies and publishes guidelines for federal agencies. The United States Department of Justice (DoJ) has established a **Computer Crime and Intellectual Property** Section (CCIPS) of the Criminal Division of the DoJ.

A key requirements program directed at insuring the **security of networks, systems, and data** is the Defense Information Technology Certification and Accreditation Program (DITSCAP) of the DoD. It provides all DoD agencies, including supporting healthcare organizations with guidance on:

- **General information security policies, procedures, and requirements** (personnel, systems, networks).
- **Risk/Threat Assessments** requirement for information (data), information technology, and critical infrastructure;
- **Documentation** requirements for a variety of prescribed security policies, plans (including Contingency and

Continuity of Operations plans), and architecture documents for systems and networks to insure establishment of common operating environments, standardization, security, and reliability;

- **Certification and Accreditation (C&A) testing** of databases, applications, systems, and networks prior to approval by a Designated Approval Authority (DAA) for provision of Certificates of Networthiness (CON) and Certificates to Operate (CTO);

- **Security Awareness Training** includes initial and recurring information security and privacy awareness training for all staff members; as well as patients to some degree as well.

The DoD DITSCAP guidance as part of the NSA Common Criteria for **information technology security guidance**, and the VA's ITSCAP security guidance, nearly identical in nature, have helped public sector healthcare providers increase security and privacy awareness, training, and capabilities toward achieving maximum security and privacy of medical information and technology possible.

Introduction of other new security technologies and requirements such as the **Public Key Infrastructure (PKI) encryption standards** has also started to significantly help further improve the security of healthcare systems, networks, and information in the public and private healthcare sectors as well; but is still new technology to many public and private sector organizations alike and will take time to be implemented.

6. International Organizations Work on Information Privacy and Security

Security and privacy of information stored in systems and shared across networks and systems are **of vital concerns for managers at all levels of organizations as well as individuals**. Because the use of information systems and networks and the entire information technology environment have changed dramatically in the last 20 to 30 years, there has been **greater emphasis on security by governments, businesses, other organizations and individual users, who develop, own, provide, and manage service and use information systems and networks**.

Many countries and multinational organizations such as the United Nations, the Organization for Economic Cooperation and Development (OECD), the Commission of Europe (COE) and the European Union (EU), the Committee of Europe (COE), and the Group of 8 (G8) have been addressing national and cross-border issues of information privacy, cyberspace security, cybercrime, and cyberterrorism.

6.1. Organization for Economic Cooperation and Development

The OECD has done extensive work related to the **security of information systems and networks** as well as **privacy of information**. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [9], adopted on 23 September 1980, continues to represent international consensus on general guidance concerning the collection and management of personal information. By setting out **core principles**, the Guidelines play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to cross-border data flows, both on and off line.

The publication reflects twenty-one years of expertise and experience shared among representatives of OECD governments, business and industry, and civil society and contains the **instruments that serve as the foundation for privacy protection at the global leve**l: the 1980 OECD Privacy Guidelines, the 1985 Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. In July 2002 the OECD published their Guidelines for the Security of Information Systems and Networks, which has a great deal of pertinent information for organizations to review and consider [3].

6.2. European Countries

The European Union **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995** [10] represents the **first comprehensive effort to implement an international harmonization privacy framework**. Data protection rules in the European Union not only regulate processing personal data in the EU Member States but also comprise provisions on the transfer of data to third countries (Articles 25 and 26 of the Directive 95/46/EC). The basic criterion is that Member States should permit transfer of personal data only when the third countries concerned ensure an appropriate level of protection. If an appropriate protection level cannot be ensured, and on the assumption that none of the exceptions envisaged would apply, Member States would prevent those transfers.

The Council of Europe is an intergovernmental organization formed in 1949 by West European countries. There are now 41 member countries. Its main role is "to strengthen democracy, human rights and the rule of law throughout its member states." Its description also notes that "it acts as a forum for examining a whole range of social problems, such as social exclusion, intolerance, the integration of migrants, the threat to private life posed by new technology, bioethical issues, terrorism, drug trafficking, and criminal activities." On September 8, 1995, the Council of Europe approved a recommendation to enhance law enforcement access to computers in member states. The **Recommendation of the Committee of Ministers to Member States**

Concerning Problems of Criminal Procedure Law Connected with Information states:

- Subject to legal privileges or protection, investigating authorities should have the power to order persons who have data in a computer system under their control to provide all necessary information to enable access to a computer system and the data therein.

- Criminal procedure law should ensure that a similar order can be given to other persons who have knowledge about the functioning of the computer system or measures applied to secure the data therein.

- Specific obligations should be imposed on operators of public and private networks that offer telecommunications services to the public to avail themselves of all necessary technical measures that enable the interception of telecommunications by the investigating authorities.

- Measures should be considered to minimize the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary.

