一個人データに対するファイアウォールの設置
パーソナル情報研究会「医療情報を受託管理する情報処理事業者向けガイドライン」

経済産業省「ソフトウエア等脆弱性関連情報取扱基準」
経済産業省「情報システム安全対策基準」
経済産業省「ソフトウエア管理ガイドライン」
経済産業省「コンピュータ不正アクセス対策基準」
経済産業省「コンピュータウイルス対策基準」
経済産業省「個人情報の保護に関する法律についての経済産業分野を対象としたガイドライン」
経済産業省「クラウドサービスの利用のための情報セキュリティマネジメントガイドライン（案）」

総務省「安心して無線LANを利用するために」
総務省「ASP・SaaS における情報セキュリティ対策ガイドライン」
総務省「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」

情報セキュリティ政策会議「重要インフラにおける情報セキュリティ確保に係わる「安全基準等」策定にあたっての指針」

JIS Q 27001:2006　情報セキュリティマネジメントシステム一要求事項
JIS Q 27002:2006　情報セキュリティマネジメントの実践のための規範
JIS Q 15001:2006　個人情報保護マネジメントシステム一要求事項

(財)日本情報処理開発協会「JISQ15001:2006 をベースにした個人情報保護マネジメントシステム実践のためのガイドライン」

(財)医療情報システム開発センター「保健医療福祉分野のプライバシーマーク認定指針」

―　関連する要求事項　―

3.4.3.2 安全管理措置 c. 最低限のガイドライン ⑤より

個人情報を取り扱うシステムとインターネットは，物理的分離を原則とする。しかし物理的分離が困難な場合は，業務上の必要性を明確にし（責任者の承認を含む），少なくとも以下のすべての対応を実施すること（**個人情報を取り扱うシステムとブラウザ等のインターネットアプリケーションを同一端末上で稼動できないことが原則**）。

1) リスク分析を実施し，リスクに対する対策の実施と残存リスクを把握

2) ファイアーウォール等による外部からの脅威への対策

3) L3 スイッチ等による内部からの漏出脅威への対策

4) 不適切な運用の抑止及び追跡のためアクセスログの記録・解析（誰が，いつ，誰の情報に，どのようなアクセスをしたか等の詳細な情報を記録し，定期的な記録の確認を行う）を定期的又はリアルタイムで実施し，異常なアクセスがあったときは警告を発生し，ネットワークを切断する機能等を付加する

5) 論理的分離ポリシー及び機器のパラメータ設定を記録し，担当者が変わってもポリシーが維持されることを担保する

２．調査項目

２-（３）事例の調査

医療機関等の設置端末からインターネットに接続している事例を調査する。

－　調査対象　－

- 九州大学医学部附属病院
  - ①　検査部
  - ②　第３内科
  - ③　放射線部

－　調査期間　－

2011年2月25日

－　調査事項　－

Q1	レセプト件数：月約何件
Q2	レセコン：あり／なし
Q3	電子カルテ：あり／なし
Q4	診療端末とメールやホームページを閲覧するインターネット端末：別々／同じ／インターネット端末なし
Q5	普段の診療におけるインターネット上の情報の必要性：必要／あれば便利／必要ない
Q6	普段の診療におけるインターネット上の情報の必要性について『**必要**』または『**あれば便利**』とお答え頂いた方にお聞きします。 **診療の際に必要またはあれば便利なインターネット上の情報**にはどのようなものがありますか？（例えば，医療機能評価機構のMINDS（診療ガイドラインデータベース），医薬品医療機器総合機構の添付文書情報等，医薬品医療機器総合機構（PMDA）のホームページ，厚生労働省の緊急安全性情報，患者の勤め先に関する情報など）
Q7	診療端末とメールやホームページを閲覧するインターネット端末について『**別々**』とお答え頂いた方にお聞きします。 **診療端末を直接インターネットに接続する場合にセキュリティ面などのリスクや投資など心配されていること**はありますか？
Q8	診療端末とメールやホームページを閲覧するインターネット端末について『**インターネット端末がない**』とお答え頂いた方にお聞きします。 **診療を行う上で，インターネットを利用できないために不便だと思われる点や利用できたら便利だと思う点**があればご記入ください。

― 調査結果 ―

● 診療の際に必要またはあれば便利なインターネット上の情報

- **副作用情報**や **EBM** などを確認する。ガイドラインが新しくなったりするし，自分の専門外のことだとすべて覚えていられない。
- この患者はこの検査にはこの薬は使えないなど，**薬に関する情報**を調べる。
- **略語**などを調べる。略語など診療科によって違ったりするので，インターネットだとそのような略語の検索もできる。
- **医療機関の電話番号**や**医師名**を調べる。一般歯科医から週に5，6件単位で検査依頼をよく受ける。依頼をしてくる歯科は数十件ある。この依頼状や紹介状が手書きなどの場合もあり，紹介元さえも不明な場合がある。
- **文献**を検索する。
- NCBI（**遺伝子の配列**）や**アミノ酸の配列**などを調べる。
- **学会やメーカーの主催するセミナー**などを調べる。HP 等で情報収集しないとわからない場合がある。

● 診療を行う上で，インターネットを利用できないために不便だと思われる点や利用できたら便利だと思う点

- 副作用情報や EBM などの確認ができないので紙面で持ち歩いている。
- 患者の紹介で，照会先の病院や医師の名前が分からない場合に困った。病院名はわかるが連絡先がわからない，先生の名前はわかるが病院名や連絡先など調べられないことがあり，困った。現在は調べられるようになったが，以前は検索もできずに，あきらめたりしたので診療に生かすことができなかった。
- 検査結果については紙で渡すことができるので問題はない。ただ，画像の印刷ができないので，患者さんに，説明のために病気の症例などから画像を印刷して渡したりすることができない。診療端末がインターネットにつながっていればいいのにとたまに思う。

● 診療端末を直接インターネットに接続する場合に心配される事項（セキュリティ面などのリスクや投資など）

- 情報リテラシーが低い場合は内部からインターネットを通じて患者さんの情報や個人情報などがもれたりするのが不安。内部から外部に漏れることのほうが外部からの攻撃よりはるかに怖い。メールでうっかり個人情報を流したりすることが怖い。外からの攻撃も心配。
- ウイルスソフトのウイルス定義ファイルを，せめて週に 1 度更新したい。

