SAPIENZA
UNIVERSITÀ DI ROMA

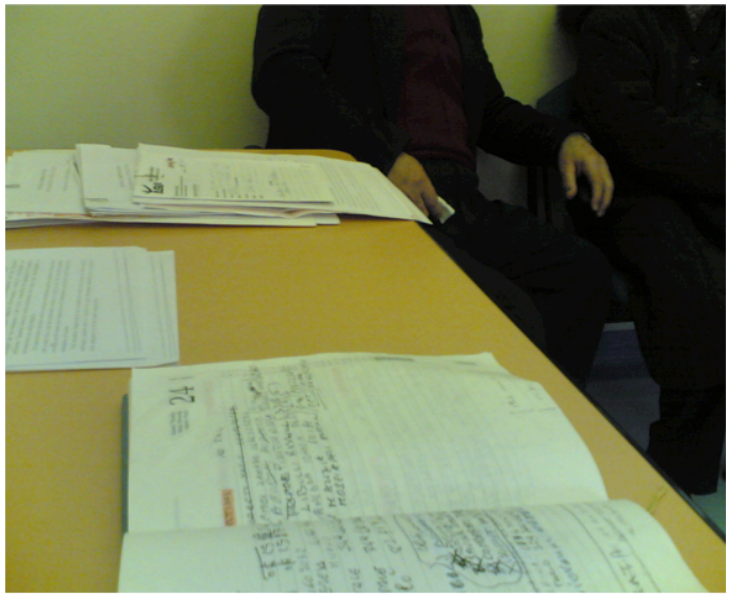
CLAUDIO CILLI
cilli@di.uniroma1.it
http://dsi.uniroma1.it/~cilli

E-HEALTH SECURITY: SPECIFICITÀ E PROBLEMATICHE

La biblioteca di Alessandria

Sanità e carta

- Se la Biblioteca di Alessandria non fosse andata distrutta da un incendio e più di cinquecentomila testi antichi non fossero andati perduti probabilmente la nostra civiltà, la nostra vita, sarebbe stata diversa. Il riferimento all'opportunità di conservare il nostro patrimonio culturale non è casuale.
- La sanità è il settore pubblico dove si producono più carta e firme



Le garanzie necessarie

Da sempre l'uomo ha chiesto ai documenti alcune importanti certezze:

- Autenticità
- Integrità
- Non ripudio
- Confidenzialità

Per ottenere queste certezze si è sempre fatto ricorso a modifiche fisiche al documento:

- firme, sigilli, timbri, punzoni, filigrane, ologrammi, …

…ma il documento moderno è immateriale!

Come agire in mancanza di un supporto fisico?

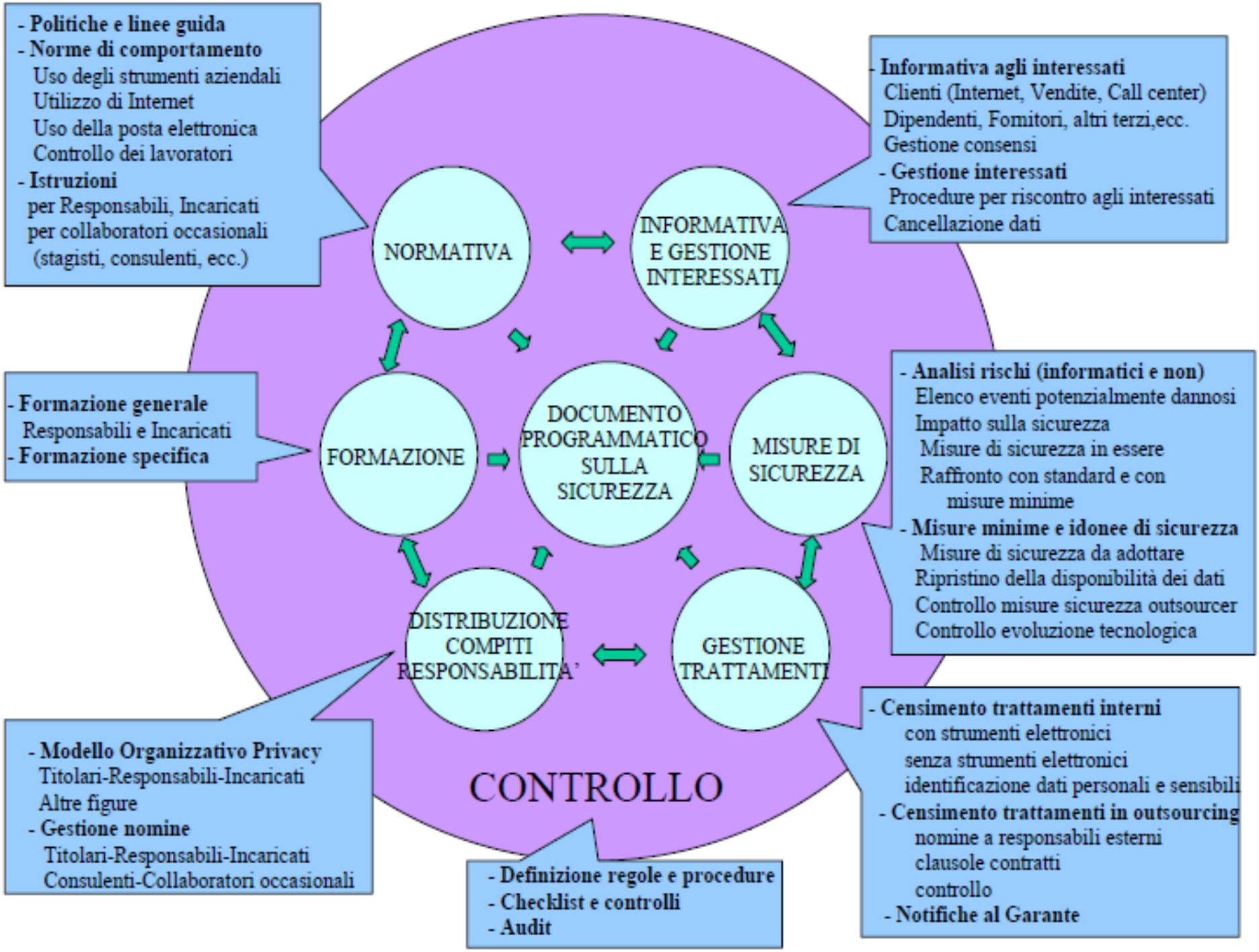
L’innovazione tecnologica ha trasformato radicalmente la nostra maniera di vivere

Ha cambiato profondamente anche il lavoro degli operatori sanitari

- Adesso tutti i medici usano tastiera, mouse e computer. Chi avrebbe mai immaginato negli anni 80 di avere il mondo a portata di mano (orecchio, mouse, tastiera, eccetera)?

