Il significato di appropriatezza nella diagnostica di laboratorio nell'ottica del risparmio delle risorse e della riduzione del rischio
Scuderie degli Estensi
Tivoli, 16 ottobre 2008

Requisiti di sicurezza nella gestione dei dati per pazienti e operatori

Marco Pradella
Asolo

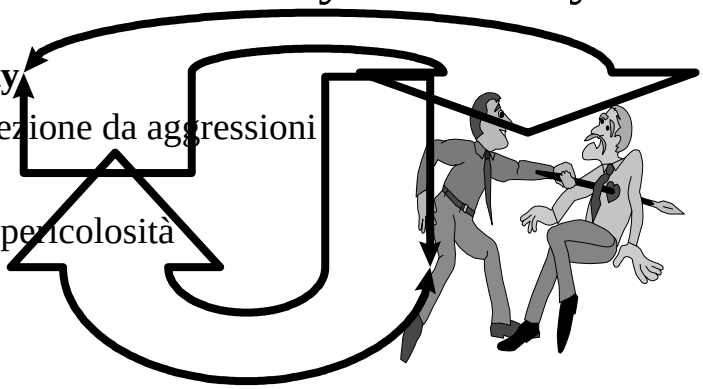
riferimenti informatica laboratorio medico

WWW.

simel.it
GdS Informatica
corso FAD sicurezza IT
cismel.it
labmedico.it
bitmedico
ihe.net

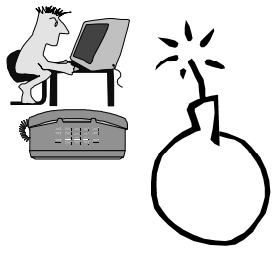
sicurezza: “security” o “safety”

- **security**
  - protezione da aggressioni
- **safety**
  - non pericolosità

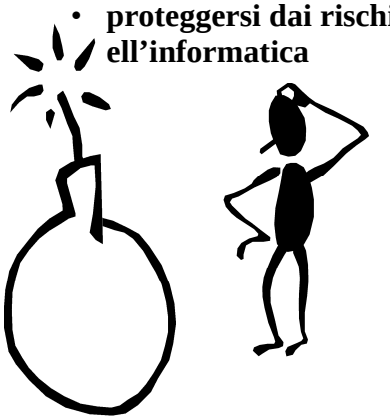


rischi, sicurezza e ICT

- **informatica per proteg gersi dai rischi**

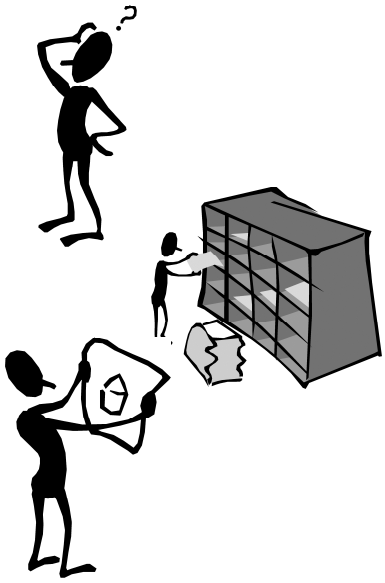


- **proteggersi dai rischi d ell’informatica**



le domande

1. perchè dovrei fare tutto ciò?
2. dove trovo indicazioni p er quello che devo fare?
3. da dove inizio a metterle in pratica?



le domande

1. perchè dovrei fare tutto ciò?
2. dove trovo indicazioni p er quello che devo fare?
3. da dove inizio a metterle in pratica?

sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali
  - ISO
  - CEN
  - CLSI
- applicazione degli standard: IHE

sicurezza ed affidabilità

- requisiti minimi nazionali

visite ispettive

visite ispettive ?

Legge regionale 16 agosto 2002, n. 22 (BUR n. 82/2002)
AUTORIZZAZIONE E ACCREDITAMENTO DELLE STRUTTURE SANITARIE, SOCIO-SANITARIE E SOCIALI
accertamento - visite ispettive - contestazione – chiusura

Art. 11 - Accertamento e verifica dei requisiti minimi e di qualità per l'autori zzazione all'esercizio.

Legge regionale 16 agosto 2002, n. 22 (BUR n. 82/2002)
AUTORIZZAZIONE E ACCREDITAMENTO DELLE STRUTTURE SANITARIE, SOCIO-SANITARIE E SOCIALI

Art. 11 - Accertamento e verifica dei requisiti minimi e di qualità per l'autorizzazione all'esercizio.

...

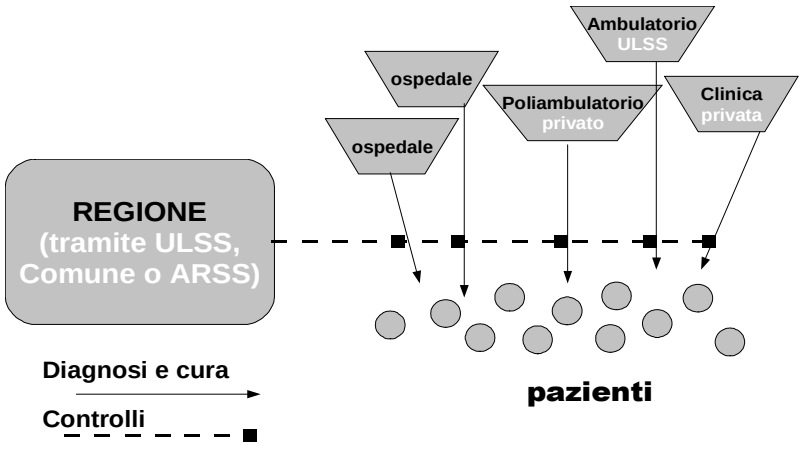
2. L'accertamento del possesso e la verifica del mantenimento dei requisiti ... La verifica deve essere effettuata con periodicità almeno quinquennale ed ogni qualvolta se ne ravvisi la necessità.