The Council created a working group on cybercrime to draft a **convention on computer crime in 1997**. A number of nonmembers are also represented as observers to the ad-hoc group including the US, Canada, Japan, South Africa, the European Commission, the OESO, UNESCO and others. The Committee of Experts on Crime in Cyberspace of the Council of Europe released its "Draft Convention on Cyber-crime" on April 27, 2000, following more than three years of discussions. Since then, it has released **several revised versions and an explanatory memorandum** but little has changed in the text since the original draft [11]. The European Committee on Crime Problems (CDPC) of the COE approved the **Cybercrime Convention** in June 2001 and by the Council of Ministers in November 2001. It was opened for signature in November 2001 and has been signed by over 30 countries

The European Commission held important fora during the last years on the issues of computer crime and on the need for Internet Service Providers and other telecommunications companies to retain transactional information about users' activities [12, 13].

6.3. The Group of Eight Countries (G8)

The Group of 8 (G8) is made up of the heads of state of eight industrialized countries (US, UK, France, Germany, Italy, Japan, Canada, and Russia). The leaders have been meeting annually since 1975 to discuss issues of importance, including the information highway, crime and terrorism. Since 1995, the G8 has become increasing involved in the issue of cybercrime, and has created working groups and issued a series of communiqués from the leaders and actions plans from justice ministers. In addition, a special working group has also been working on the issues almost constantly for several years. The working group released **recommendations to combat transnational organized crime** efficiently. These included:

- States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized, and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention, and international cooperation in respect of such abuses are effectively addressed.

- Liaison between law enforcement and prosecution personnel of different States should be improved, including the sharing of experience in addressing these problems.

- States should promote study in this area and negotiate arrangements and agreements to address the problem of technological crime and investigation.

- Emphasize the relevance and effectiveness of techniques such as electronic surveillance, undercover operations and controlled deliveries.

- States must review domestic arrangements for those techniques and to facilitate international cooperation in these fields, taking full account of human rights implications

- States must exchange experiences on the area.

- Accelerate consultations, in appropriate bilateral or multilateral forum, on the use of encryption that allows, when necessary, lawful government access to data and communications in order to, *inter alia*, prevent or investigate acts of terrorism, while protecting the privacy of legitimate communications.

- Intensify exchange of operation information, especially as regards the use of communications technologies by terrorist groups.

At the G8 Summit of June 1997, the issue was raised up to the head of state level. The G8 issued a communiqué stating: "We must intensify our efforts to implement the **Lyon recommendations**. In the coming year we will focus on two areas of critical concern: first, the investigation, prosecution, and punishment of high-tech criminals, such as those tampering with computer and telecommunications technology, across national borders; second, a system to provide all governments the technical and legal capabilities to respond to high- tech crimes, regardless of where the criminals may be located". A separate "Foreign Ministers Progress Report" examined issues of high tech crime and recommended greater identification and tracking of users and restrictions on encryption. **The G8 countries have established a 24-hour network of law enforcement experts capable of responding swiftly to requests for help with investigations that cross international borders, including hacking cases**. The network, which is now in use, is open to wider membership and a number of non-G8 countries have already joined.

6.4. Diverging Interpretations

Although the EU countries and the U.S. share similar concerns about the impact of electronic networks on the information privacy, the EU has addressed these concerns in very different ways from the U.S. When the Transatlantic Business Dialogue (TABD) met in November 1997, both European and American participants recognized the **threats to global commerce posed by privacy regimes that require conformity to a certain approach**. It supported mutual recognition by governments of industry-led, market-driven privacy protection principles to ensure consumer trust in electronic commerce. It also suggested that national privacy protection allow for differences in privacy protection, based on national political systems and local cultures. The TABD urged the governments of both the U.S. and the EU to work together with industry to understand how market-driven, self-regulatory solutions provide protection of, and ensure the continuation of, cross-border personal data flows [14].

Following the lead of the EU, most countries in Latin America, New Zealand, Canada, and the Asia-Pacific region have chosen the legislative path, as opposed to self-regulation, the model sponsored by the U.S. and Japan. The **global trend has been toward the adoption of legislation type models** – Australia, which initially preferred a self-regulating approach, has backed away from self-regulation and is now adopting the legislative model [15]. Regardless of the regulatory model that is implemented, the goal is to ensure the development, agreement, and application of a fair and predictable set of rules across countries and regions, and to reduce the complications of jurisdiction and applicable law.

7. HIPAA Security Checklists: A Working Model for Systems Privacy and Security in Healthcare

The purpose of this section is to summarize very briefly some of the **requirements** that must be considered by anyone in the healthcare industry based upon the data collected and referenced by electronic information systems. In this section, we will examine a **model for privacy and security standards and electronic signature issues** as implemented by the United States Department of Health and Human Services (USDHHS) as part of the **Health Insurance Portability and Accountability Act of 1996, P.L. 104-91 (HIPAA)**.

7.1. Health Insurance Portability and Accountability Act (HIPAA) Security Summary

The United States Federal Law (P.L. 104-91) of 1996 was the **most sweeping legislation to affect the healthcare industry in the United States in over 30 years**, and it applies to many healthcare market players, not just health plans and insurance companies. HIPAA regulatory body has a broad scope and comprises access to healthcare, portability of administrative and clinical data, prevention of fraud and abuse, simplification of administrative procedures, data protection to ensure privacy of personal information, and taxation changes.