Eccellenza informatica

- Oggi il livello d'eccellenza delle strutture sanitarie si valuta, tra l'altro, dall'utilizzo degli strumenti informatici e dalla competitività innovativa, poiché comportano una maggiore efficienza sia dal punto di vista organizzativo che della qualità delle cure


- Politiche e linee guida
- Norme di comportamento
Uso degli strumenti aziendali
Utilizzo di Internet
Uso della posta elettronica
Controllo dei lavoratori
- Istruzioni
per Responsabili, Incaricati
per collaboratori occasionali
(stagisti, consulenti, ecc.)
NORMATIVA
INFORMATIVA E GESTIONE INTERESSATI
- Informativa agli interessati
Clienti (Internet, Vendite, Call center)
Dipendenti, Fornitori, altri terzi,ecc.
Gestione consensi
- Gestione interessati
Procedure per riscontro agli interessati
Cancellazione dati
- Formazione generale
Responsabili e Incaricati
- Formazione specifica
FORMAZIONE
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
MISURE DI SICUREZZA
- Analisi rischi (informatici e non)
Elenco eventi potenzialmente dannosi
Impatto sulla sicurezza
Misure di sicurezza in essere
Raffronto con standard e con misure minime
- Misure minime e idonee di sicurezza
Misure di sicurezza da adottare
Ripristino della disponibilità dei dati
Controllo misure sicurezza outsourcer
Controllo evoluzione tecnologica
DISTRIBUZIONE COMPITI RESPONSABILITA'
GESTIONE TRATTAMENTI
- Modello Organizzativo Privacy
Titolari-Responsabili-Incaricati
Altre figure
- Gestione nomine
Titolari-Responsabili-Incaricati
Consulenti-Collaboratori occasionali
CONTROLLO
- Definizione regole e procedure
- Checklist e controlli
- Audit
- Censimento trattamenti interni
con strumenti elettronici
senza strumenti elettronici
identificazione dati personali e sensibili
- Censimento trattamenti in outsourcing
nomine a responsabili esterni
clausole contratti
controllo
- Notifiche al Garante

Il passaggio dalla carta ai bit è ineluttabile

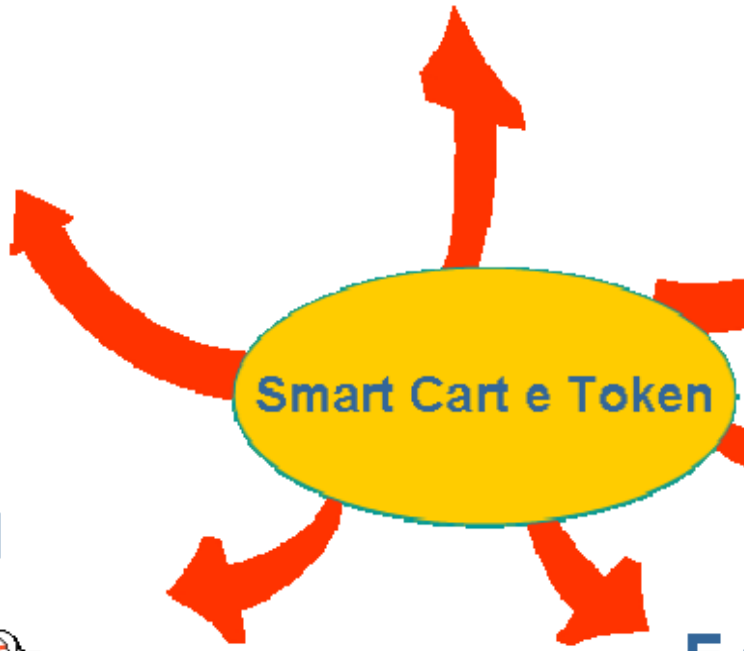
- A livello globale, c'è sicuramente una fortissima accelerazione sul tema della sicurezza delle informazioni e la consapevolezza comune che si tratti di un elemento imprescindibile è ormai assodata
- Il ciclo delle innovazioni tecnologiche non corre più sul mese o sul giorno, bensì sull'istante