●その他

－ メールの利用について －

- 外注検査の会社とのやりとりにメールは一切利用しない。フロッピーなどの外部媒体を利用している。１枚に収まらない場合，CDやDVDの利用も考えている。他の大学病院ではMOを利用していた。
- 部内や病院内の連絡や情報伝達にはアクティブメールを利用している。診療端末でもインターネット端末でも同じように見ることができる。また，科内は週に１回ミーティングをおこなう。週１で技術部会のミーティング（各科から各１名技術部員）や２週に１回システム委員会（各科？２名）で通達は行われる。
- 業務連絡については，３内科の中ではメールのやり取りが多い。ほかの科とはPHSなどで済ませたり，受診願いなどで連絡している。電子カルテの中で書く場合も多い。
- 放射線部に技師が６３名いて，業務連絡などメールを利用している。掲示板を見るように！と言っても人数が多いので周知が難しく，メールは大体みな１日に１度チェックをしているのみ。当日の用事はだいたいPHSを利用して連絡する。それ以外の急用でなければメールで連絡している。どこでも確実に伝達できるし見ることができるため。

－ セキュリティ事故について －

- USBフラッシュメモリによる情報の持ち出し，紛失？があった。それをきっかけに規則で持ち出しを禁止し，USBフラッシュメモリも各科で管理しているのでそれ以後は一切ない。

－ セキュリティ教育について －

- 数年前から，九大病院に勤務する時には個人情報に関しての誓約書を書かされる（個人情報に関する取り扱い等の書類を全て読んで問題なければサインする）。これらによって，少しは個人情報の保護や守秘義務に関して意識の喚起になっていると思う。ただ，サインしたことでさえ何も感じない人間も中にはいると思う。部内でもセキュリティに関して注意などはあるが特に規則などはない。
- 情報セキュリティに関しての教育などは病院がやるべきだとは思うが，大学病院のように大きな規模だと管理が行き渡らないので結局は各部や科で教育や管理を行うべきだと思う。

2．調査項目

2-（4）洗い出された課題，脅威への適切な対処の検討

現在の規制に対応し，かつ，インターネット上の最新の脅威に対抗するため，効率的かつ効果的な対処策について検討する。

― 効率的かつ効果的な対処策 ―

＜マネジメント系＞

- 年間活動計画の策定
- 定期的（少なくとも年１回）及び業務着任時の教育実施
- 定期的（少なくとも年２回以上）及び脅威認知時の点検実施
- 定期的（少なくとも年１回）及び必要時の監査実施

＜技術系＞

- ネットワークセキュリティポリシーの策定と実装
  - ➢ 利用者の識別及び認証
  - ➢ 情報の区分管理とアクセス権限の管理
  - ➢ アクセスログの取得と定期的又はリアルタイムのチェック
  - ➢ 不正ソフトウェア対策
    - ✧ ウイルスパターンファイルの定期的及びタイムリーな更新
    - ✧ 修正プログラムのタイムリーな適用
    - ✧ ソフトウェアの脆弱性対応（タイムリーはバージョンアップなど）
  - ➢ ネットワーク上からの不正アクセス
    - ✧ ファイアウォールの設置とその的確な設定及びログの取得とその定期的又はリアルタイムのチェック
  - ➢ 情報及び情報機器（USB フラッシュメモリなどの可搬媒体含む）の持ち出し及び持ち込みの管理
  - ➢ メール誤送信対策
    - ✧ 宛先二重チェック
    - ✧ メール添付ファイルの暗号化

資料２

Time	Title	Name
8:30 - 8:45	International collaboration - strategic focus of the University of Applied Sciences	Prof. Dr. Andreas Frey Director of International Collaboration
8:45 - 9:45	eHealth activities in Japan	Prof. Dr. Ryuichi Yamamoto Tokyo University President JAMI
9:45 - 10:15	Coffee break	
10:15 - 10:45	eHealth activities in Germany	Prof. Dr. Ursula Hübner Health Informatics Research Group
10:45 - 11:00	eHealth in nursing - the HL7 eNursing Summary	Dipl.-Kfm. Daniel Flemming Health Informatics Research Group
11:00 - 11:15	Integrated (electronic) care in Germany and Austria - a comparison	Nicole Egbert, MA Health Informatics Research Group
11:15 - 11:45	Secure networks for internal and external information exchange in hospitals	Ass. Prof. Katsuya Tanaka Tokyo University
11:45 - 14:00	Lunch break	
14:00 - 14:15	Japanese - German cooperation: economic importance and challenges	Burkhard Weller Toyota Germany
14:15 - 15:15	eHealth activities in Japan	Prof. Dr. Ryuichi Yamamoto Tokyo University President JAMI
15:15 - 15:45	Secure networks for internal and external information exchange in hospitals	Ass. Prof. Katsuya Tanaka Tokyo University
15:45 - 16:00	Coffee break	
16:00 - 16:30	Medical informatics and eHealth in Germany	Prof. Dr. Alfred Winter University of Leipzig
16:30 - 16:45	Characteristics of innovative hospitals - empirical results	Jan-David Liebe, MA Health Informatics Research Group
16:45 - 17:00	Data mining methods in nursing	Dr. Björn Sellemann Health Informatics Research Group
17:00 - 17:15	Final discussion	

Morning lectures - Business Information Management students (BIM3/5) and Health Management students (MIG3)
Afternoon lectures - Health Management students (MIG1)

Guests: Prof. Takahashi, Waseda University Tokyo guest professor University of Applied Sciences Osnabrück, Mrs. Grünanger, International Office, Dr. Holtkamp, Technology Transfer

資料３

e-Health in Japan
EHR strategy and Security guidelines in Japan

Ryuichi Yamamoto, M.D., PhD
Interfaculty Initiative In Information Studies,
the University of Tokyo
Japan Association for Medical Informatics

Japan Association for Medical Informatics

Total number of members: 2700
8 regional branches
Division for training and educating health information technologists
Division for nursing informatics
Division for standardization
Division for researching policy and national strategy
9 special research working groups
Autumn annual congress. (over 2500 attendants)
Spring symposium (over 1000 attendants)

Brief History of Healthcare ICT in JAPAN

1970s Computerized financial systems
1980s Order Entry systems
1990s Electronic Medical Record systems
Just started to developing experimental systems
1999 Government determined requirements for paperless EMR.
2001 Government made "Grand Design for Healthcare ICT in Japan"
2006 Government made "New IT Reform Strategy"
2009 i-Japan 2015 – Power Shift (LDP to DP)
2010 A New Strategy in Information and Communications Technology