3. Qualora si verifichino inadempienze ... contesta alla struttura inadempiente le irregolarità rilevate e, con formale diffida, ne impone l'eliminazione ... ordina la chiusura temporanea, totale o parziale, della struttura medesima ... procede alla revoca dell'autorizzazione

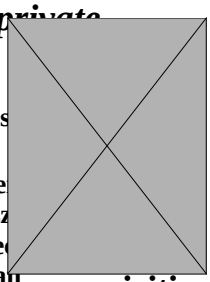
4. ... accertamento del possesso dei requisiti ... anche attraverso visite ispettive.

2. accertamento
... verifica
3. contestazione
... diffida
... chiusura temporanea, totale o parziale,
... revoca dell'autorizzazione
4. visite ispettive.

i controlli



Legge regionale 16 agosto 2002, n. 22 (BUR n. 82/2002)
AUTORIZZAZIONE E ACCREDITAMENTO DELLE STRUTTURE SANITARIE, SOCIO-SANITARIE E SOCIALI
requisiti - strutture pubbliche - strutture private



Art. 10 - Requisiti minimi e di qualità per l'autorizzazione all'esercizio.

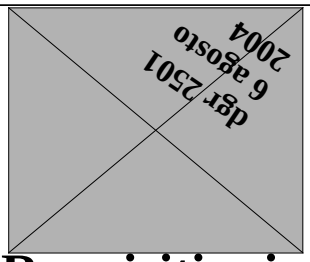
1. Entro centoventi giorni dall'entrata in vigore della presente legge la Giunta regionale, sentite le istituzioni e le organizzazioni interessate, stabilisce i requisiti minimi, generali e specifici e di qualità, per l'esercizio di attività sanitarie e socio-sanitarie da parte delle strutture pubbliche, di istituzioni ed organismi a scopo non lucrativo, nonché delle strutture private, in attuazione a quanto disposto dall'articolo 8 ter del d.lgs. n. 502/1992 e successive modificazioni, e dal decreto del Presidente della Repubblica 14 gennaio 1997 in materia di requisiti strutturali, tecnologici ed organizzativi minimi per l'esercizio delle attività sanitarie.

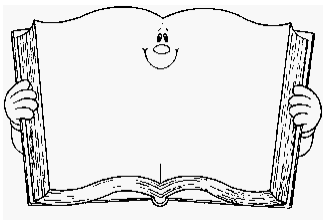
requisiti
minimi
generali
specifici

Requisiti minimi

Regione del Veneto -ARSS -Manuale programma Autorizzazione e Accreditamento Istituzionale dei Servizi Sanitari, Socio-Sanitari e Sociali (lr 22 del 16 agosto 2002) Versione 18/08/2004

(dgr 2501 del 6 agosto 2004)





Requisiti minimi per informatica nelle strutture sanitarie

Regione del Veneto -ARSS -Manuale programma Autorizzazione e Accreditamento Istituzionale dei Servizi Sanitari, Socio-Sanitari e Sociali (lr 22 del 16 agosto 2002) Versione 18/08/2004

(dgr 2501 del 6 agosto 2004)

Requisiti minimi per informatica nelle strutture sanitarie

(dgr 2501 del 6 agosto 2004)

AREA 5. Requisiti organizzativi: sistema informativo

- **GENER05.AU.1.1 referente**
- **GENER05.AU.1.2 obiettivi**
- **GENER05.AU.1.3 impegno direzione**
- **GENER05.AU.2.1 documenti**

Requisiti minimi per informatica nelle strutture sanitarie

(dgr 2501 del 6 agosto 2004)

AREA 2. Requisiti organizzativi: valutazione del raggiungimento degli obiettivi programmati interni alla struttura

GENER02.AU.2.6 verifiche valutazioni s.i.

AREA 5. Requisiti organizzativi: sistema informativo

GENER05.AU.1.1 referente

GENER05.AU.1.2 obiettivi

GENER05.AU.1.3 impegno direzione

GENER05.AU.2.1 documenti

Requisiti minimi per informatica nelle strutture sanitarie

(dgr 2501 del 6 agosto 2004)

AREA 2. Requisiti organizzativi: valutazione del raggiungimento degli obiettivi programmati interni alla struttura

GENER02.AU.2.6 verifiche valutazioni s.i.

AREA 5. Requisiti organizzativi: sistema informativo

GENER05.AU.1.1 referente

GENER05.AU.1.2 obiettivi

GENER05.AU.1.3 impegno direzione

GENER05.AU.2.1 documenti

AREA 6. Requisiti organizzativi: linee guida, procedure e regolamenti interni

GENER06.AU.1.8 documenti sanitari

GENER02.AU.2.6 verifiche e valutazioni

GENER02.AU.2.6 Vengono svolte verifiche e valutazioni periodiche della validità del Sistema Informativo nel suo complesso.

Analisi & Rapporti specifici aggiornati sulla val utazione di :

1) qualità degli strumenti di raccolta dei dati ;

2) qualità dei flussi informativi;

3) utilità specifica dei flussi informativi ,

4) qualità del dato raccolto.