Web

E-mail

Secure Desktop

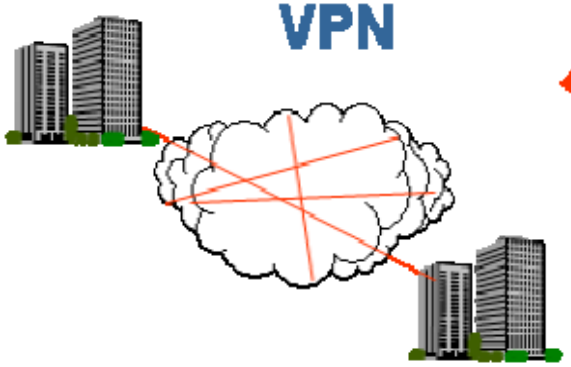
Mobile



Single Sign On

****

VPN

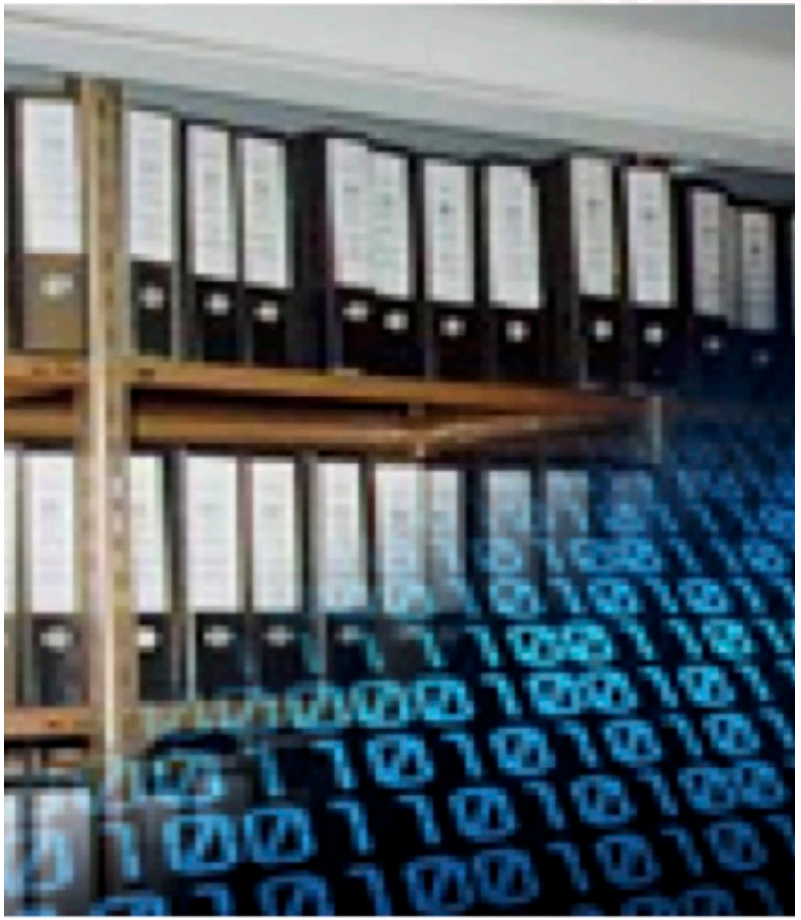


E-commerce

La conservazione digitale
Schema generale

Dematerializzazione

- La dematerializzazione è un processo per mezzo del quale si opera la trasformazione di un documento cartaceo in documento digitale o si genera lo stesso direttamente in forma digitale



Conservazione digitale

"..È la conseguenza diretta del progressivo incremento della gestione documentale informatizzata all'interno delle strutture amministrative pubbliche e private e come effetto dei processi di sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico, a cui la normativa recente ha conferito pieno valore giuridico"

Obbligo di comunicare l'avvenuta adozione del FSE entro il 31/12/2009 (mancata comunicazione sanzione da 30 a 180 mila euro)

LG - FSE e dossier sanitario
16.7.2009 Garante Privacy

La conservazione digitale

- È il processo finalizzato a rendere non deteriorabile e quindi disponibile nel tempo, in tutta la sua integrità ed autenticità, un documento. E' sempre generato da documenti digitali, opportunamente differenziati per la loro tipologia d'origine (fonte CNIPA)
- Strumento potente sul piano dell'archiviazione di quantità di documenti, della consultazione locale e remota e della elaborazione dei dati nel tempo

Il dilemma digitale

- La smaterializzazione dell'informazione, comporta dei rischi ed apre il dilemma digitale: quanto sono affidabili le nuove tecnologie per consegnare la memoria del presente alle generazioni future?

La necessità di protezione

- L'attività di protezione e di prevenzione contro il falso, le truffe, gli incidenti, presuppone, la necessaria presenza nelle aziende della figura dell'information security manager
- Oggi però la presenza nelle aziende di questo tipo di manager, che deve essere un po' tecnologo, psicologo, avvocato, poliziotto, auditor e soprattutto manager con strutture proprie (C2 ossia comando e controllo), non è ancora prevista e reputata necessaria

“La Rete non è il Far West”

- Da tutto ciò emerge la figura del direttore d’spedale, più complessa, più poliedrica, che non si deve fermare solo all’uso personale del PC e della rete, quale fattore di lavoro, ma essere…

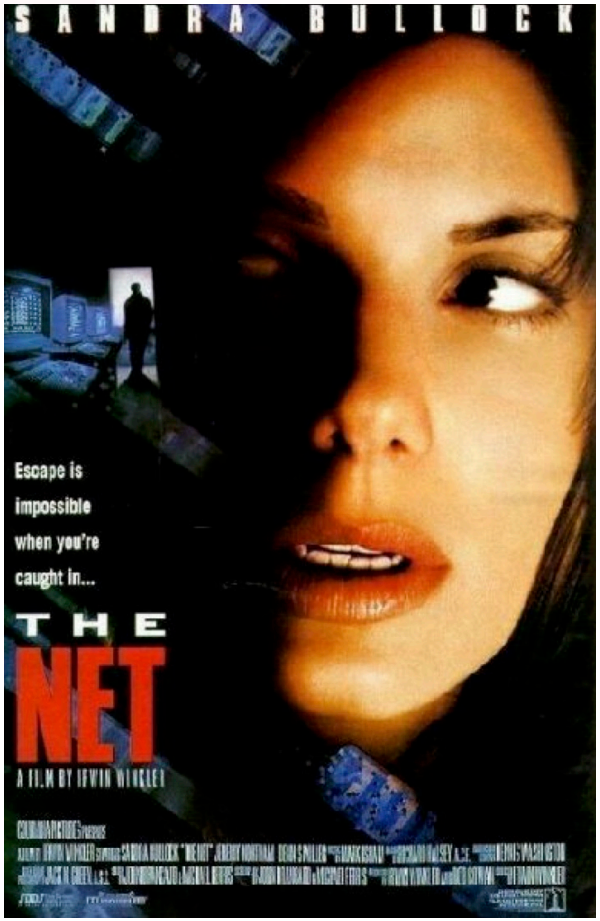
...un Netizen (cybercitizen)

- "È una persona che partecipa attivamente alla vita di Internet, contribuendo e credendo fermamente nella libertà di espressione tramite questo mezzo"

netizen

ANMDO
Associazione Nazionale dei Medici delle Direzioni Ospedaliere

Rischi futuri: il furto di identità



- Per opportunità o obblighi, il *netizen* vive e si esprime sempre più soltanto in Rete
- Anche senza chiamare in causa la fantascienza, la Rete tende a mediare e sostituire i contatti sociali
- Il problema principale in futuro sarà sempre più il furto d'identità
- La dimensione transnazionale della Rete e dei suoi servizi non fa che aggravare i rischi e i problemi...