Requirements for Paperless EMR
Ministry of Health and Welfare, 1999

3 Major requirements
- Integrity and Responsibility of EMR data
- Readability of EMR data
- Keep these for legally required period

Privacy protection

With suitable technology and operation

Grand Design for Healthcare ICT

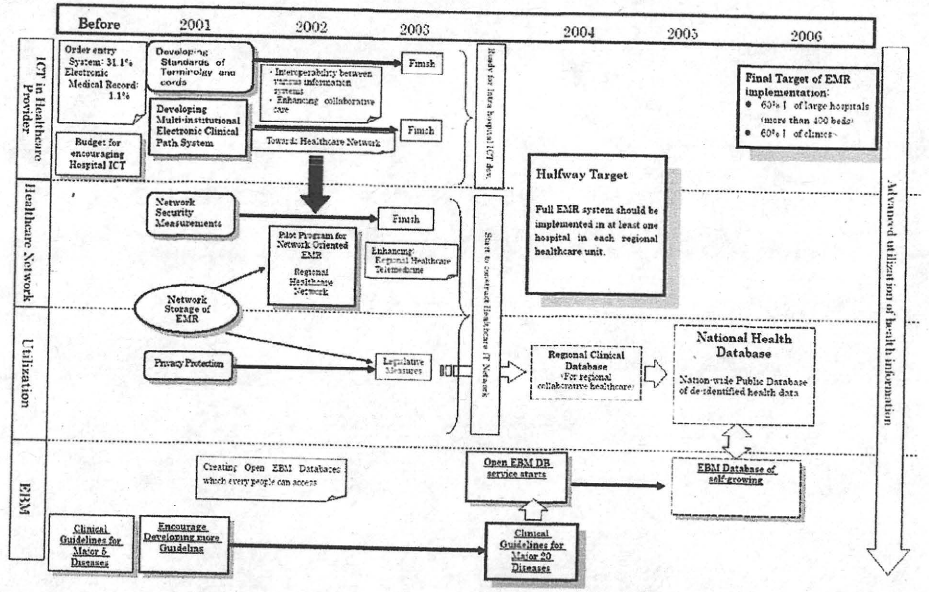
EMR

In 2006, 60% of all medical institutions shall implement the EMR systems.

Electronic Insurance Claim (Not Online)

In 2006, 70% of all hospitals shall implement the electronic insurance systems

Healthcare ICT Action Plan (2001)



Before | 2001 | 2002 | 2003 | 2004 | 2005 | 2006

ICT in Healthcare Provider

Order entry System: 31.1%
Electronic Medical Record: 1.1%

Budget for encouraging Hospital ICT

Developing Standards of Terminology and cords

Developing Multi-institutional Electronic Clinical Path System

- Interoperability between various information systems
- Enhancing collaborative care

Toward: Healthcare Network

Finish

Finish

Ready for Intra hospital ICT dev.

Healthcare Network

Network Security Measurements

Finish

Pilot Program for Network Oriented EMR

Regional Healthcare Network

Enhancing: Regional Healthcare Telemedicine

Network Storage of EMR

Start to construct Healthcare IT Network

Utilization

Privacy Protection

Legislative Measures

Regional Clinical Database (For regional collaborative healthcare)

National Health Database

Nation-wide Public Database of de-identified health data

EBM

Creating Open EBM Databases which every people can access

Clinical Guidelines for Major 5 Diseases

Encourage Developing more Guidelins

Clinical Guidelines for Major 20 Diseases

Open EBM DB service starts

EBM Database of self-growing

Halfway Target

Full EMR system should be implemented in at least one hospital in each regional healthcare unit.

Final Target of EMR implementation:

- 60% [of large hospitals (more than 400 beds)
- 60% [of clinics

Advanced utilization of health information

Electronic Documents Act for Private Sector (2005)

Legal base for e-commerce

Based on Digital Signature Act (2004)

In Healthcare field, mere replacement of 1999 requirements for paperless EMR.

New IT Reform Strategy (2006)

Realizing Ubiquitous and Universal Network Society Where Everyone Can Enjoy the Benefits of IT

1. Structural reform of healthcare through IT
2. An environmentally-friendly society that utilizes IT
3. The world's leading safe and secure society
4. The world's safest road traffic environment
5. The world's most convenient and efficient e-Government
6. Enhanced business competitiveness through establishment of management by utilizing IT
7. Prosperous lifestyle throughout people's lifetime

Action Plan 2006 (Health field)

Make New Grand Design for Healthcare ITC

MHLW announced first draft and emphasizing constructing Japanese EHR

Common Infrastructure

Healthcare PKI ,Secure Network, and Healthcare smart card

ITC Based Healthcare Network

Regional and inter-regional healthcare network

Gathering nation-wide heath data (EHR) and analysis.

Developing healthcare terminology and ontology

Full Online Handling of Insurance Claims

i-Japan Strategy 2015 Striving to Create a Citizen-Driven, Reassuring & Vibrant Digital Society

Vision of Japan in 2015

● Create a society in which digital technologies will be accepted like air and water, create a condition of digital inclusion throughout the economy and society, enrich lives and connections among people

● Digital technology and information will lead to digital innovation and new vitality throughout the economy and society where individuals and society as a whole can use this vitality to undertake spontaneous creation and innovation that generate new value

Perspectives for Achieving the Future Vision

● Make the strategy for a digital society in which human-centric digital technologies are as easy to use as water and air and are accepted universally by citizens

● A digital strategy from four new perspectives:
- Easy to use digital technologies
- Breaking down the barriers that hinder the use of digital technologies
- Ensuring security when using digital technologies
- Creating a new Japan by diffusing digital technologies and information throughout the economy and society

Main Aspects of the Strategy

Electronic Government and Local Government

● Create structures to implement electronic government (appoint government CIOs, etc.), follow up on prior plans and establish PDCA structures

● Broadly expand the National e-PO Box* (tentative name) to provide one-stop administrative services and make government more transparent

* National e-PO Box are to be established by fiscal year 2013 and considered integration with the Social Security Number & Card (tentative name) to facilitate the use of existing systems; the basic concept is to be adopted this fiscal year.