HIPAA portability provisions establish substantial limitations on “pre-existing condition exclusion” for the group and individual health insurance marketers and **establishes consumer protections to guarantee availability and renew ability of insurance and prevent discrimination based on health status**. The law establishes a new coordinated program to **combat fraud**, a Medicare Integrity Program which provides HCFA with greater flexibility to choose program safeguard contractors, an account to hold criminal and civil fines related to healthcare fraud, and a national healthcare fraud and abuse data collection program for reporting final adverse actions against providers and others.

Most importantly, besides emphasis on **data protection and privacy** HIPAA requires the secretary of the USDHHS to **adopt certain standards for information transactions, data elements for such transactions, and standards relating to security and performance of specific tasks**. Standards include the following:

- Unique Identifiers for providers, health plans, individuals and employers
- Transactions including: claims and encounters, claims attachments, enrollment and disenrollment, eligibility, healthcare payment and remittance advice, health plan premium payments, first report of injury, health claim status, referral certification and authorization, and coordination of benefits
- Code Sets
- Security
- Requires all health plans to be able to receive and send standard transactions electronically within 24 months after the standard is established (36 months for small plans)
- Requires all healthcare providers who elect to submit transactions electronically to use the standard format
- Establishes financial penalties for failure to comply with standards

7.2. HIPAA Details and Checklists

The following overview is a useful tool for any healthcare agency or provider for guidance related to privacy and security of information, transactions, information technology, and finances.

7.2.1. Security Components

Security refers to a **set of techniques or methods for implementing systems so that they protect rights and discharge responsibilities**. Security implements privacy and confidentiality policies. Security denotes the **procedures, techniques and technologies employed to protect information from accidental or malicious destruction, alteration or access**.

Under HIPAA Administrative Simplification, standards must be set for the security **of individual health information and electronic signature usage by health plans, healthcare clearinghouses and healthcare providers**. These entities must have security standards in place in order to comply with the law that requires healthcare information and individually identifiable healthcare information to be protected to ensure privacy and confidentiality when it is electronically stored, maintained or transmitted. There are four components of security:

- **Administrative procedures** are documented formal practices to manage the selection and execution of security measures to protect data, and the conduct of personnel in relation to the protection of data.

- **Physical safeguards** relate to the protection of physical computer systems related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. This also covers use of locks, keys, and administrative measures used to control access to computer systems and facilities.

- **Technical security services** include the processes that are put in place to protect, control, and monitor information access.

- **Technical security mechanisms** include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

7.2.2. Requirements for Implementation of Systems Security

Administrative Procedures

- **Certification** - evaluate computer systems/network designs either internally or externally to certify that appropriate security is in place.

- **Chain of Trust Partner Agreement** - if a third party is concerned; there should be a contract between the parties to agree to electronically exchange data and to protect the transmitted data. Multiple two-party contracts maybe involved in moving information from the originating party to the ultimate receiving party.

- **Contingency Plan** - for responding to emergencies within the system with all of the following requirements: applications and data criticality analysis, a data backup plan, a disaster recovery plan, an emergency mode operation plan, and testing and revision procedures.

- **Formal Mechanism for Processing Records** - documented policies and procedures for routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of health information.

- **Information Access Control** - establish and maintain formal, documented policies and procedures for granting different levels of access including: authorization, establishment, and modification policies and procedures.

- **Internal Audit** - ongoing internal audit process of system activity (i.e. logins, file accesses, security incidents).

- **Personnel Security** - authorization through appropriate clearances and meeting the following conditions: assure supervision of personnel performing technical systems maintenance activities by authorized, knowledgeable persons; maintain access authorization records; insure

that operating and maintenance personnel have proper access; employ personnel clearance procedures; employ personnel security policy/procedures; ensure that system users, including technical maintenance personnel, are trained in system security.

- **Security Configuration Management** - implement measures, practices and procedures for security of information systems, coordinated and integrated with other system configuration management practices for system in integrity. Requires: documentation; hardware/software installation and maintenance; review and testing for security features; inventory procedures; security testing; and virus checking.

- **Security Incident Procedures** - formal, documented instructions for reporting security breaches including report procedures and response procedures.

- **Security Management Process** - creating, administering and overseeing policies to ensure the prevention, detection, containment and correction of security breaches. This is a formal process that includes: risk analysis, risk management, a sanction policy and a security policy.

- **Termination Procedures** - formal, documented instructions, including appropriate security measures for the ending of an employee's employment or an internal/external user's access. This would include the following mandatory features: changing combination locks, removal from access lists, removal of user accounts, turn in of keys, tokens or cards that allow access.

- **Training** - for all staff regarding the vulnerabilities of the health information in an entity's possession and procedures to be followed. This would include: awareness training for all personnel, including management, periodic

security reminders, user education concerning virus protection, user education in importance of monitoring login success/failure, how to report discrepancies and user education in password management.

