Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Indice

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Sicurezza informatica in sanità

Non è semplice affrontare il tema della sicurezza informatica in sanità, in un contesto complicato da interventi di varia natura e persino da interessi divergenti. Nei tempi recenti persino la percezione della sicurezza ha subito modificazioni, non sempre giustificate. La Decisione 814/2005/CE del 11 maggio 2005 da Parlamento e Consiglio Europeo ha consentito l'istituzione di un programma comunitario pluriennale inteso a promuovere un uso più sicuro di internet e delle nuove tecnologie online, denominato "Safer Internet". In questa occasione sono stati identificati come principali fenomeni negativi spamming, pornografia infantile, razzismo. E' stato previsto un investimento di: 45 milioni di euro fino al 2008 (rif. http://www.eu.int/scadplus/leg/it/lvb/l24190.htm, http://europa.eu.int/information_society/activities/sip/programme/decision/index_en.htm). Questo investimento è stato ripartito indicativamente nei capitoli lotta ai contenuti illegali (25-30%), contrasto ai contenuti indesiderati o spam e nocivi o virus (10-17%), promozione ambiente più sicuro con il forum Safer Internet (8-12%), infine sensibilizzazione su contenuti illegali, indesiderati e nocivi, "se del caso" tutela consumatori, protezione dati, sicurezza reti (47-51%). Da ciò si vede che la posizione della "privacy individuale" sarebbe marginale rispetto ad altri obiettivi, mentre è difficile individuare un riferimento preciso alla firma digitale..

I corsi di Sicurezza Informatica realizzati in questo periodo contengono argomenti come virus, firewall, reti back up, disaster, recovery. La firma digitale, se cè, sta in secondo piano.

La lingua inglese è più efficace dell'italiano in questo ambito. Con il significato di "sicurezza" troviamo due termini diversi "security" e "safety". Security sta per protezione da aggressioni, mentre safety per non pericolosità. Il primo quindi è riferito alla vittima, il secondo all'aggressore.

La sicurezza informatica è definita in ISO/IEC 17799 come "preservation of confidentiality, integrity and availability of information.", quindi come caratteristica multifattoriale. Altre proprietà, come responsabilità degli utenti, autenticità, non-ripudio, affidabilità sono da considerare derivati dalle tre fondamentali.

Il responsabile di un sistema informatico sanitario dovrebbe porsi tre quesiti: è necessario occuparsi di sicurezza? Dove si trovano le indicazioni relative? Come si inizia a metterle in pratica?

La Tabella XXX contiene i principali riferimenti, tra i tanti disponibili in questa materia. Essi sono leggi dello Stato, norme tecniche degli enti di standardizzazione (ISO e CEN), linee guida delle associazioni professionali di laboratorio e di informatica.

Tabella XXX. Riferimenti per la sicurezza informatica in sanità ordinati secondo il flusso operativo

PREPARAZIONE

- ISO/IEC 27001 "Sistema per la Gestione della Sicurezza Informatica"
- ISO/IEC 17799 analisi dei rischi per la sicurezza
- ISO/DIS 27799 linee guida per 17799 nell'informatica sanitaria
- ISO/TR 16142 selezione delle norme tecniche per la sicurezza.
- CEN/TS 15260 tecniche di "risk management"

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

REALIZZAZIONE DISPOSITIVI E PROCEDURE
• ENV 12924 profilo di rischio
• ISO/DTS 25238 -2006 Classificazione dei rischi per la salute dal software
• EN 14484 trasferimento internazionale di dati personali.
• ISO 17090 infrastruttura di chiave pubblica
• linee guida per messaggi HL7 (IHE, ELINKS)
ADEMPIMENTI DI LEGGE E PROFESSIONALI
• misure minime previste dall'art. 169 del Codice della Privacy (D.Lvo 196/03), con sanzioni penali.
• College of American Pathologists checklists: gestione delle verifiche, degli errori e delle correzioni sicurezza dei dati e dei sistemi

Geografia della normazione

Una trattazione completa del panorama degli enti di normazione e standardizzazione esula dagli scopi di questo capitolo. Si può però ricordare che negli USA abbiamo ANSI e ASTM (www.ANSI.org, www.ASTM.org), in Europa il CEN (www.CENORM.be), a livello internazionale ISO (www.ISO.org) ed in Italia UNI (www.UNI.com).