Three Major Fields

Healthcare and Health

● Address issues including shortages of doctors in rural areas
- Use telemedicine technologies
- Maintain and enhance skills of doctors and others
- Implement cooperation among regional healthcare facilities

● Implement Japanese EHR* (tentative name)
- Reduce medical errors and provide continuous treatment throughout individuals' lives
- Use electronic prescriptions and drug dispensing information
- Use anonymous health-related information for epidemiological purposes

* Electronic Health Records

Education and Human Resources

● Encourage the use of digital technologies in classrooms and raise children's desire to learn, academic abilities and ability to use information
- Raise the teaching abilities of teachers using digital technologies
- Establish easy-to-understand classes that use digital equipment such as electronic blackboards

● Develop highly-skilled digital human resources stably and continuously
- Broadly establish and improve practical educational bases
- Improve and expand national center functions through collaboration among industry, academia, and government

Revitalizing Industry and Local Communities and Nurturing New Industries

Use digital technologies and information to transform structures in all industries and revitalize local communities and enhance the international competitiveness of Japanese industries.
- Develop business foundations for small and medium businesses
- Promote green IT and ITS
- Establish new business types in local industry
- Increase the number of teleworkers (double teleworkers who work from home)
- Create new creative markets

Development of Digital Infrastructure

Support advances in the use of digital technologies in all fields and promote growth
- Establish broadband infrastructure (in excess of 100 Mbps for mobile and 1 Gbps for fixed)
- Establish information security countermeasures
- Promote development of digital fundamental technologies
- Develop infrastructure for distribution and utilization of digital information

Issues That Require Further Investigation

•Priority Inspection of Regulations, Systems, Practices, etc.: Drastic reviews of regulations, systems, and practices that hinder the use of digital technologies and information will be performed and an initial priority inspection will be conducted in 2009. Based on the results, the government will take necessary measures and continue implementation in the future.

•Adoption of the Digital Global Vision (tentative name): The Digital Global Vision will be adopted by the end of fiscal 2009 concerning reinforcement of the international competitiveness of Japan's digital technologies and related industries.

Three Major Fields

Healthcare and Health

● Address issues including shortages of doctors in rural areas
- Use telemedicine technologies
- Maintain and enhance skills of doctors and others
- Implement cooperation among regional healthcare facilities

● Implement Japanese EHR* (tentative name)
- Reduce medical errors and provide continuous treatment throughout individuals' lives
- Use electronic prescriptions and drug dispensing information
- Use anonymous health-related information for epidemiological purposes

* Electronic Health Records

A New Strategy in Information and Communications Technology (May 2010

1. Delivering a citizen-oriented electronic administration

   Initiating a citizen identification (ID) system

2. Recreating bonding in local communities

   A national-level information service shall be created to allow the citizens to electronically manage and utilize their own medical and health-related information in order to create an environment where the citizens may receive medical care based on their medical records anywhere in the country and undertake their own health management. As the first step toward this end we shall create a mechanism enabling individuals to electronically manage their own medication and other information. We shall also create a mechanism wherein anonymized medical insurance claims are listed in databases so that they may be utilized in the process of standardizing and improving the efficiency and quality of services related to medical care.

3. Creating new markets and expanding internationally

Recreating bonding in local communities

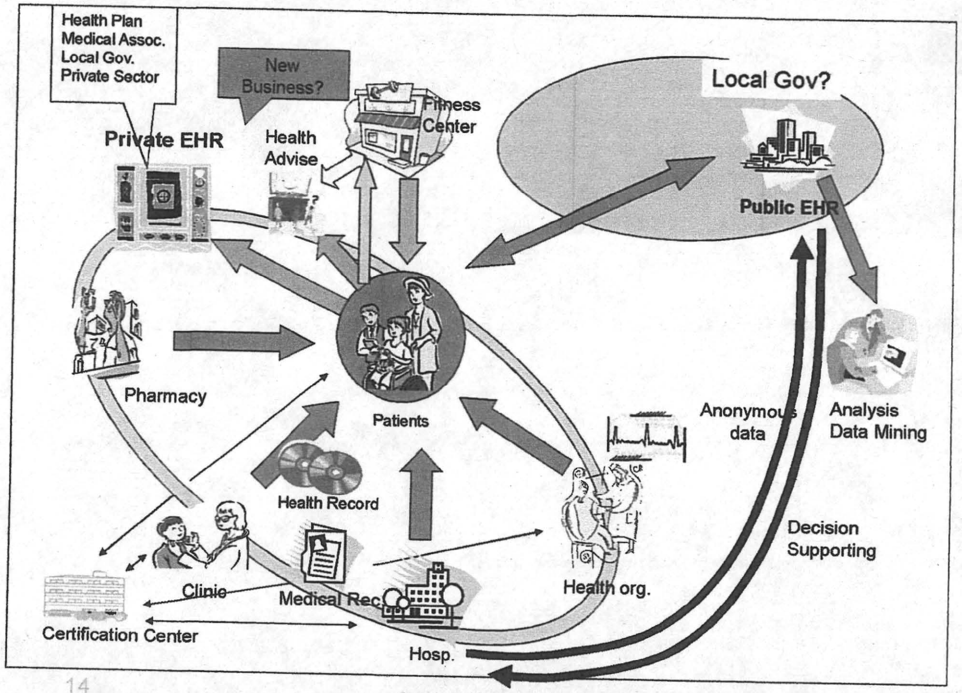
"My Hospital Everywhere"
(Japan's Personal Health Record service)

Seamless community-collaborated medical services
(Advanced Healthcare information network)