Physical Safeguards

- **Assigned Security Responsibility** - assigned to a specific individual or organization and documented with the following responsibilities: management and supervision of the use of security measures to protect data and the management and supervision of the conduct of personnel in relation to the protection of data.

- **Media Controls** - formal, documented policies and procedures that govern the receipt and removal of hardware/software (i.e. diskettes, tapes) into and out of the facility. These controls would include: controlled access to media; accountability (tracking mechanism); data backup; data storage; and disposal.

- **Physical Access Controls** - formal, documented policies limiting access. These controls would include: disaster recovery; emergency mode operation; equipment control (into and out of site); a facility security plan; procedures for verifying access authorizations prior to physical access; maintenance records; need-to-know procedures for personnel access; sign-in for visitors and escorts; testing and revision.

- **Policy/Guideline on Workstation Use** - documented instructions and procedures such as logging off before leaving a terminal unattended.

- **Secure Workstation Location** - physical safeguards in place to eliminate or minimize the possibility of unauthorized access. For instance, locating a terminal used to access sensitive information in a restricted-access locked room or not placing a terminal used to

access patient information in any area where unauthorized persons can view the screen contents.

- **Security Awareness Training** - for all employees, agents and contractors to understand their security responsibilities and make it part of their daily activities.

Technical Security Services to Guard Data Integrity, Confidentiality and Availability

- **Access Control** - restrict access to resources. Types of access control include mandatory access control, discretionary access control, time-of-day, classification and subject-object separation. The following must be implemented: procedure for emergency access, and at least one of the following-context-based, role-based or user-based access. Encryption is optional.

- **Audit Controls** - to record and examine system activity.

- **Authorization Control** - mechanism for obtaining consent for the use and disclosure of health information. Either of the following may be used: role-based access or user-based access.

- **Data Authentication** - provide corroboration that data in an organization's possession has not been altered or destroyed in an unauthorized manner.

- **Entity Authentication** - corroboration that an entity is what it claims to be using the following features: automatic log off; unique user identification and at least one of the following-biometrics identification system, password system, personal identification number (PIN), telephone callback or token system which uses a physical device for user identification.

Technical Security Mechanism to Guard Against Unauthorized Access to Data Transmitted Over a Communications Network

- **Communication/Network Controls** - if communications or networking is employed, the following implementation features must be implemented: **integrity controls** and **message authentication**. In addition, one of the following implementation features must be implemented: **access controls** or **encryption**. Additionally, if an organization is using a network, the following four implementation features must be implemented: **alarm, audit trail, entity authentication and event reporting**.

- **Electronic Signatures (Digital Signatures)** - the following three implementation features must be implemented: **message integrity, non-repudiation and user authentication**. Other features are optional: **ability to add attributes, continuity of signature capability, countersignatures capability, independent verifiability, interoperability, multiple signatures and transportability**.

7.3. Digital Signatures

Digital signature is a mean to **guarantee the authenticity of a set of input data** the same way a written signature verifies the authenticity of a paper document. It is implemented through a cryptographic transformation of data that allows a recipient of the data to **prove the source and integrity of the data and protect against forgery**.

Digital signatures are a core function of Public Key Infrastructure (PKI). To sign a document, the document and private key are entered to a cryptographic process that outputs a bit string or the signature. To verify a signature, the signature and public key is entered into a cryptographic process, which returns an indication of success or failure (integrity).

In the health sector, the goal is to ensure that healthcare information remains secure as risk factors increase and there has been continuing growth for data security measures to ensure that healthcare information is secured in an appropriate manner. Currently there are no transactions mandated by HIPAA that require electronic signatures. However, other standards still need to be proposed by the USDHHS, with suggestions that the claims segment may be a transaction that will require electronic signatures. Digital signatures are the only type of electronic signature that is being proposed in the regulation because it "provides the combination of authenticity, message integrity and non-repudiation which is viewed as a desirable complement to the security standards required by the law."

7.4. HIPAA Transactions Overview

A transaction can be defined as an **action that is carried out to perform a key function of business**. In healthcare, examples of transactions could he a health claim, the action to enroll an individual in a health plan, the action required to define eligibility of that individual in a health plan, or the payment for healthcare services rendered. In HIPAA, transactions obey the following rules:

- Applies to all health plans, all healthcare clearinghouses, healthcare providers, and associated intermediaries that transmit any of the covered administrative health information in electronic form. This is true of all the administrative simplification provisions.

- The health plan may not refuse to conduct the transaction as a standardized transaction.

- The health plan may not delay the transaction or otherwise adversely affect, or attempt to adversely affect, the person or the transaction on the basis that the transaction is a standard transaction.

- The health information transmitted and received in connection with the transaction must be in the form of standard data elements of health information.

- A health plan that conducts transactions through an agent must assure that the agent meets all the requirements of this part that apply to the health plan.