Velocità di propagazione

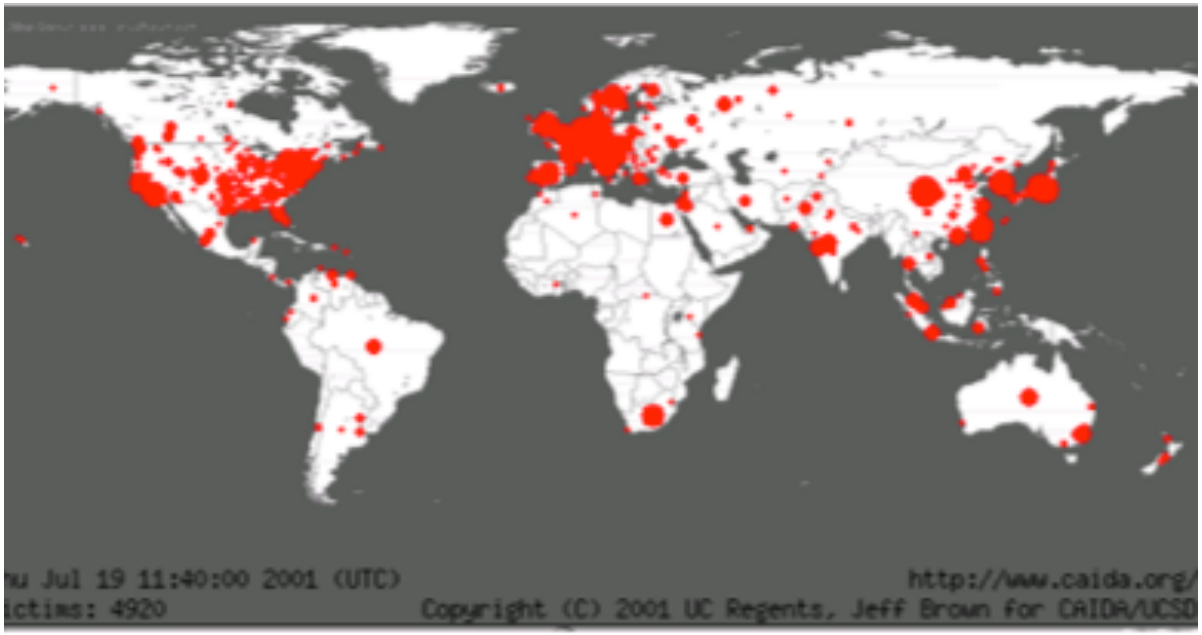
- La velocità di propagazione delle notizie in Internet è spaventosa
- La rete internet ha memoria, come il nostro cervello, e ogni notizia inserita resta permanentemente memorizzata, modificando le caratteristiche di interconnessione tra i vari nodi

- Un utente di una rete sociale (es.: facebook) con degli amici sparsi in giro per il mondo immette un'informazione personale (es.: una sua foto)

Start time: 00:00:00 (hh:mm:ss)

Velocità di propagazione

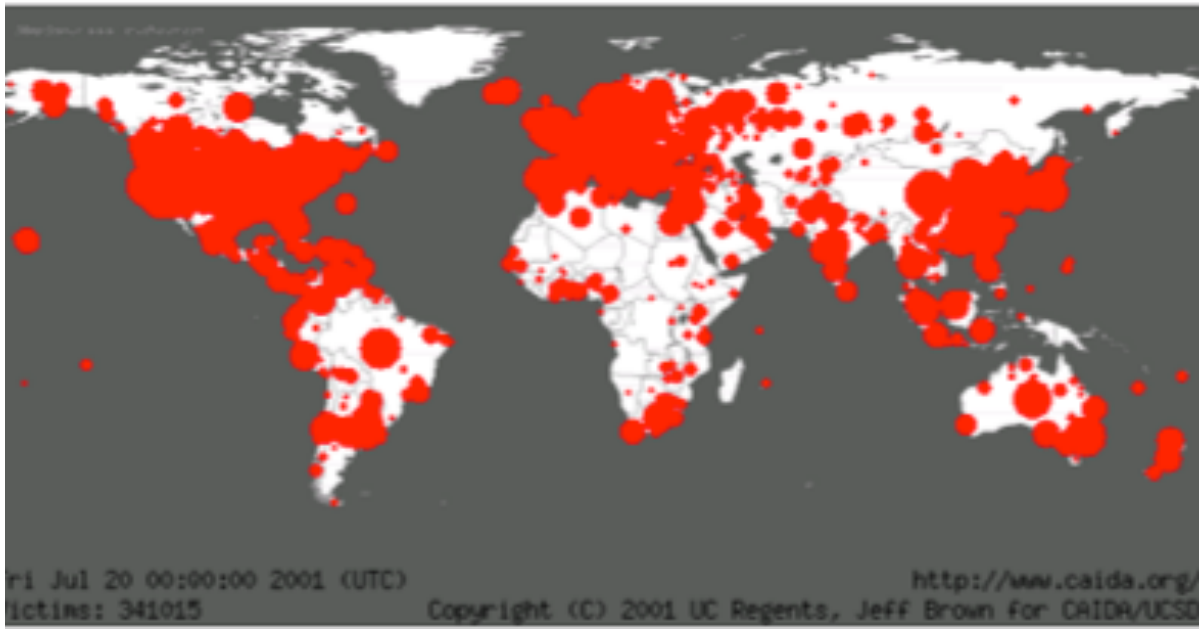
- Dopo 1.2 minuti 4,920 elaboratori (gli “amici degli amici”) dispongono dell’informazione, che resta memorizzata anche nei loro PC



Elapsed time: 00:01:20 (hh:mm:ss)

Velocità di propagazione

- Dopo 2.4 minuti – 341,015 elaboratori dispongono dell'informazione che è ormai impossibile tenere sotto controllo, e soprattutto eliminare dalla rete



Elapsed time: 00:02:40 (hh:mm:ss)