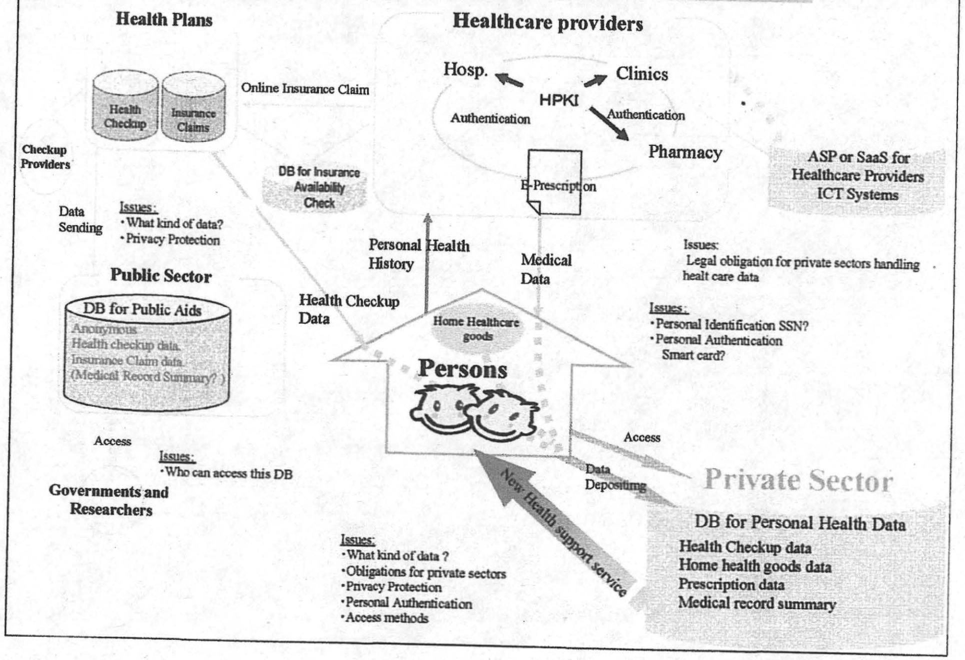
Planning for efficient medical services using medical insurance claim data and others
(National medical insurance and health checkup DB)

Promoting pharmaceutical safety through the use of medical information database
(Large scale medical information DB)

Advancing in-home medical, care, watching, and other services for the aged



Project for EHR of MHLW, METI and MIC



Issues:
- What kind of data?
- Privacy Protection

DB for Public Aids
Anonymous
Health checkup data,
Insurance Claim data,
(Medical Record Summary?)

Issues:
Legal obligation for private sectors handling healt care data

Issues:
- Personal Identification SSN?
- Personal Authentication
Smart card?

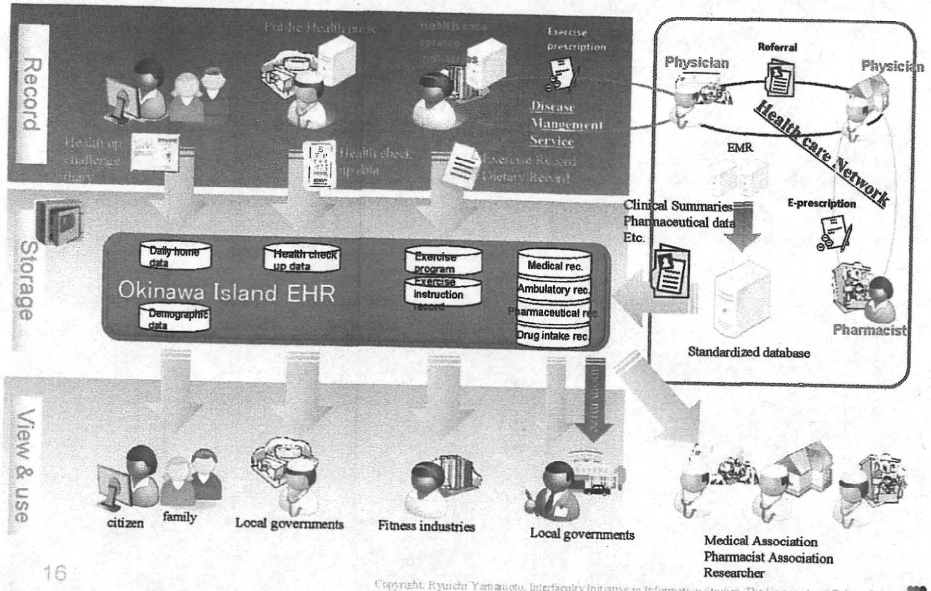
Issues:
- Who can access this DB

Issues:
- What kind of data ?
- Obligations for private sectors
- Privacy Protection
- Personal Authentication
- Access methods

DB for Personal Health Data
Health Checkup data
Home health goods data
Prescription data
Medical record summary

3 Ministries EHR Project in Okinawa Island 2007 - 2010

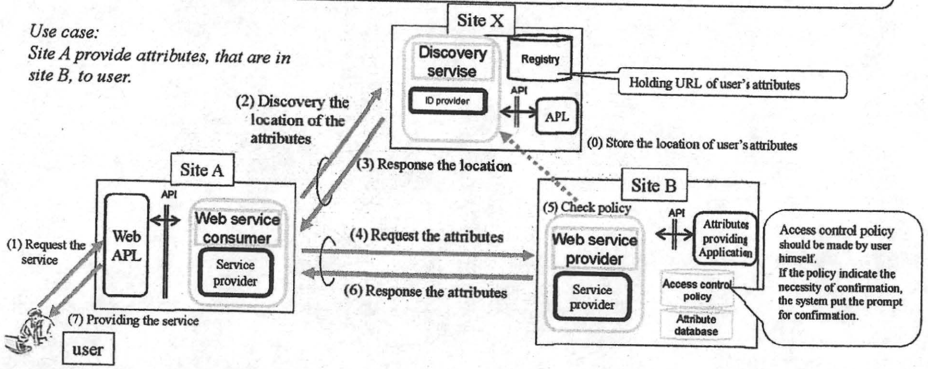
厚生労働省 経済産業省 総務省 MIC 浦添市



Infrastructure of EHR in Okinawa Island (SAML2.0 and ID-WSF2.0)

Discovery service of attributes, Request and response of the attributes under user's consent, Policy-based access control, Group management

Use case:
Site A provide attributes, that are in site B, to user.


Site X
Discovery servise
ID provider
Registry
API
APL
Holding URL of user's attributes
(0) Store the location of user's attributes
(2) Discovery the location of the attributes
(3) Response the location
Site A
Web APL
API
Web service consumer
Service provider
(1) Request the service
(7) Providing the service
user
(4) Request the attributes
(6) Response the attributes
Site B
(5) Check policy
Web service provider
Service provider
API
Attributes providing Application
Access control policy
Attribute database
Access control policy should be made by user himself.
If the policy indicate the necessity of confirmation, the system put the prompt for confirmation.