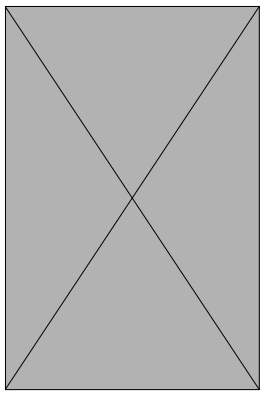
GENER05.AU.1.1 referente

GENER05.AU.1.1 E' stato individuato un **referente** del sistema informativo responsabile, che oltre al le responsabilità specifiche previste dalla **norma tiva** nazionale, abbia la responsabilità delle proc edure di **raccolta**, **verifica della qualità** e **diffus ione** dei dati.

Evidenza dell'attribuzione delle responsabilità per consent ire: 1) l'individuazione dei bisogni informativi dell'org anizzazione; 2) la progettazione e la realizzazione artic olata del sistema informativo; 3) il rispetto delle indica zioni della normativa sulla **privacy**; 4) le modalità di r accolta dei dati; 5) le modalità di registrazione, **elabor azione**, archiviazione e conservazione dei dati; 6) la ve rifica della **qualità** del dato / riproducibilità, accuratez za, completezza)..

GENER06.AU.1.8

- GENER06.AU.1.8 E' disponi bile una procedura relativa all e modalità di compilazione, c onservazione, archiviazione d ei documenti, comprovanti un attività sanitaria
  - Esistono **procedure scritte**



GENER05.AU.1.2 obiettivi

GENER05.AU.1.2 Il sistema informativo deve pers eguire i seguenti obiettivi:

GENER05.AU.1.2.1 -sostanziare e ridefinire le politiche e gli obiettivi del presidio e dell'azie nda

GENER05.AU.1.2.2 -rispondere al debito infor mativo nei confronti dei livelli sovra-ordinat

GENER05.AU.1.2.3 -fornire il ritorno informa ivo alle strutture organizzative, necessario pe r le valutazioni di loro competenza

Evidenza (indicare)

GENER05.AU.1.3 impegno informatica direzione

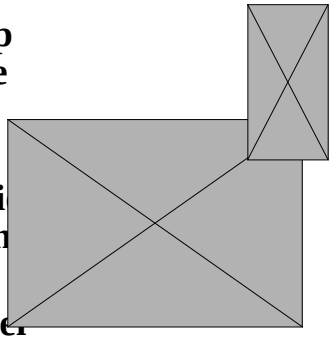
GENER05.AU.1.3 la Direzione assicura:

- **GENER05.AU.1.3.1 -l'individuazione dei bisogni info rmativi dell'organizzazione**
- **GENER05.AU.1.3.2 -la struttura del sistema informat ivo**
- **GENER05.AU.1.3.3 -le modalità di raccolta**
- **GENER05.AU.1.3.4 -la diffusione ed utilizzo delle inf ormazioni**
- **GENER05.AU.1.3.5 -la valutazione della qualità dei d ati**
- **GENER05.AU.1.3.6 -l'integrazione delle informazioni prodotte nelle attività correnti delle singole unità o perative, sezioni, uffici, ecc.**

Evidenza (indicare)

GENER05.AU.2.1 documentazione

- **GENER05.AU.2.1 E' stato predisp osto un sistema interno di gestione della documentazione sanitaria.**
- **GENER05.AU.2.3 La raccolta dei egolamenti interni e delle linee gui a è facilmente accessibile al person ale**
- **GENER05.AU.2.3.1 La raccolta dei regolamenti interni e delle linee gui da è aggiornata o confermata ogni t re anni**



sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento

ISO 9000 - normative riferimento

ISO 9000

3.9.3 criteri della verifica ispettiva:

- Insieme di politiche, procedure (3.4.5), o **requisiti** (3.1.2) utilizzati come riferimento.

3.1.2 requisito

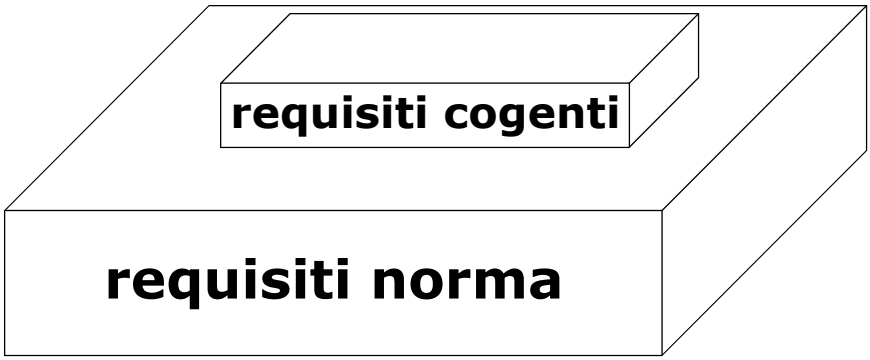
- Esigenza o aspettativa che può essere espressa, ge neralmente implicita o cogente.