7.5. HIPPAA Project Planning and Assessment Tools

7.5.1. Areas to be Considered

Topics	Further Detail
▪ Assess existing resources versus required resources for operation of HIPAA ▪ Resolve if resources exist internally or if there is a need to outsource ▪ Establish HIPAA Program Office Within organization ▪ Appoint single responsible Project Manager for operating HIPAA with reporting line to Operations Officer ▪ Appoint Security Officer to coordinate security requirements ▪ Appoint multidisciplinary team to form HIPAA compliance team ▪ Establish budget for operation ▪ Establish compliance strategy	*Resource needs:* 1. Project Management 2. Technically skilled individuals 3. Executive sponsorship of project who has influence over all affected areas 4. Enterprise coordination and communication 5. Involvement of end-users 6. Financial support to meet demands of regulations *Considerations for hiring outside assistance:* 1. Participation in standard- developing organizations 2. Understanding of the healthcare industry and the flow of information 3. Familiarity of security measures in HIPAA and security vendors 4. Determine relationships with trading partners to ensure buy-in of partners

7.5.2. HIPAA Considerations for an Organization

Area	Considerations	Further Detail
(1) **HIPAA Awareness**	▪ Assess and plan communication awareness requirements ▪ Develop and plan a HIPAA awareness communication plan ▪ Conduct an awareness program to promote organizational involvement ▪ Monitor communication efforts for effectiveness ▪ Review brochures and promotion items as to how HIPM is mentioned in literature	*Communication considerations:* ▪ Clear, consistent message ▪ Communicate multiple times ▪ Communicate in various mediums
(2) **Education**	▪ Identify key audiences for education ▪ Determine level of knowledge of staff about HIPAA ▪ Determine communication mechanisms and tools to educate (seminars, toolkits etc.) ▪ Assess if trading partners should be included in education efforts ▪ Prepare for and conduct education sessions ▪ Obtain commitment and appoint accountable leader ▪ Develop tests to measure effectiveness of education	*Education considerations*: 1. Gather information compiled and available about HIPAA 2. Research web sites with HIPM information

Area	Considerations	Further Detail
(3) **Trading Partners**	▪ Review contracts to assess responsibilities for HIPAA compliance with partners ▪ Communicate HIPAA compliance responsibilities to partners in writing ▪ Assess trading partner readiness for HIPAA ▪ Ask specific questions about HIPAA that will ascertain the trading partners knowledge about HIPAA ▪ Consider partners viability for future business, and evaluate relationships ▪ If considering mergers or acquisitions, consider HIPAA readiness with interested parties. ▪ Consider implementation coordination with multiple partners ▪ Consider contract negotiation timing with implementation	*Relevant documents to gather for review:* ▪ License/development agreements for software or databases ▪ Partner contracts ▪ Customer contracts ▪ Maintenance and support agreements ▪ Manuals, brochures, promotional materials *Key areas of focus in contracts:* ▪ Warranties ▪ Specific HIPAA provisions ▪ Indemnification and limitation of liability ▪ Remedies ▪ Term and termination ▪ Requirements with respect to submission of electronic ▪ Performance incentives of penalties ▪ Confidentiality or security provisions
(4) **System Considerations (Vendors)**	▪ Assess vendor's readiness for HIPAA ▪ Ask specific questions about HIPAA that will ascertain the vendors knowledge about HIPAA ▪ Debate conversion vs. replacement of systems ▪ If decide on conversion, determine how vendors will comply with HIPAA and timeline to do so ▪ Negotiate HIPAA warranties into contracts with vendors ▪ Renew computer services agreements ▪ Review maintenance and support agreements	*Questions to ask vendors:* **1.** Question the vendor's strategy for complying with the HIPAA security requirements **2.** Discuss how the product(s) handles audits and access control **3.** Question the vendor's organizations and their participation in HIPAA NPRMs, education seminars, etc.

Area	Considerations	Further Detail
(5) **Code Sets**	▪ Assess current state of business ▪ If local codes are used, determine if national code now exists, number of claims submitted with codes, and decide to nationalize or not. Determine how business practices will have to be altered once local codes are eliminated. (Even if you petition for a national code, it could take a long time) ▪ Determine impact of potential length changes for code sets ▪ Determine impact of migration from J codes to NDCs ▪ Determine impact of converting historical data	▪ Impacts to consider when changing code set lengths: Files, Databases, Reports, and Screens ▪ Impacts of migration from J codes: Files, Databases, Pricing, Edits, and Audits ▪ Impacts to consider of converting historical data: Audits, Data Warehouse, and Fraud and Abuse detection
(6) **Unique Identifiers**	▪ Determine current state of business and what type of identifiers are being utilized ▪ Determine impact of potential alphanumeric provider identification number ▪ Determine impact of potential length changes for identifiers ▪ Determine impact of converting historical data ▪ Determine impact of possibly maintaining dual systems ▪ Determine whether to build a permanent crosswalk or perform a conversion	▪ Impacts of changing to alphanumeric ID: Edits, Audits, Voice response systems, Screens, Reports, Files, and Databases ▪ Impacts of changing length of identifiers: Files, Databases, Reports, and Screens ▪ Impacts of converting historical data: Audits, Data Warehousing, and Fraud and Abuse detection
(7) **Contingency Planning**	▪ Perform risk and business impact assessment ▪ Develop contingency plan for each high-risk, high impact area ▪ Test and monitor contingency plans ▪ Create plans to maintain contingency plan	*Assessment steps:* ▪ Identify mission-critical business processes ▪ Identify business and consumer obligations ▪ Review facilities and data centers ▪ Develop project plan for development of contingency plan