SAML 2.0

- Unification of user ID of different sites
- Enabling single sign on

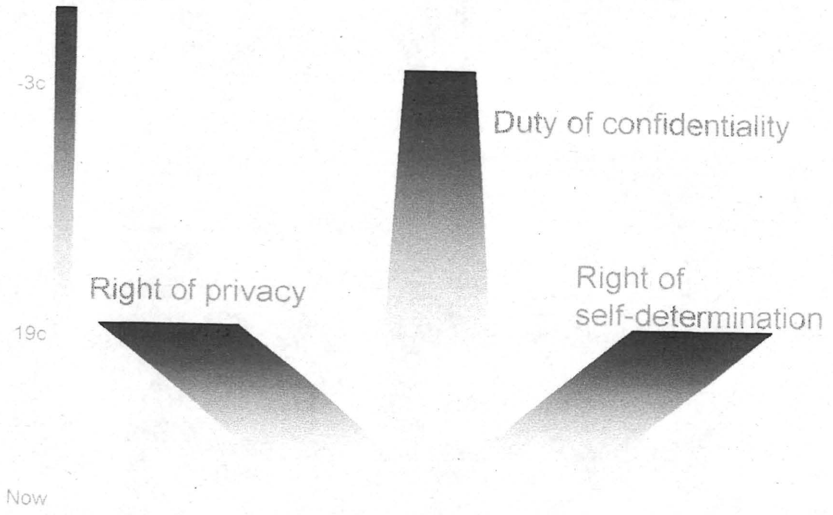
ID provider	Providing the assertion based on user authentication
Service provider	Check the assertion and authenticate the user

ID-WSF2.0

- allow the move of attributes among different sites

Discovery service	Provide the location of each attribute
Web service provider	Provide the attributes
Web service consumer	Get the attributes from other site and provide them to user

Act on the Protection of Personal Information, 2005



Act on the Protection of Personal Information, 2005

Chapter 1. General Provisions (Articles 1 to 3)

Chapter 2. Responsibilities of the State and Local Public Bodies, etc. (Articles 4 to 6)

Chapter 3. Measures for the Protection of Personal Information, etc.

Section 1. Basic Policy on the Protection of Personal Information (Article 7)

Section 2. Measures of the State (Articles 8 to 10)

Section 3. Measures of Local Public Bodies (Articles 11 to 13)

Section 4. Cooperation between the State and Local Public Bodies (Article 14)

Chapter 4. Duties of Entities Handling Personal Information, etc.

Section 1. Duties of Entities Handling Personal Information (Articles 15 to 36)

Section 2. Promotion of the Protection of Personal Information by Private Institutions (Articles 37 to 49)

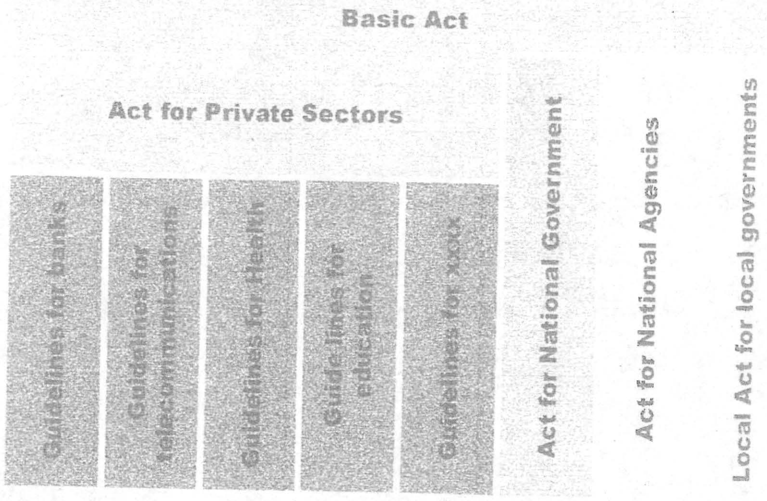
Chapter 5. Miscellaneous Provisions (Articles 50 to 55)

Chapter 6. Penal Provisions (Articles 56 to 59)

Supplementary Provisions

3 2

Acts and Guidelines for privacy protection in Japan - Hard and soft law -


Basic Act

Act for Private Sectors

Guidelines for banks

Guidelines for telecommunications

Guidelines for Health

Guide lines for education

Guidelines for xxxx

Act for National Government

Act for National Agencies

Local Act for local governments

Security Guidelines for Health Information Systems

Version 1 MHLW 2005 - 10 Chapters and 3 Appendices, over 100 pages

1. Introduction
2. How to Read This Guidelines
3. Scope
4. About Self-responsibility
5. Interoperability and Standardizations
6. Basic Security Guidelines for General Health Information Systems
7. Requirements for full digital systems
   Integrity and Responsibility, Readability, Sustainability, and Digital Signature
8. Requirements for Outsourcing of Data Storage
9. Scanning or Digitizing of Analog Data.
10. Rules for Maintaining and Using Health Information Systems

Appendix 1. Sample of rules for Basic Security Measurements
Appendix 2. Sample of rules for Full Digital Systems
Appendix 3. Sample of rules for Outsourcing of Data Storage

Security Guidelines for Health Information Systems

Chapter 6 Basic Security Guidelines for General Health Information Systems

6.1 Policy and Disclosure
6.2 Identify the Data and Risk Analysis
6.3 Organizational Security
6.4 Physical and Environmental Security
6.5 Technical Security
6.6 Personnel Security
6.7 Abandonment of Health Data
6.8 System Development and Maintenance
6.9 Security for Information Exchange with Other Institutes with Information Networks

Structure of Guidelines

Each Articles has 4 Categories

A. Requirements by lows, directives and other guidelines

B. Explanations of Requirements and Key Issues

C. Category I Guideline
   Action must be taken to address these

D. Category II Guideline
   Action should be considered to address these

Example: Technical Security

A. Requirements
   APPI, Duty of Confidentiality (Penal Code, etc.)

B. Explanations
   1. Authentication
      Robustness of each authentication method
      Notices for using security token such as smart cards
      Notices for using biometrical authentication
   2. Asset classification and access control
   3. Audit log
   4. Measures for mal-software

Example: Technical Security

C. **Category I Guidelines**
1. Identification and Authentication
2. Attention for information leak on system test
3. Access control by professions etc.
4. Logging and audit
5. Requirement for timestamp
6. Measures for computer viruses and worms

D. **Category II Guidelines**
1. Asset classification and access control by classification
2. Confirmation of effect of measures for viruses and worms
3. Screen locking on leaving

Action Plan 2006 (Health field)