ISO 9000 - normative riferimento

ISO 9001
5.1 Impegno della direzione.
L'alta direzione dà evidenza del suo impegno nello sviluppo e attuazione del S GQ e nel miglioramento continuo della sua efficacia:
a) comunicando all'organizzazione l'importanza di ottemperare ai requisiti d el cliente ed a quelli cogenti applicabili

7.2 Processi relativi al cliente 7.2.1 Determinazione dei requisiti relativi al pro dotto
Sono determinati:
… c) I requisiti cogenti relativi ai prodotti
d) Ogni altro requisito aggiuntivo stabilito dall'organizzazione stessa
7.3.2 Elementi in ingresso alla progettazione e sviluppo
… b) requisiti cogenti applicabili

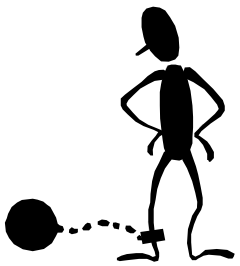
requisiti norma - requisiti cogenti



requisiti qualità - cogenti - servizio

Decreto Legislativo 30 giugno 2003, n.196

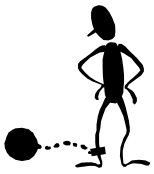
Sanzioni 196/03



- **Violazioni amministrative**
  - **161. 3-18000 €, 5-30000 € (aum. fino 3 volte)**
  - **162. 5-30000 € 500-3000 €**
  - **163 10-60000 € + diffusione media**
  - **164. 4-24000 €**
  - **165. 161 162 164 event. diffusione media**

- **Illeciti penali**
  - **167. 6-18m / 6-24m / 1-3a**
  - **168. 6m-3a**
  - **169. 0-2a / 10-50000 €**
  - **170. 3m-2a**
  - **171. Legge 300/70 art. 38**
  - **172. + diffusione media**

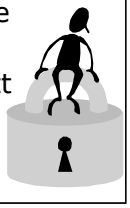
Illeciti penali **196/03** Art. 169
Misure di sicurezza



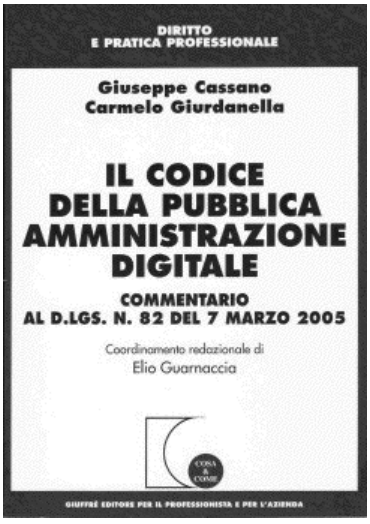
- Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall' articolo 33 è punito con **l'arresto sino a due anni** o con l'ammenda da **dieci mila euro a cinquantamila euro**
- **Art. 33 Misure minime**
  - 1. Nel quadro dei piu' generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

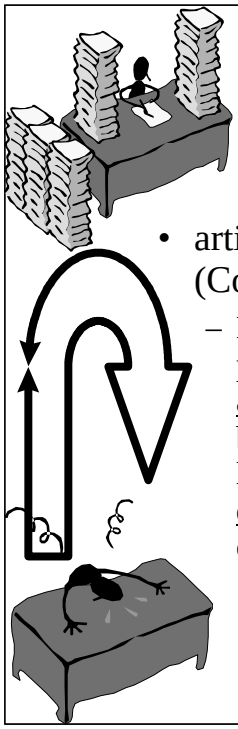
196/03 Art. 34 Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronic i è consentito solo se sono adottate, nei modi previsti dal discipli nare tecnico contenuto nell'allegato B), le seguenti **misure mini me**:
   a. **autenticazione** informatica;
   b. adozione di procedure di **gestione delle credenziali** di autenticazione;
   c. utilizzazione di un sistema di **autorizzazione**;
   d. **aggiornamento** periodico dell'individuazione dell'ambi to del trattamento consentito ai singoli incaricati e adde tti alla gestione o alla manutenzione degli strumenti ele ttronici;
   e. **protezione** degli strumenti elettronici e dei dati rispett o a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
   ...



decreto legislativo 7 marzo 2005 n. 82 (Codice dell'Amministrazione digitale)





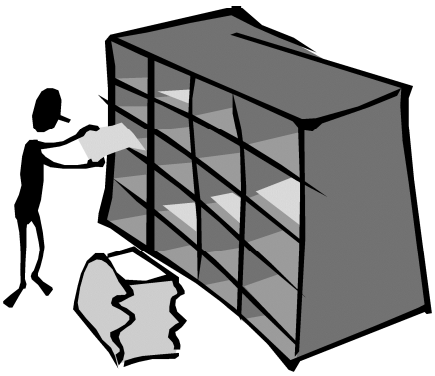
Dematerializzazione

- articolo 42 decreto legislativo 7 marzo 2005 n. 82 (Codice dell'Amministrazione digitale)
  - Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

www.cnipa.gov.it

le domande

1. perchè dovrei fare tutto ciò?
2. dove trovo indicazioni per quello che devo fare?
3. da dove inizio a metterle in pratica?



sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme

L'integrazione dei sistemi di gestione

Milano 19 - 20.05.08

Corso

* Applicare l'integrazione dei sistemi **IS O 9001**, Privacy (D.lgs. **196/03**), Sicur ezza delle Informazioni (**ISO/IEC 270 01**) e SOX (**Sarbanes Oxley**)

Istituto Internazionale di Ricerca
Know how to achieve

http://www.iir-italy.it/i309

Corso

* Applicare l'integrazione dei sistemi **ISO 900 1**, Privacy (D.lgs. **196/03**), Sicurezza delle In formazioni (**ISO/IEC 27001**) e SOX (**Sarba nes Oxley**)

Istituto Internazionale di Ricerca
Know how to achieve

http://www.iir-italy.it/i309

sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio

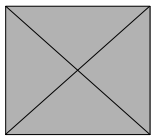
3 MEDICINA DI LABORATORIO - REQUISITI ORGANIZZATIVI

MDLB01.AU.3.8 Il sistema inform
o consente la gestione informat
a dei seguenti dati: anagrafica
aziente, accettazione, refertazi
archiviazione dei referti

qua ?
epidem ?
manag ?
196 ?