A questi va aggiunto, per la normazione in laboratorio, il CISMEL, Comitato Italiano per la Standardizzazione dei Metodi Ematologici e di Laboratorio (www.CISMEL.it).

UNI contiene uno specifico organo tecnico, la Commissione Informatica medica, il cui campo di attività è costituito da "Aspetti tecnico-informatici nel settore medico, con particolare riguardo a terminologia, modello dei dati, formato dei messaggi, strumentazione, strategie e aspetti non tecnologici, tipo etico-legali, sicurezza, riservatezza e qualità", ha come riferimenti CEN il TC 251 Informatica medica e come riferimenti ISO il TC 215 Informatica medica.

(rif. www.uni.com/uni/controller/it/normazione/commissioni_tecniche/informatica_medica.htm e www.uni.com/uni/controller/it/normazione/commissioni_tecniche/informatica_medica_struttura.html)

Nella commissione Informatica medica è attivo un gruppo di lavoro specifico per i laboratori medici (GL10).

ISO TC 215 è organizzata in sette gruppi di lavoro. 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.

CEN, European Committee for Standardization o Comité Européen de Normalisation, fonda la sua attività sui principi di apertura e trasparenza, consenso, impegno nazionale e coerenza tecnica, integrazione con il restante lavoro internazionale (http://www.cenorm.be/cenorm/aboutus/generalities/how+we+work/index.asp). I gruppi di lavoro di CEN TC 251 sono solo quattro: Working Group I Information Models, Working Group II

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Terminology and Knowledge Bases, Working Group III Security, Safety and Quality, Working Group IV Technology for Interoperability.

Non è facile selezionare le norme più importanti per la sicurezza informatica. La Tabella XXX ne richiama alcune, senza pretendere di comprenderle tutte.

Tabella XXX. Recenti norme tecniche per Informatica e sicurezza informatica in sanità
– ISO/IEC 17799:2005 security
– prEN 14720:2003 service request report
– prEN 12251:2003 password
– ISO/IS 17113:2003 sviluppo messaggi
– ISO/FDIS 18812:2003 interfaccia analizzatore
– ISO/DIS 17115:2005 vocabulary
– prEN 12264:2005 strutture concetti
– prEN 1614:2005 nomenclatura laboratorio
• ISO/TS/ 17090-1: Health Informatics --Public Key Infrastructure – Part 1: Framework and overview
• ISO/TS 17090-2: Health Informatics --Public Key Infrastructure – Part 2: Certificate profile
• ISO/TS 17090-3: Health Informatics --Public Key Infrastructure –Part 3: Policy management of certification authority.
• ISO/IS ISO/22857 "Health Informatics: Guidelines on data for health care -Management and security of authentication by passwords protection to facilitate trans-border flows of personal health information".
• CEN ENV 12924: Medical Informatics – Security Categorisation and Protection for Healthcare Information System
• CEN prEN 12251 Health informatics -Secure user identification
• ISO/TS 22600-1: Health informatics – privilege management and access control – Part and policy management
• ISO/TS 22600-2: Health informatics – privilege management and access control – Part models.
• ISO/TS 22600-3: Health informatics – privilege management and access control Implementations
• ISO/TS 21091 Health informatics –directory services for security, communications, and of professionals and patients.
• ISO technical specification 21298 Health informatics – functional and structural roles.
• ISO TR 20514, Health informatics -Electronic health record – Definition, scope and context
• ISO/IEC 27799 Health Informatics: Guideline for security management using ISO/IEC 17799
• ISO/NWIP/DTS #29321 Health Informatics: Application of Risk Management to the Manufacture of Health Software
• ISO/NWIP/DTR #29322 Health Informatics: Guidance on Risk Evaluation and Management in the Deployment and Use of Health Software
• ISO/TR 27809:2007(E)Health informatics — Measures for ensuring patient safety of health software
• ISO/IEC 17799:2005, Information technology — Code of practice for information security management,
• ISO/IEC 15408, Information Technology—Security techniques—Evaluation Criteria for IT Security (Parts 1, 2 and 3), 1999.
• ISO/IEC TR 13335-1 Information technology --Guidelines for the management of IT Security --Part 1: Concepts and models for IT security
• ISO/IEC TR 13335-2 Information technology --Guidelines for the management of IT Security --Part 2: Managing and Planning IT security
• ISO/IEC TR 13335-3 Information technology --Guidelines for the management of IT Security --Part 3: Techniques for management of IT security
• ISO/IEC TR 13335-4 Information technology --Guidelines for the management of IT Security --Part 4: Selection of Safeguards
• ISO/IEC TR 13335-5 Information technology --Guidelines for the management of IT Security --Part 5: Management guidance on network security family of information security related ISO standards -2700x