Alcune fonti normative

Codice Amministrazione Digitale (D. Lgs. n. 82/2005 del 7 marzo 2005) aggiornato con le modifiche di cui al Decreto Legislativo 30 dicembre 2010 , n. 235 (G. U. del 10 gennaio 2011;

Ministero della salute. Linee Guida Nazionali "Il fascicolo sanitario Elettronico". Roma 11 novembre 2010;

Garante Privacy - Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009. (G.U. n. 178 del 3 agosto 2009);

Garante Privacy - Linee guida in tema di referti on-line - 19 novembre 2009. (G.U. n. 288 dell'11 dicembre 2009);

Decreto Legislativo 4 aprile 2006, n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005 recante codice dell'amministrazione digitale;

Decreto Legislativo 7 marzo 2005, n. 82 Codice dell' Amministrazione digitale (GU n. 112 del 16.5.2005 Supp.Ord. n. 93);

Deliberazione CNIPA 19 febbraio 2004, n. 11 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali – Art. 6 comma 1 e 2 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 (Deliberazione n. 11/2004). (GU n. 57 del 9.3.2004);

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale dei documenti informatici (GU n. 95 del 27.4.2004);

Decreto legislativo 30 giugno 2003, n. 196. Codice in materia di protezione dei dati personali. G.U. n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123

Decreto Ministeriale 14 febbraio 1997 n. 230 Norma di attuazione del D.lgs n. 230/95. "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare ed i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche ai sensi dell'art. 111 comma 10 del decreto legislativo 17 marzo 1995 n.230;

Circolare del Ministero della Sanità del 14.3.96, n. 900.2/2.7/190 "Registro Operatorio";

Decreto Legislativo 17 marzo 1995, n. 230 Attuazione delle direttive EURATOM 80/836. 84/467. 84//466. 89/618. 90/641. E 92/3 in materia di radiazioni ionizzanti (GU n. 136 del 13.6.1995);

D.M. del 28.12.1991 "Istituzione della scheda di dimissione ospedaliera";

Circolare del Ministero della sanità 19 dicembre 1986, n. 61 Circolare avente per oggetto il periodo dio conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura.

Il ruolo dell'Unione Europea
"Perchè rispettare la riservatezza?"

Who has a right to know your healthcare information?

- If you are >18
- Are fully competent (or are competent to understand your medical information in order to make a decision)
- And are alive
- Only you and the people you authorise to share your private information with have a right to view your information (relatives of a competent adult do not)

Incapacity

- Where an individual cannot; comprehend or retain treatment information, believe it and weigh it in the balance to arrive at a choice then they are considered unable to consent to that treatment

- If a doctor decides to breach confidentiality on the 'best interest' argument, first they must weigh the possible harms against the benefits, second, they must be prepared to justify their decision and third if unsure they should consult experienced colleges

Death

- Declaration of Geneva – ‘respect for the secrets confided… even after the patient has died’
- General Medical Council – ‘extends after death’
- Morally an individual’s confidentiality is still considered to require respect

- Legally - confidence is prima facie a personal matter thus the legal duty ends with the death of a patient
- Death certificate is a public document
- Medical records can be accessed if certain criteria are met

Minors

- Unwanted parental intrusion to confidentiality can result in minors loosing trust in healthcare providers and move away from health care

How can healthcare providers insure confidentiality is maintained

- **Discretion in general conversations**
  - 'New technology' : Facebook, Twitter
  - Online posting of unprofessional content

    (Katherine C. Chretien, et al. *JAMA. 2009;302(12):1309-1315 Oct, 2009)*
- **Examining how we talk to patients**
  - Out-side work
  - With Non-clinical personnel:(confidentiality agreement)
- **How do we 'carry' data?**
  - Unsecured laptops
  - USB keys
  - Is data anonymized where possible
- **When information is shared – every party must be aware of his/her obligation of confidentiality**
- **Seek patient consent as early as is reasonably possible**

Definitions

- eHealth:healthcare practice supported by electronic processes and communications. It covers a wide range of services and systems at the edge of healthcare such as EHR, telemedicine, health information networks, e-prescription, etc.

- Telemedicine: is the provision of healthcare services through the use of ICT, in situation where patient and health professional are not in the same location

Hybrid character of eHealth

- EHealth is at the crossroad of various topics: health policy, ICT (e-commerce & e-signature), consumer protection, data protection, medical devices, freedom to provide services etc.

- No EU legislation specifically on eHealth

European Commission (EC) actions in eHealth

- **1-2004 eHealth action plan *to be updated in 2012*:**
  - Adressing common challenges such as interoperability
  - Creating pilot projects to speed deployment of eHealth (e.g. epSOS, renewing Health)
  - Disseminating best practices and benchmarking among Member States
- **2-Studies published by the Commission on the legal aspects of eHealth covering both the EU and the national levels**
- **3-Commission communication on telemedicine COM (2008) 689 emphasizing the need to bring legal clarity**
- **4-2008 Commission recommendation on cross-border interoperability of Electronic Health Records (EHR)**
- **5-2010 Commission communication on a Digital Agenda for Europe**
- **6-2011 Directive on Patients rights in cross-border healthcare which covers telemedicine – Article 14 eHealth voluntary network**
- **7-Preparation of a Staff Working Paper mapping existing EU legislation that could apply to telemedicine and identifying the open issues**

eHealth voluntary network

- The 2011 Directive on patient rights in cross-border healthcare provides for the creation of voluntary network of Member States health authorities to facilitate cooperation and the exchange of information among Member States in the field of eHealth (Article 14).
- The voluntary network should draw guidelines on:
  - A minimum set of data to constitute patients' summaries that can be shared between health professionals and across borders;
  - effective methods for enabling the use of medical information for public health and research.
- The network should also support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.