MDLB01.AU.3.9 I <u>risultati</u> degli esam
i sono conservati e disponibili pe
lmeno un anno

copie ?
196 ?



MDLB01.AU.3.12 E' disponibile un
procedura di <u>identificazione</u> e <u>rintr</u>
<u>acciabilità</u> dei campioni, reattivi e
ati

log ?

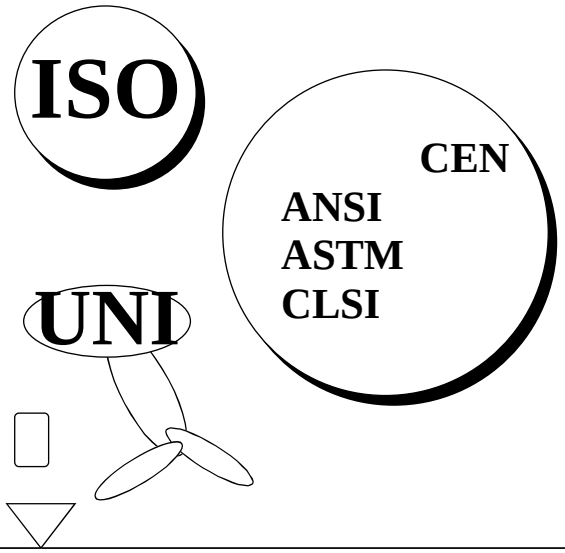
sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali

geografia della normazione

www.ANSI.org w
ww.ASTM.org w
ww.ISO.org www
.CENORM.be ww
w.UNI.com

www.CLSI.org



CISMEL

Comitato Italiano per la Standardizzazione dei Metodi Ematologici e di Laboratorio

www.CISMEL.it

ISO/TC 215
International Organization for Standardization's (ISO) Technical Committee (TC) on Health informatics.

WG 1: Health Records and Modelling Coordination
WG 2: Messaging and communications
WG 3: Health Concept Representation
WG 4: Security
WG 5: Health Cards
WG 6: Pharmacy and Medication
WG 7: Devices
WG 8: Business requirements for Electronic Health Records

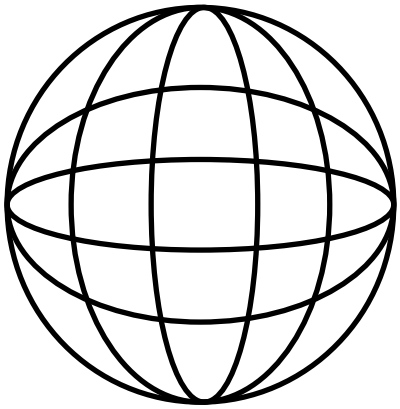
http://en.wikipedia.org/wiki/ISO_TC_215
last modified 01:28, 2 February 2007.

CEN TC 251

Working Group I Information Models
Working Group II Terminology and Knowledge Bases
Working Group III Security, Safety and Quality
Working Group IV Technology for Interoperability

http://www.centc251.org/

...globalizzazione...



ISO/TC 215
International Organization for Standardization's (ISO)
Technical Committee (TC) on Health informatics.

WG 1: Health Records and Modelling Coordination
WG 2: Messaging and communications
WG 3: Health Concept Representation
WG 4: Security
WG 5: Health Cards
WG 6: Pharmacy and Medication
WG 7: Devices
WG 8: Business requirements for Electronic Health Records

WG 9: Joint Initiative on SDO Global Health Informatics St andardization - Joint Working Group (WG9)

Joint Initiative of SDO Global Health Informatics Standardization

CEN/TC 251, ISO/TC215 and HL7 launched their inaugura l Joint Initiative Council and Joint Working Group at the ISO meeting last week in Brisbane [August 26, 2007] ho sted by Standards Australia. *This is in response to calls f or coordination and collaboration of health informatics s tandards developments from government, health provide r and vendor communities across the world.*

The next meeting of the Joint Working Group is scheduled to coincide with the CEN TC 251 meetings at Dublin on Oc tober 2nd, 2007.

http://www.healthinformaticsnews.com/?q=node/2

CLSI (ex NCCLS)

CLINICAL AND LABORATORY STANDARDS INSTITUTE ™

CLSI-NCCLS: Laboratory automation

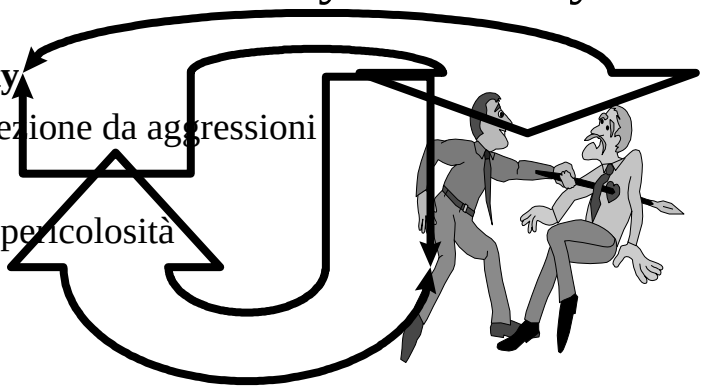
AUTO1 contenitore carrier
AUTO2 codice barre
AUTO3 comunicazioni strumenti
AUTO4 cruscotto sistemi
AUTO5 interfacce elettromeccaniche
AUTO6 poct (ora POCT01)
AUTO7 identificazione campione
AUTO8 validazione LIS
AUTO9 accesso remoto internet
AUTO10 autoverifica
AUTO11 IVD software
LIS1 interfaccia strumento
LIS2 interfaccia LIS-HIS
POCT1 connettività point-of-care
M39 statistica resistenze

sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali
  - ISO

sicurezza: “security” o “safety”