Area	Considerations	Further Detail
(8) **Security Awareness and Education Program**	▪ Define the relationship among the people, the program's responsibilities and the protection of the organization's assets ▪ Plan an awareness program as this will serve for the foundation of the information security program	*Seven steps in awareness program:* ▪ To start an Information Security Program in an organization the first step is to establish a strategic plan for the desired goals and perform a needs determination ▪ Program definition should include vulnerability and risk identification ▪ Program analysis should include assessment of current awareness level, requirements and resource definition ▪ Program implementation includes kick off, incorporation of the program and personnel training ▪ Program monitoring will assess the results and suggest improvements that should be made
(9) **Security Assessment**	▪ Review security organization and job descriptions ▪ Determine if resources exits internally to conduct security assessment or if outside resources will be required ▪ Determine level of expertise if utilizing inside resources ▪ Set up time frames to complete assessment ▪ Compare legal and regulatory requirements vs. existing security ▪ Compare EDI and business strategies with technology capabilities as it relates to security	*Full security assessment could include:* ▪ Security policy review ▪ Physical security review ▪ Desktop security review ▪ Security administrative processes review ▪ Applications review ▪ Business continuity review ▪ Network security review ▪ Network assessment with best-practices benchmarking review

Area	Considerations	Further Detail
(10) **Security Policy**	▪ Define the scope of the security policy ▪ Review existing security policies if they exist ▪ Develop security policy one does not exist	*What might be included in a security policy?* ▪ Purpose of the document ▪ Primary points of contract ▪ Change logs or documentation of the policy's history ▪ Security policy requirement's scope of boundaries ▪ Policy requirements, such as: ▪ Organizational information making policy ▪ Organizational network making policy ▪ Host-security control requirements ▪ Network-control requirements ▪ Network-control requirements ▪ Alarm requirements ▪ Accountability and responsibility identification ▪ Password use ▪ System access ▪ Computer viruses ▪ Alteration/correction ▪ Faxed information ▪ Spoken information ▪ Clinical research and quality assurance ▪ Breach of confidentiality ▪ Patient rights *Many resources already exist:* ▪ AHIMA: "Security and Access: Guidelines for Managing Electronic Patient Information" ▪ CPRI: Security Toolkit ▪ Faulkner & Gray: The 200 Guide to Health Data Security ▪ For the Record: Protecting Electronic Health Information

Area	Considerations	Further Detail
(11) **Physical Security Review**	Review policies and procedures related to physical security and safety	*Typical areas to review* ▪ Perimeter review ▪ Parking and lighting review ▪ Review of police reports for crime rate in vicinity to establish physical threats or risk factor ▪ Physical security of desktop ▪ Physical security administration review ▪ Security awareness review ▪ Contingency plan review as it relates to physical facilities ▪ Physical intrusion detection: Alarm-point door, Motion detectors, Physical alarms
(12) **Security** Applications	▪ Review identification, authentication and access-control parameters ▪ Review mechanisms in place to control identification, access and authentication ▪ Conduct product review of various vendors ▪ Ensure that applications relate to overall business strategy ▪ Develop an enterprise vision (most likely have to be phased in to complete vision) rather than point product solution	*Questions to ask vendors:* ▪ Question the vendor's strategy for comp8lying with the HIPAA security requirements ▪ Discuss how the product(s) handles audits and access control ▪ Question the vendor's organizations and their participation in HIPAA, NPRMs, education seminars, etc.
(13) **Business Continuity**	▪ Determine if formal policy in place, if one exists ▪ Review to determine if current ▪ If one does not exist, determine if it will be done internally or externally ▪ Develop a task force from all operational areas to develop contingency plan for organization ▪ Test contingency plan at least once a year	*Considerations of business continuity plan:* ▪ Off-site storage ▪ Key contracts for emergency plan ▪ Alternatives for physical facilities to run mission-critical functions