Telemedicine: Focus areas

- Starting point – legal qualification: telemedicine is an information society service
- Licensing, registration, authorisation of health professionals
- Reimbursement
- Liability
- Personal data protection

Starting point – legal qualification : Telemedicine services as information society services (ISS)

- Is Telemedicine an "information society service (ISS)"?
- Definition of information society services: "any service normally provided for remuneration, at a distance, by electronic means, at the individual request of a recipient of service"
- Most telemedicine services fall within this definition and so are information society services - therefore covered by the scope of the ecommerce directive
- Exceptions: telemedicine services provided by traditional telephone and services provided in the presence of the patient

Licensing/registration of health professionals

- In a cross-border telemedicine scenario, does the telemedicine practitioner need to be licensed/ registered also in the Member State of the patient?
  - Directive 2005/36 on recognition of professional qualifications is not applicable – requires physical presence of the health professional in the patient's country
  - If telemedicine is an ISS => E-Commerce directive is applicable –> country-of-origin principle – but exceptions possible on ground of public health safety + MS obligation to notify

Reimbursement

- National level
  - It is up to the Member States to decide whether telemedicine is reimbursed.
  - Some Member States do not recognise telemedicine as a proper medical act and therefore it is not reimbursed
- Cross-border level (when CB dimension)
  - 2011 Directive on patients' rights in cross-border healthcare covers telemedicine services
  - General rule on reimbursement: patients allowed to receive healthcare in another Member State and be reimbursed up to the level of reimbursement applicable for the same treatment in their national health system – (prior authorisation can be necessary)
- Conclusion: MS may have to recognize telemedicine as a medical act when implementing the directive

Liability

- Medical liability and services liability
  - no EU legislation
  - National legislation applies
  - Applicable national law needs to be determined
- EU consumer protection legislation: liability for defective products
- No liability of intermediaries (ex. Internet service providers) for “mere conduit”, “catching” or “hosting” (e-Commerce Directive)

Health data protection

- **General principles of data processing in 95/46/EC Data Protection Directive:**
  - Health data are sensitive data – prohibition to process – exemption: preventive medicine, medical diagnosis, the provision of care or the management of healthcare services + professional secrecy
  - Reform of the European Data protection rules ongoing - proposal by end 2011

Relevant documents

- EC Studies on legal aspects of eHealth covering both the EU and the national levels (2006-2007): http://ec.europa.eu/information_society/activities/health/studies/published/index_en.htm#Legally_eHealth
- 2008 Communication on Telemedicine: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:EN:PDF
- 2008 Commission Recommendation on cross-border interoperability of Electronic Health Records (EHR): http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=510
- Commission Communication 'A comprehensive approach on personal data protection in the European Union' COM(2010) (reform of data protection) 609: http://ec.europa.eu/justice/policies/privacy/review/index_en.htm

Relevant documents

- 2008 Commission Recommendation on cross-border interoperability of Electronic Health Records (EHR): http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=510
- Commission Communication ‘A comprehensive approach on personal data protection in the European Union’ COM(2010) 609: ttp://ec.europa.eu/justice/policies/privacy/review/index_en.htm

HCISPP℠

HealthCare Information
Security and Privacy Practitioner

The front-line defense in protecting

PATIENT INFORMATION

(ISC)²

Who is (ISC)²?

- Established in 1989 – Not-for-profit consortium of information security industry leaders
- Global leaders in certifying and educating information security professionals throughout their careers
- Over 100,000 certified professionals in more than 160 countries

www.isc2.org/credentials

HCISPP HealthCare Information Security and Privacy Practitioner

(ISC)²

(ISC)² Mission

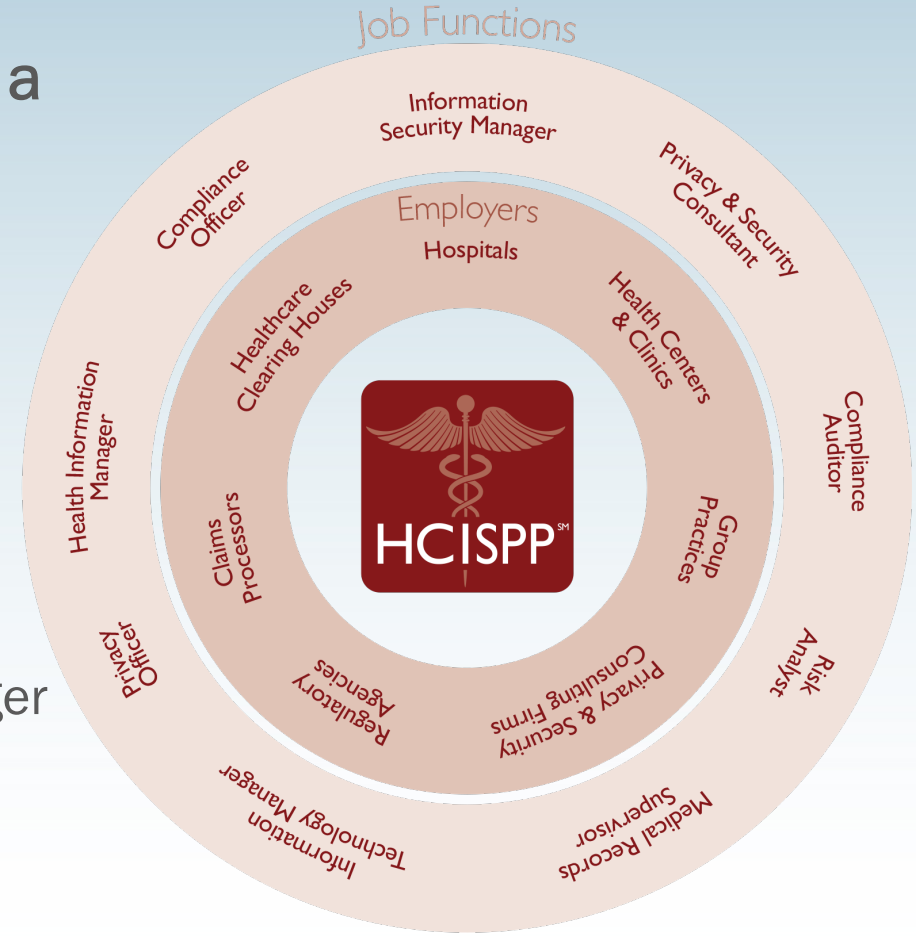
Support and provide members and constituents with credentials, resources, and leadership to secure information and deliver value to society

Who are HCISPPs?

- HCISPPs are the practitioners whose foundational knowledge and experience unite healthcare information security and privacy best practices and techniques under one credential to protect organizations and sensitive patient data from emerging threats and breaches.