- **security**
  - protezione da aggressioni
- **safety**
  - non pericolosità



ISO/FDIS 27799:2008(E)

Health informatics — Information security management in health using ISO/IEC 27002

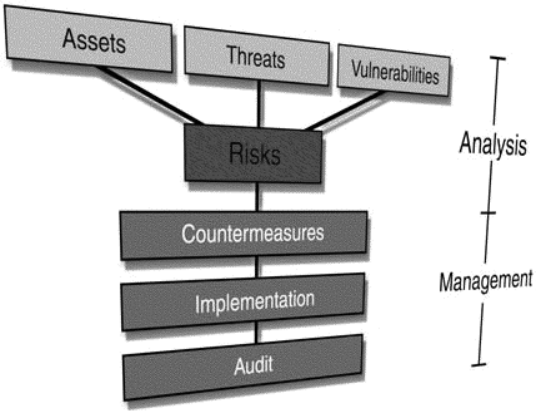
ex Guideline for security management using ISO/IEC 17799

Voting begins on: 2008-03-13

Voting terminates on: 2008-05-13

International Electrotechnical Commission (IEC)

17799:
reference to ISO/IEC 13335



ISO

ISO/IEC 27001 risk-based approach - continual process improvement

ISO/IEC 27002 (previously BS 7799 part one and ISO/IEC 17799) code of pr actice for information security management

ISO/IEC 27003 ISMS implementation guidance in support of ISO/IEC 27001

ISO/IEC 27004 information security measurements

ISO/IEC 27005 ISMS risk management methods and techniques

ISO/IEC 27006 accreditation requirements used together with ISO/IEC 1702 1-1, the generic accreditation standard

ISO/IEC 27007 auditing Information Security Management Systems.

ISO/IEC TR 27008 auditing information security controls.

ISO/IEC 27010 sector-to-sector interworking and communications

ISO/IEC 27011 telecommunications (also known as X.1051)

ISO/IEC 27012 automotive requirements

ISO/IEC 27013 world lottery association requirements

ISO/IEC 27014 transportation information systems requirements

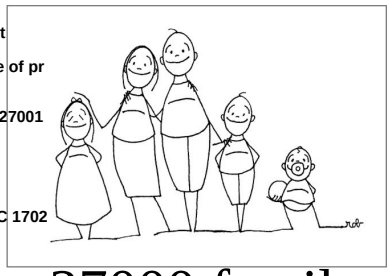
ISO/IEC 27031 business continuity

ISO/IEC 27032 cybersecurity.

ISO/IEC 27033 IT network security.

ISO/IEC 27034 application security.

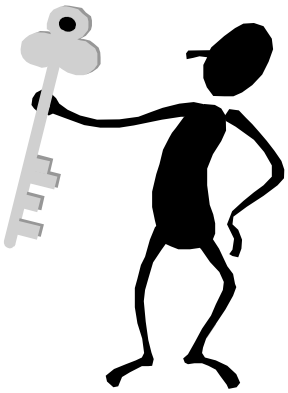
ISO/IEC 27799 health sector specific

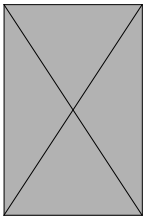


27000 family

ISO

firma digitale





DRAFT INTERNATIONAL STANDARD ISO/DIS 17090

- ISO © International Organization for Standardization, 2005
  - ISO/TC **215** Secretariat: **ANSI**
    - Voting begins on: **2005-08-25**
    - Voting terminates on: **2006-01-25**

Health informatics — Public key infrastructure

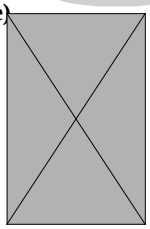
- Part 1:**Overview of digital certificate services**
- Part 2: **Certificate profile**
- Part 3: **Policy management of certification authority**

ISO/DIS 17090-2:

Root & Subordinate CA Certificates

End Entity Certificates

- **Individual**
  - **Regulated Health Professional (Qualified Certificate)**
  - **Non Regulated Health Care Employee (Qualified Certificate)**
  - **Patient/Consumer (Qualified Certificate)**
  - **Supporting Organization Employee (Qualified Certificate)**
- **Organization**
- **Devices**
- **Application**



corsi 27000

sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali
  - ISO
  - CEN

European Standards Organizations Launch Joint Project on Interoperability of eHealth standards

POSITIVE PROGNOSIS FOR eHEALTH STANDARDIZATION

Brussels (7 February 2008) CEN, CENELEC, and ETSI, the thr ee European Standards Organizations (ESOs) are pleased to a nnounce the launch yesterday of the joint project '**eHEALT H-INTEROP**', which will address the requirements of the **E uropean Commission** mandate on standardization in the fiel d of e-health. This mandate (**M/403**) aims to provide a consis tent set of standards to address the needs of this rapidly-evolv ing field for the benefit of future healthcare provision.

European Standards Organizations Launch Joint Project on Interoperability of eHealth standards

mandate (**M/403**)

In **phase 1**, a team of appointed experts reporting to the ESOs will examine the portfolios of existing s tandards from the many different organizations in the sector, including international formal bodies a nd industry standards consortia.

Phase 2, in 2009 and 2010, will see the execution o f that work program.