7.5.3. HIPAA Standards for Transaction and Code Sets

Requirement	Details
Applicability	▪ HIPPA requirements for standard transactions and code sets apply to all health plans, healthcare code sets apply to all providers who choose to submit electronic transactions ▪ Electronic transmissions include magnetic tape, disk or CD, Internet, extranet, leased lines, dial-up or CD, Internet, extranet, leased lines, dial-up lines and private networks. ▪ Telephone voice response and “faxback” systems would not be included.
Health Claims and Encounters	▪ Retail Drug: NCPDP Telecommunication Version 3.2 or equivalent NCPDP Batch Standard Version 1.0 ▪ Dental Claim: ASC X12N 837 version 4010 ▪ Professional Claim: ASC X12N 837 version 4010 ▪ Institutional Claim: ASC X12N 837 version 4010
Healthcare Payments and Remittance Advice	▪ Healthcare Payment/Advice ASC X12N 835 version 4010
Coordination of Benefits	▪ Retail Drug: NCPDP Telecommunication Version 3.2 or equivalent NCPDP Batch Standard Version 1.0 ▪ Dental Claim: ASC X12N 837 version 4010 ▪ Professional Claim: ASC X12N 837 version 4010 ▪ Institutional Claim: ASC X12N 837 version 4010
Health Claim	▪ Healthcare Claim Status Request and Response ASC X12N 276/277 version 4010
Enrollment and Disenrollment in a Health Plan	▪ Benefit Enrollment and Maintenance ASC X12N 834 version 4010
Health Plan Premium Payments	▪ Payment Order/Remittance Advice ASC X12N 820 version 4010
Referral Certification and Authorization	▪ Healthcare Services Review-Request for Review and Response ASC X12N 2789 version 4010
First Report of Injury	▪ Not yet proposed
Health Claims Attachments	▪ 275/277 ▪ Hl7-Derivative of ORU

Requirement	Details
Health Plans (requirement for all transactions listed above)	Health plans may accept only the specified standards for electronic health transaction.
Healthcare Clearinghouses Healthcare Providers	Each healthcare clearinghouse must use the specified standards electronic health transactions.
Compliance Testing ▪ ***Level 1- Developmental Testing*** ▪ ***Level 2- Validation Testing*** ▪ ***Level 3- Production Testing***	▪ Developmental Testing-This is done by the standards setting organization during the development process. ▪ Validation Testing-This tests a sample transactions to see whether they are being written correctly. It is expected that private industry will provide commercial testing at this level. ▪ Production Testing- these tests a transaction from a sender through the receiver's system.
Code Sets ***Diseases, injuries, impairments, other health related problems and their manifestations*** ***Causes of injury, disease, impairment or other health-related problem*** ***Actions taken to prevent, diagnose, treat or manage disease, injuries, and impairments and any substances, equipment, supplies or other items used to perform these actions.***	 ICD-9-CM (International Classification of Diseases, Ninth Revision, Clinical Modification), versions 1 and 2 ICD-9-CM CPT (Physicians' Current Procedural Terminology) CDT (Current Dental Terminology) NDC (National Drug Codes) HCPCS (Healthcare Procedure Coding System)

7.5.4. Security and Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability

Requirement	Details
Certification	Not Implemented
Chain of Trust Partner Agreement	Not Implemented
Contingency Plan	*All Listed features must be implemented:* ▪ Applications and data criticality analysis ▪ Data backup plan ▪ Disaster recovery plan ▪ Emergency mode operation plan ▪ Testing and revision
Information Access Control	*All listed features must be implemented:* ▪ Access authorization policies and procedures ▪ Access establishment policies and procedures ▪ Access modification policies and procedures
Personnel Security	*All listed features must be implemented:* ▪ Assure supervision of maintenance personnel by authorized knowledgeable person ▪ Maintenance of record of access authorization ▪ Operating, and in some cases, maintenance personnel have proper access authorization ▪ Personnel clearance procedure ▪ System users, including maintenance personnel, trained in security
Security Configuration Management	*All listed features must be implemented:* ▪ Documentation ▪ Hardware/software installation and maintenance review and testing for security features ▪ Inventory ▪ Security testing ▪ Virus checking
Security Incident Procedures	*All listed features must be implemented:* ▪ Report procedures ▪ Response procedures

Requirement	Details
Security Management Process	*All listed features must be implemented:* ▪ Risk analysis ▪ Risk management ▪ Sanction policy ▪ Security policy
Termination Procedures	*All listed features must be implemented:* ▪ Combination locks changed ▪ Removal from access lists ▪ Removal of user account(s) ▪ Turn in keys, token or cards that allow access
Training	*All listed features must be implemented:* ▪ Awareness training for all personnel (including management) ▪ Periodic security reminders ▪ User education concerning virus protection ▪ User education in importance of monitoring log in success/failure, and how to report discrepancies ▪ User education in password management
Assigned Security Responsibility	Not Implemented
Media Controls	*All listed features must be implemented:* ▪ Access control ▪ Accountability (tracking mechanism) ▪ Data Backup ▪ Data Storage ▪ Disposal
Physical Access Controls	*All listed features must be implemented:* ▪ Disaster recovery ▪ Emergency mode operation ▪ Equipment control (into and out of site) ▪ Facility security plan ▪ Procedures for verifying access authorizations prior to physical access ▪ Maintenance records ▪ Need to know procedures for personnel access ▪ Sign-in for visitors and escort, in appropriate ▪ Testing and revision