Make New Grand Design for Healthcare ITC

MHLW announced first draft and emphasizing constructing Japanese EHR

Common Infrastructure

Healthcare PKI ,Secure Network, and Healthcare smart card

ITC Based Healthcare Network

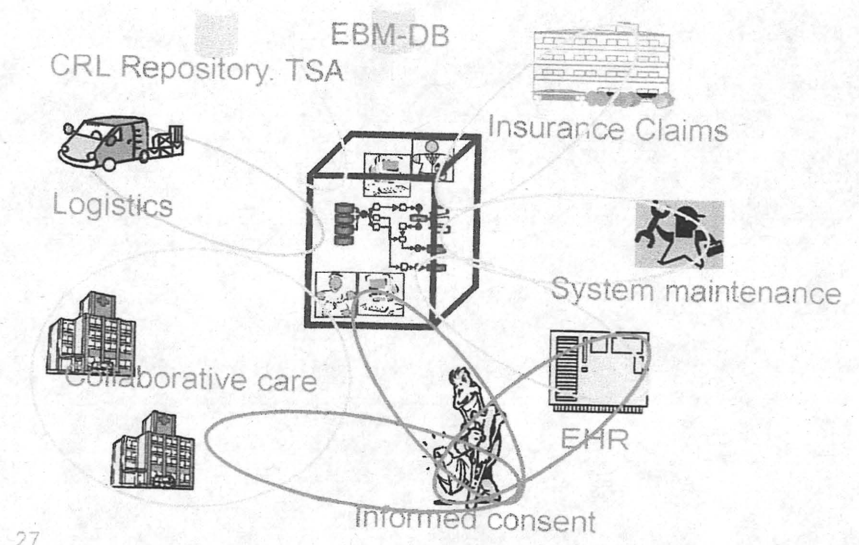
Regional and inter-regional healthcare network

Gathering nation-wide heath data (EHR) and analysis.

Developing healthcare terminology and ontology

Full Online Handling of Insurance Claims

Network, network, network.....



Security Guidelines for Health Information Systems

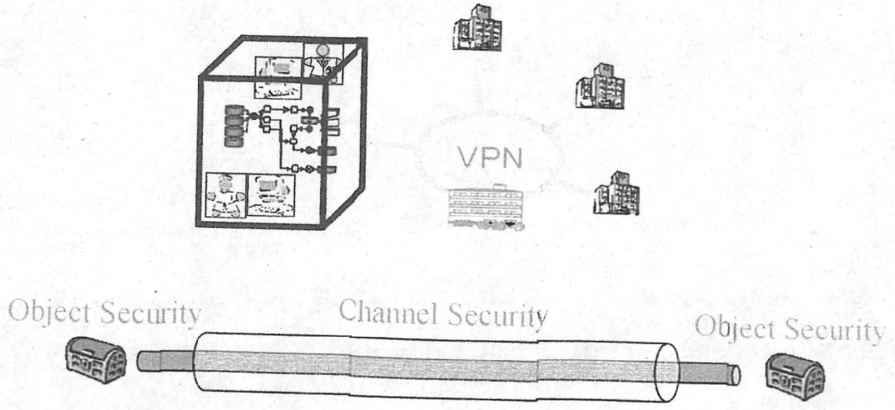
Version 2 MHLW 2007 - 10 Chapters and 3 Appendices, over 100 pages

Completely rewriting 6.9 (Security for Information Exchange with Other Institutes with Information Networks)

Adding sub-section for measures for major disaster and cyber terrorism (BCP etc.)

Some editorial corrections

Requires both Channel Security and Object Security



B to C case: Appropriate authentication with encryption (SSL)

Security Guidelines for Health Information Systems v.3

Chapter 4 Responsibility of security measures

Demarcation of responsibility for information security between stakeholders

Are Data transferred as trust operation or as transfer operation?

Who is responsible for what part of information security?

Network availability

Network (Channel) confidentiality

Object confidentiality

Accidental inappropriate routing

Etc...

What is the responsibility?

Responsibility in usual operation

- Accountability
- Keep appropriate operation
- Continuous Check and improve the system and operation

Responsibility on accidents

- Accountability
- Protect the worsening process and recover abnormal state as soon as possible
- Compensation if necessary

Who is responsible?

Data moves as trust operation

- Primarily, Healthcare institute that patient visits is responsible.
- Healthcare institute must make contraction or memorandum to clarify the responsibility for maintenance, recovering on accidents, and compensation.

Data moves as transfer operation

- Responsibility moves as data move completely.
- Stakeholders must clarify the state that is declared as data are completely transferred.
- Also, Healthcare institute must remind that digital data is not erased besides intentional removing when data are transferred.

Security Guidelines for Health Information Systems v.4

- Rewriting all sections for simplicity and easy to recognize, and updating relating standards

Reducing volume, especially in sections for full digital systems

Updating relating standards and interoperability factors

Adding the guidelines for the internet access to own hospital information systems by healthcare professionals

Correlation with METI (Ministry of Economy, Trading and Industry) and MIC (Ministry of Internal Affairs and Communication)

Guidelines of METI and MIC

Security Guidelines for Health Information Systems 3rd ed.

【MHLW】

Security Guidelines for Data Center Service Providers with health data handling 1st ed.

【METI】

Security Guidelines for ASP・SaaS 1st ed.

【MIC】

4th Edition (Mar. 2009)

Security Guidelines for Health Information Systems 4th ed.

【MHLW】

Ver. 4.1 (Dec. 2009)

Security Guidelines for Data Center Service Providers with health data handling 2nd ed.

【METI】

Security Guidelines in Health care field for ASP・SaaS providers 2nd ed.

【MIC】

Allows full ASP, SaaS or Cloud EMR with real thin client…

Thank you for your attention!

資料４

Secure networks for internal and external information exchange in hospitals

Katsuya Tanaka
The University of Tokyo Hospital
katsuya@hcc.h.u-tokyo.ac.jp

Outline

- Network Security
  - ➢Risk Analysis
  - ➢Basic Technical Measures
- Internal Network Security
  - ➢Security Monitoring of Wireless Network System
- External Network Security
  - ➢Secure Remote Access for Web Based Clinical Information System

Guidelines in Japan

- “Guidelines for the Security Management of Health information Systems”, March 2005, Ministry of Health, Labour and Welfare, Japan
- Edition 4.1 was published, Feb. 2010.

- These guidelines include those for the electronic storage of clinical and other records legally subject to storage (including the external storage of hard copies) and those for information system operation management relating to the protection of personal information at medical and nursing care institutions.