CEN/CENELEC/ETSI
M403 – eHealth Interoperability

Overview of interim draft, and proposed content
May 28, 2008
Prepared by Melvin Reynolds
Editor for the Project Team

eHealth-INTEROP Report
The project team will bear in mind:
The desire of the Member States to retain their autonomy;
The goal of the EC to have joint European/global standards and to have Europe an policy on eHealth;
The consequences for the working methods of the ESOs;
The need for use cases, such as the 3 priorities of the EC but also that emerge fr om consulting patients, clinicians and health authorities.

eHealth-INTEROP Report: Phase 1 Timescale: 1/2

Wider Co-ordination group in Gothenburg
28 May 2008, connected to MIE
Meeting to discuss the pre-final draft and to make pro posals for amendments
July 2008
Consultation on the pre-final draft
July/August 2008
Final phase 1 report and work programme Public cons ultation
Sept/Oct 2008

May 28, 2008
Prepared by Melvin Reynolds

eHealth-INTEROP Report: Phase 1 Timescale: 2/2

Public presentation of the report under consultation Crete
9-10 October 2008, connected to IHIC'08
Open consultation Copenhagen
7 November 2008, connected to WoHIT
Approval of the ESOs of the work programme and Submissi on of the phase 1 work programme to the EC/EFTA
Dec 2008

May 28, 2008
Prepared by Melvin Reynolds

eHealth-INTEROP Report:

in response to
EU Mandate/403-2007:

Annex A – Inventory of Standards
http://www.ehealth-interop.nen.nl
ESO_eHealth-INTEROP_A0500_20081009.doc
2008-10-09 21:35

Contents

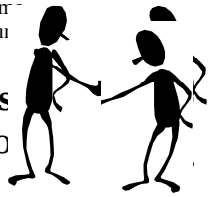
sicurezza ed affidabilità

- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali
  - ISO
  - CEN
  - CLSI

CLSI AUTO11: IT Security

Clinical and Laboratory Standards Institute document AUTO11-P

IT Security of In Vitro Diagnostic Instruments and Software Systems; Proposed Stand ard specifies technical and operational requirements, as well as technical implem ntation procedures related to security of IVD systems (devices, analytical instru ents, data management systems, etc.) installed at a healthcare organization.



The intended users for this standard are **vendors** (IVD system manufacturers), **users** (e.g., labo atory personnel), and **IT management** of the healthcare organizations.

Clinical and Laboratory Standards Institute (CLSI). IT Security of In Vitro Diagnostic Instruments and Software Systems; Proposed Standard. CLSI document AUTO11 -P (ISBN 1-56238-593-3). Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2006.

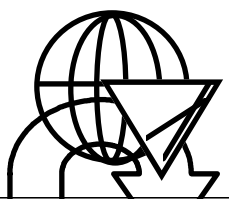
CLSI AUTO11: IT Security

3 Delineation of Vendor and HCO R bilitie s

4 Technical Design Guidelines Related to F ory Requirements

5 Process and Operational Requirements

6 Applicability to Device Classes



Technical Design Guidelines Related to Regulatory Requirements

4.1 Preventing Unauthorized Application Usage

4.2 Preventing Unauthorized Data Access

4.3 Protection From Malicious Software

4.4 Security Monitoring

4.5 Preventing Loss of Data

4.1 Preventing Unauthorized Application Usage

4.1.1 Unique User Identification

4.1.2 Authentication Mechanisms

4.1.3 Password Management

4.1.4 Password Creation and Modification

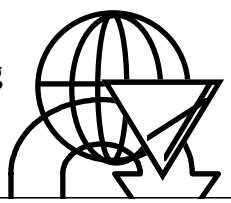
4.1.5 Password Protection, Disclosure, and Control

4.1.6 Emergency Access Procedure

4.1.7 Automatic Logoff

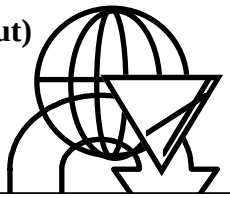
4.1.8 Login Procedures Including Monitoring

4.1.9 Operating System Access Control



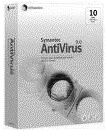
4.2 Preventing Unauthorized Data Access

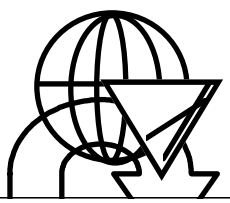
4.2.1 Choice of Development Tools
4.2.2 Minimize Network Exposure
4.2.3 System Platform Hardening
4.2.4 Security of Data Storage
4.2.5 Authentication of Data Sources
4.2.6 Transmission Security/Encryption
4.2.7 Transmission Integrity Controls
4.2.8 Limit Access to Physical I/O (input/output)
4.2.9 Tamper Resistant Hardware



4.3 Protection From Malicious Software

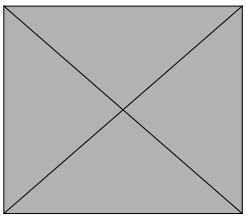
4.3.1 Operating System Vulnerabilities
4.3.2 Antivirus and Antispyware Software
4.3.3 Protection During Manufacturing, Transport, and Installation
4.3.4 Other Protections for Networked Systems
4.3.5 Limit General Purpose Usage





4.4 Security Monitoring
4.5 Preventing Loss of Data

4.4.1 Audit Controls/Accountability
4.4.2 Security Incident Reporting
4.4.3 Verify Data Integrity
4.4.4 Verify Application Integrity