7.5.5. Technical Security Services to Guard Data Integrity, Confidentiality, and Availability

Access Control	Details
Access Control	*The listed feature must be implemented:* ▪ Procedures for emergency accesses *At least one listed feature must be implemented:* ▪ Context-based access ▪ Role-based access ▪ User-based access *Optional:* ▪ Encryption
Audit Controls	Not Implemented
Authorization Control	*At least <u>one</u> listed feature must be implemented:* ▪ Role-based access ▪ User-based access
Data Authentication	Not Implemented
Entity Authentication	*All listed features must be implemented:* ▪ Automatic logoff ▪ Unique user identification *At least <u>one</u> listed feature must be implemented:* ▪ Biometrics ▪ Password ▪ PIN ▪ Telephone call back ▪ Token

7.5.6. Technical Security Mechanisms to Guard Against Unauthorized Access to Data Transmitted Over a Communications Network

Requirement	Details
Communications/ Network Controls	*If communications or networking is employees, the following implementation features must be implemented:* ▪ Integrity controls ▪ Message authentication *At least <u>one</u> listed feature must be implemented:* ▪ Access controls ▪ Encryption *If using a network, the following features must be implemented:* ▪ Alarm ▪ Audit trail ▪ Entity authentication ▪ Event reporting

7.5.7. Electronic Signature

Requirement	Details
Digital Signature	*If digital signature is employed, the following features must be implemented:* ▪ Message integrity ▪ Non-repudiation ▪ User authentication *Optional:* ▪ Ability to add attributes ▪ Continuity of signature capability ▪ Countersignatures ▪ Independent verifiability ▪ Interoperability ▪ Multiple signatures ▪ Transportability

References

[1] Carr C (2003). *The Lessons of Terror: A History of Warfare Against Civilians.* Random House Trade Paperback, New York, ISBN 0 375 76074 1

[2] Evolvent Technologies (2002). *White Paper: Information Assurance Core Competencies.* Falls Church VA, April

[3] Organization for Economic Cooperation and Development (2002). *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Recommendation of the OECD Council adopted at its 1037th Session on 25 July 2002

[4] Markoff MG (2002). *Remarks to the Committee on Hemispheric Security of the Organization of the American States on Deccember 2, 2003*. Washington DC

[5] National Institute of Standards and Technology (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems*. NIST Technology Administration, U.S. Department of Commerce

[6] Rodrigues RJ, Wilson P, Schanz SJ (2001). *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-Identifiable Health Databases.* Pan American Health Organization, Washington DC. ISBN 92 75 12385

[7] Cerf VG (2001). *Cybercrime*. Keynote address at the OECD Cybersecurity Workshop: Information Security in a Networked World. Hotel Nikko, Tokyo, Japan, September 12, 2001

[8] U.S.Government (2003) .*The National Strategy to Secure Cyberspace*. The White House, February 2003. Available online at: http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

[9] Organization for Economic Cooperation and Development (1980). *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*. Adopted by the Council 23 September 1980. Available online at: http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/priv.htm or http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

[10] European Union (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*.

[11] Council of Europe (2001). *Draft Convention on Cyber-crime and Explanatory Memorandum Related Thereto*. Final Activity Report of the European Committee on Crime Problems (CDPC). Prepared by the Committee of Experts on Crime in Cyber-Space (PC-CY). Available online at: http://www.privacyinternational.org/issues/cybercrime/coe/cybercrime-final.html

[12] European Commission (2000). *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime.* Communication of the European Commission, 26 January 2001, COM(2000) 890. Available online at: http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm

[13] European Commission (2001). *EU Working Paper. Online Discussion on Data Retention*. PI submission to the Committee. Available online at: http://cybercrime-forum.jrc.it/default/page.gx/_app.page/entity.html/_app.action/entity/_entity.object/KM------0000000000000583/_entity.name/Data-Retention-Working-Paper-Final.pdf

[14] Wellbery BS, Wolfe CC (1997). *Privacy in the Information Age*. Office of Service Industries, U.S. Department of Commerce, Washington DC

[15] de Graaf G (2001). *European Data Privacy: 21st Century Challenges of Transatlantic Policy Cooperation in Electronic Commerce*. In Transatlantic Regulatory Harmonization and Global Standards, The George Washington University School of Business and Public Management, Washington DC, Januray 2001

Web Sites

Accredited Standards Committee (ASC) X 12
http://www.x12.org

Data Interchange Standards Association-Test conditions and results from when the workgroups test transactions proposed for HIPAA
http://www.disa.org

Department of Health and Human Services-HIPAA Administrative Simplification information
http://aspe.os.dhhs.gov/admnsimp

Electronic Healthcare Network Accreditation Commission (EHNAC)
http://www.ehnac.org

Healthcare Financing Administration-National Provider Identifier and Payer ID
http://www.hcfa.gov/hcfainit.htm

National Committee on Vital and Health Statistic's Report
http://www.ncvhs.hhs.gov

National Council or Prescription Drug Programs (NCPDP) Standards, Implementation Guides and Data Dictionaries
http://www.ncpdp.org/hipaa.htm

National Uniform Claim Committee-Data content used in standardized messaging format to transit data electronically for non-institutional claim and encounter information
http://www/nucc/org

Washington Publishing Company-X12N Implementation Guides for EDI
http://www.wpc-edi.com/hipaa/