Security Management (Chap.6)

6 Basic Security Management of an Information System
6.1 Establishment and Announcement of Policies
6.2 Implementation of Information Security Management System (ISMS) at a Medical Institution
6.2.1 ISMS Construction Procedure
6.2.2 Grasp of Handled Information
6.2.3 Risk Analysis
6.3 Systematic Security Management Measures (System and Operation Management Regulations)
6.4 Physical Security Measures
6.5 Technical Security Measures
6.6 Human Security Measures
6.7 Discard of Information
6.8 Alteration and Maintenance of Information System
6.9 Taking out Information and Information Equipment
6.10 Emergency Action in Disasters or Other Incidents
6.11 Security Management at External Exchange of Health information Including Personal Information
6.12 Electronic Signature for Compulsory Signing and Sealing

Risk Analysis (Chap. 6.2.3)

1. Electronic data stored in a health information system
   (a) Illegal access, tampering, damage, loss, or leakage by an unauthorized person
   (b) Access, tampering, damage, loss, or leakage for an unjust purpose by an authorized person
   (c) Access, tampering, damage, loss, or leakage by illegal software, such as a computer virus

2. Memo, script, examination data, etc. used for input
   (a) Peering at memos, scripts, examination data, etc.
   (b) Taking out memos, scripts, examination data, etc.
   (c) Copying memos, scripts, examination data, etc.
   (d) Inappropriate discard of memos, scripts, and examination data

3. Information terminal, such as a notebook PC storing personal information and other data
   (a) Taking out an information terminal
   (b) Access, tampering, damage, loss, or leakage through a network by illegal software, such as a PC
   (c) Information leakage by inappropriate handling of software (Winny and other file exchange software, etc.)
   (d) Theft or loss of an information terminal
   (e) Inappropriate discard of an information terminal

Risk Analysis(Cont.)

4. Portable media, etc. storing data
   (a) Taking out portable media
   (b) Copying portable media
   (c) Inappropriate discard of portable media
   (d) Theft or loss of portable media

5. Browsing screen of terminal, etc.
   (a) Peering at a terminal screen

6. Data printed paper, film, etc.
   (a) Peering at paper, film, etc.
   (b) Taking out paper, film, etc.
   (c) Copying paper, film, etc.
   (d) Inappropriate discard of paper, film, etc.

Risk Analysis(Cont.)

7. Health information system itself
   (a) IT faults by cyber attacks
   - Illegal intrusion
   - Tampering
   - Illegal command execution
   - Information disturbance
   - Virus attack
   - Denial of Service (DoS)
   - Information leakage, etc.

   (b) IT faults by unintentional factors
   - System specification or program bug
   - Operational error
   - Fault
   - Information leakage, etc.

   (c) IT faults due to disasters
   - Power failure due to a disaster, such as an earthquake, flood, lightning, fire, etc.
   - Communication failure due to a disaster, such as an earthquake, flood, lightning, fire, etc.
   - Computer facility damage due to a disaster, such as an earthquake, flood, lightning, fire, etc.
   - IT malfunction in an important infrastructure operation, etc. due to a disaster, such as an earthquake, flood, lightning, fire, etc.

Technical Security Measures

<u>(1) User identification and authentication</u>

(2) Information classification management and access authority management

(3) Access log

<u>(4) Illegal software measures</u>

<u>(5) Illegal access from network</u>

<u>(6) Other</u>

（1） User identification and authentication

- The general means of authentication are the combination of an ID and a password using the “memory” of the user, “biometrics” using the body characteristics of the user, such as a fingerprint, veins, and iris, and “physical media” like an IC card (security device).

（4） Illegal software measures

- The most effective measures may be illegal software scan software. Illegal software can be detected and removed by keeping the scan software resident in terminals, servers, and network equipment of the information system.
- This is also true for information terminals and PCs used outside a Medical Institution.
- Since computer viruses are always changing, it is essential to keep the pattern files up to date for detection.

（5） Illegal access from network

- For security from a network, a firewall is a means of protection from a hacker, computer virus, or software attack for illegal access.
- If a wireless LAN or information wall socket may allow physical network connection by an outsider, it will be possible to connect an illegal computer for virus infection, an attack to a server or network equipment (DoS: Denial of Service, etc.), or illegal data monitoring or tampering on a network.

(6) Other

- A wireless LAN is very useful when a nurse uses an information terminal at the side of a patient's bed. On the other hand, since there are also concerns regarding a communication failure, information availability should be ensured. Due care is also necessary for uses around equipment that may be affected seriously by radio waves.

Firewall

- Acts as a security gateway between two networks
  - ✓ Usually between trusted and untrusted networks
    (ex. between a private network and the Internet, internal/external)
- Function
  - ✓ Prevent attacks from untrusted networks
  - ✓ Protect data integrity of critical information
- Internal Use
  - ✓ Access Control to Clinical Information Systems
  - ✓ Access Control between terminals
    - ➢ prevent outbreak of computer virus/worms

Security Management at External Exchange of Health information Including Personal Information (6.11)

I. Connection by Closed Network
- ✓ Leased line
- ✓ Public network, ie. ISDN
- ✓ Closed-area IP communication network, IP-VPN

II. Connection by Open Network
- ✓ Health information itself must be encrypted.

III. Connection from Outside with Mobile Terminal, etc.

SSL, Secure Socket Layer

- Widely deployed security protocol
  - Supported by almost all browsers and web servers
  - https
- Originally designed by Netscape in 1993
- Number of variations:
  - TLS: transport layer security, RFC 2246
- Provides
  - Confidentiality
  - Integrity
  - Authentication
- Original goals:
  - Had Web e-commerce transactions in mind
  - Encryption (especially credit-card numbers)
  - Web-server authentication
  - Optional client authentication
- Available to all TCP applications
  - Secure socket interface, Server & Client Applications.

Remote Access to Medical Instituitions

Channel Security
- Measures shall be taken to prevent message insertion, virus infection, and other tampering on a network channel.
- Measures shall be taken to prevent a hacker from tapping a password or text on a channel between facilities.
- Measures shall be taken to prevent session hijacking, IP spoofing, and other spoofing.
- Measures that satisfy the above requirements may be those which reserve a secure communication channel by using IPSec and IKE.

Object Security
- Security measures, such as encryption of the said information itself, shall be taken between the sender and receiver. Such measures shall include SSL/TLS, S/MIME, and file encryption. An encrypt key of the e-Government recommended ciphers shall be used.