HCISPP Candidates

- HCISPPs are instrumental to a variety of job functions:
  - Compliance Officer
  - Information Security Manager
  - Privacy Officer
  - Compliance Auditor
  - Risk Analyst
  - Medical Records Supervisor
  - Information Technology Manager
  - Privacy & Security Consultant
  - Health Information Manager



HCISPP
HealthCare Information Security and Privacy Practitioner

(ISC)²

HCISPP Domain Overview

HCISPP™ HealthCare Information Security and Privacy Practitioner

(ISC)²

Overview of the HCISPP Domains

- Healthcare Industry
- Regulatory Environment
- Privacy and Security in Healthcare
- Information Governance and Risk Management
- Information Risk Assessment
- Third Party Risk Management

Healthcare Industry Domain Objectives

- Identify the different types of health care organizations
- Identify the various health care information technologies
- Define the different aspects of health insurance, including processing claims, coding, billing, and reimbursement
- Describe the regulatory environment with regard to security, privacy, and oversight
- Explain the processes of clinical research and the requirements for public health reporting
- Describe the management of health care records
- Identify external third-party requirements
- Explain the Foundational Health Data Management Processes

Regulatory Environment Domain Objectives

- Identify and interpret all applicable regulations related to the health care information industry
- Describe the international regulations and controls pertaining to the health care industry
- Identify policies, procedures, and standards needed for the internal organization based on new information security and privacy policies and procedures
- Describe the health care industry compliance frameworks
- Identify the different risk-based decision processes
- Define the health care information industry environment code of ethics and reasons for compliance

Privacy and Security Domain Objectives

- Describe basic objectives of security based on confidentiality, integrity, and availability
- Provide definitions and concepts of generally used security terms
- Describe the general privacy principles as defined by the health care industry
- Compare and contrast the relationship between security and privacy
- Define the different categories of sensitive data

Privacy and Security Domain Objectives

- Describe the unrelated nature of health care data handling implications
- Define terms specific to security and privacy for the health care industry

Information Governance and Risk Domain Objectives

- Define security and privacy with regard to information and governance and their structures
- List and describe risk management methodologies
- Describe the risk management life cycle
- Explain the risk management activities that are specific to the health care industry

Information Risk Assessment Domain Objectives

- Describe the risk assessment processes, procedures, and concepts as they relate to the health care industry
- Use organizational risk frameworks to identify the control assessment procedures
- Based on the organizational role, participate in the risk assessment
- Identify ways to mitigate and reduce gaps in information risk

Third-Party Risk Management Domain Objectives

- Define what constitutes a third party within the health care industry
- Define processes for maintaining third-party health care organizations
- Describe the management standards and best practices for engaging with third parties in the health care industry
- Identify the required third-party assessments
- Define the role regarding the supporting activities for third-party assessments

Third-Party Risk Management Domain Objectives

- Identify messaging requirements for responding to security and privacy incidents
- Describe the connectivity requirements for third parties
- Describe responsibilities in the promotional awareness of all third-party requirements
- Identify requirements for participation in remediation efforts
- Describe the process for responding to third-party events regarding security and privacy

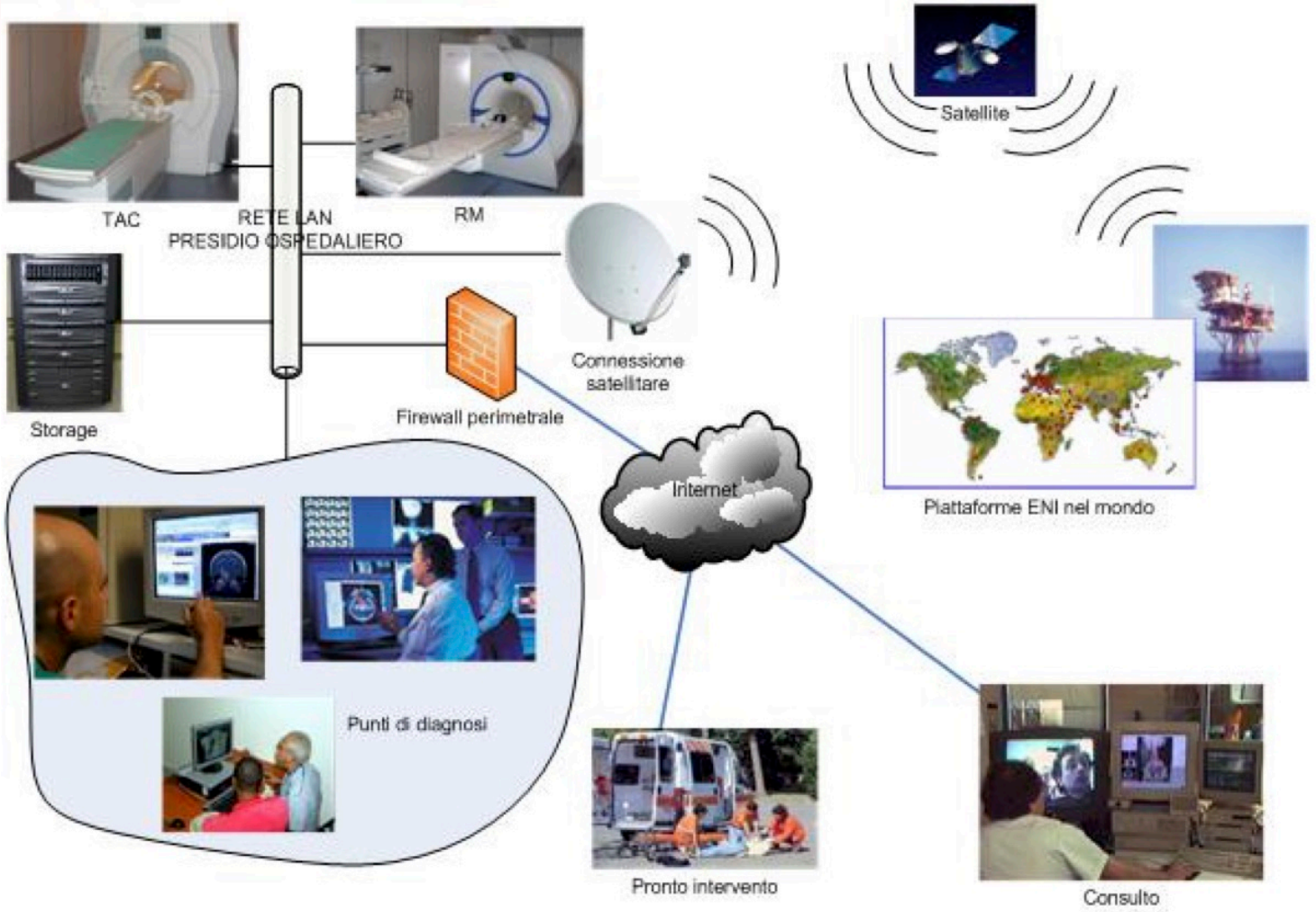
Azienda Ospedaliera San Camillo-Forlanini