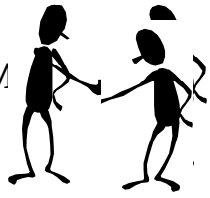


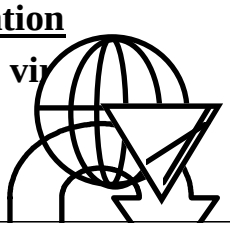
4.5.1 Data Backup and Storage
4.5.2 Eliminate Single Points of Failure
4.5.3 Fail Open

CLSI AUTO11: IT Security

Process and Operational Requirements

5.1 IT Security Requirements Engineering and Management
5.2 IT Security Hazard Analysis and Risk Management
5.3 Vendor System Validation/Verification
5.4 Vendor Security Audits/Assessments/Tests
5.5 Documents for Health Care Organization
5.6 Preventive Actions (software patches, virus definitions)



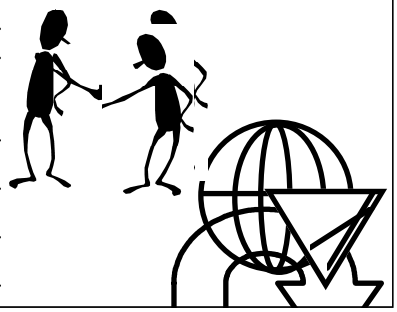


CLSI AUTO11: IT Security

Table 3. Applicability of Security Requirements to Device Classes

#	System functions & features / Regulatory requirements	Unique User Identification Req	Password Management	Emergency Access Procedure	Automatic Logoff	Login Procedures Incl. Monitoring	Operating System Access Control	Development Tools	Minimizing Network Exposure	System Platform Hardening	Secure Data Storage
General Aspects (independent of systems functions & features)											
0	All systems						V	V		V	
User Authentication & Management											
1	Single user local access (personal product)						V H				
2	Multiple users local[a] access	V H	V H	V H	V	V	V H				
3	Multiple users network[b] access	V H	V H	V H	V	V	V H		V H		
4	Multiple users remote[c] access	V H	V H		V	V	V H		V H		

6 Applicability to device classes



sicurezza ed affidabilità

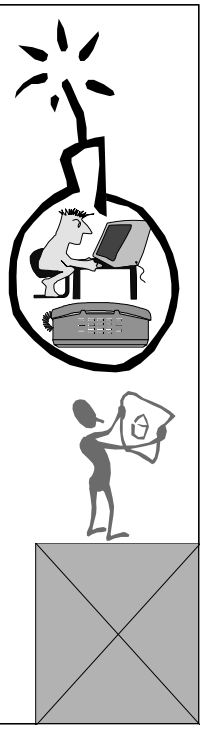
- requisiti minimi nazionali
- norme cogenti
- norme di riferimento
- integrazione delle norme
- requisiti specifici laboratorio
- norme tecniche internazionali
  - ISO
  - CEN
  - CLSI

Standard informatici

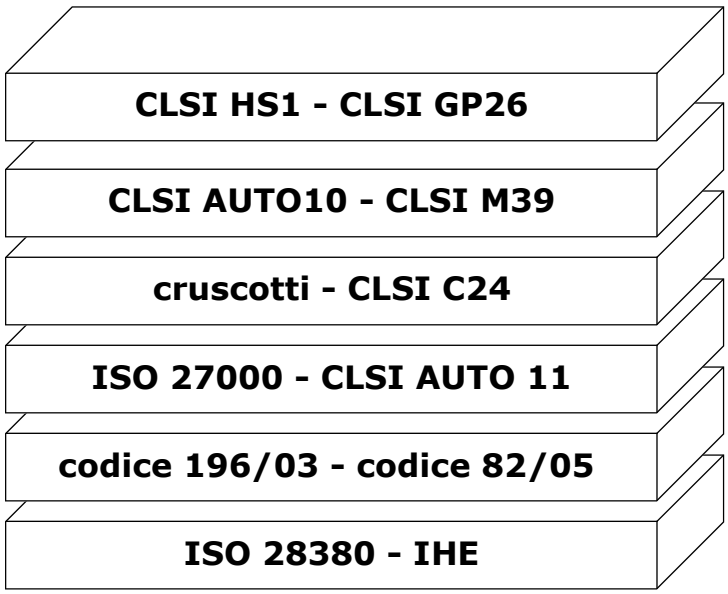
- requisiti minimi
- sicurezza
- gestione degli errori

take home

- **l'informatica sanitaria si avvale di norme tecniche già sviluppate e ben articolate**
- **le norme sono poco note**
- **senza applicazione delle norme tecniche non si soddisfano i requisiti di accreditamento professionale**
- **se non si rispettano le norme cogenti si viola la legge, talora con conseguenze penali**

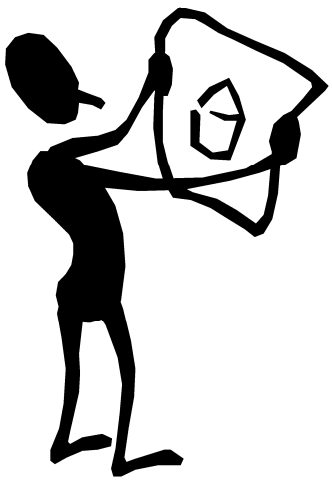


modello sicurezza affidabilità



le domande

1. perchè dovrei fare tutto ciò?
2. dove trovo indicazioni p er quello che devo fare?
3. da dove inizio a metterle in pratica?



riferimenti informatica laboratorio medico

WWW.

simel.it

GdS Informatica

corso FAD sicurezza IT

cismel.it

labmedico.it

bitmedico

ihe.net