PROGETTO: TELERX - EHEALTH

AZIENDA OSPEDALIERA SAN CAMILLO FORLANINI

- **Realizzazione di una "Piattaforma di e-Health – Portale di Teleradiologia e Telemedicina dei Servizi" finalizzato alla:**
  - Telediagnosi, il Teleconsulto e la Telemedicina a supporto dei Progetti Territoriali, nazionali di ricerca e di Cooperazione Sanitaria Internazionale (Ospedali italiani nel Mondo, contingenti per operazioni umanitarie, emergenze sanitarie, Missioni Civili, Militari e Industriali).
  - Programmi Sanitari di Diagnosi, Epidemiologia e Screening radiologico nelle aree endemiche o depresse.
  - Unità di crisi per Epidemie e Medicina delle Catastrofi
  - Collegamento sanitario interospedaliero permanente nazionale e internazionale (missioni laiche e religiose, civili e militari [di pace]) operanti in situazioni critiche

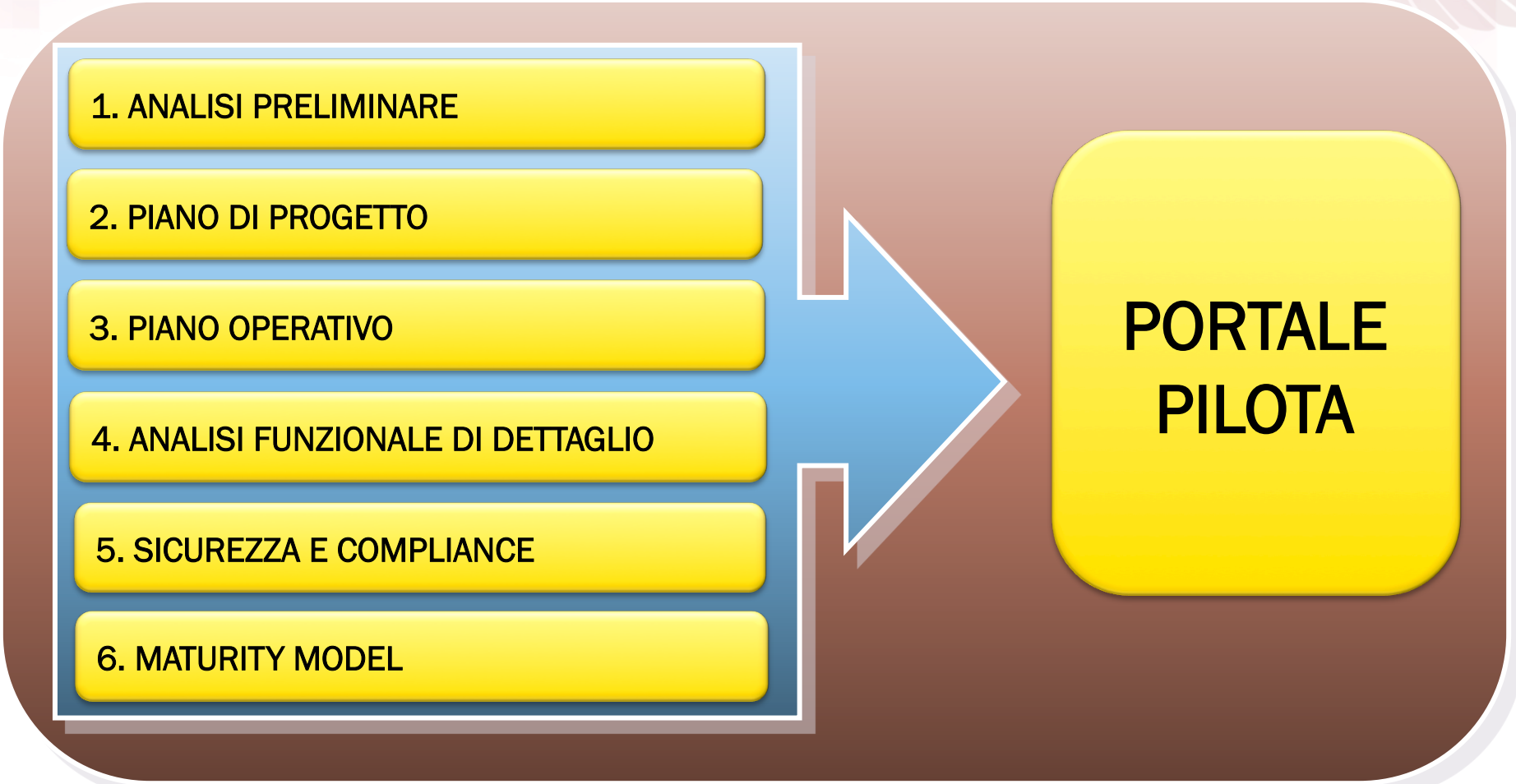
“TELERX – Piattaforma E-Health”



Benefici della piattaforma

- Forte riduzione dei costi di progettazione
- Forte riduzione del Time To Market
- Accesso alle competenze necessarie senza assunzione/formazione di risorse interne
- Forte focalizzazione sui requisiti del cliente
- Indipendenza dai fornitori
- Risposte di maggior qualità dal mercato

Le fasi della progettazione



Grazie per l'attenzione!