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Tabella XXX. La famiglia ISO 2700X

* ISO/IEC 27000 -a vocabulary or glossary of terms used in the ISO 27000-series standards * ISO/IEC 27001 -the certification standard against which organizations' ISMS may be certified (2005) * ISO/IEC 27002 -the proposed re-naming of existing standard ISO 17799 * ISO/IEC 27003 -a new ISMS implementation guide * ISO/IEC 27004 -a new standard for information security measurement and metrics * ISO/IEC 27005 -a proposed standard for risk management, potentially related to the current British Standard BS 7799 part 3 * ISO/IEC 27006 -a guide to the certification/registration process

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Un punto fermo è oggi costituito dalla famiglia ISO/IEC 2700X (Tabella XXX), soprattutto perchè ISO/IEC 27001 consente di procedere alla certificazione dei sistemi informatici sul piano della sicurezza.

La certificazione ISO/IEC 27001 si realizza con un processo di verifica (audit) in due fasi. Prima una revisione a tavolino della documentazione chiave (politiche della sicurezza, iniziative di applicazione, sistema di gestione (Information Security Management System, ISMS). Solo successivamente si passa alla verifica sul campo di esistenza ed efficacia dei controlli definiti nel ISMS. (http://en.wikipedia.org/wiki/ISO_27001). ISO 27001 è l'evoluzione delle norme già note con l'identificativo ISO 17799.

ISO/IEC 27799 è precisamente la linea guida per applicare ISO 27001 (ossia ISO 17799) all'ambiente sanitario, votata nel 2006. ISO/IEC DIS 27799 contiene varie cose, quelle importanti stanno nel capitolo 5 (Health information security), 6 (Practical action plan for implementing ISO/IEC 17799), 7 (Healthcare implications of ISO/IEC 17799) e nelle appendici Annex A (Threats to health information security), Annex B (Tasks and related documents of the Information Security Management System), Annex C (Potential benefits and required attributes of support tools), Annex D (Related standards in health information security).

La sicurezza in informatica non è un tema molto antico, rispetto alla storia di queste tecnologie. Risalgono agli anni '70 negli USA le prime raccomandazioni sulla sicurezza dei sistemi operativi (“Orange book”), mentre negli anni '80 in ISO ed in Europa si è badato soprattutto alla sicurezza tecnologica (ITSEC, ITSEM, Common criteria). Solo negli anni '90 è comparso il concetto di “processo della sicurezza” che ha prodotto BS7799, ISO/IEC 17799, ENV 16924 e successivi.

BS7799 non è stata adottata subito come norma internazionale, avendo incontrato alcune importanti resistenze. Solo nel 2000 abbiamo l'adozione della parte 1 come ISO/IEC 17799 e solo recentemente la parte 2 come ISO 27002.

La famiglia ISO 2700X, ISO/IEC 17799, ISO 27799

ISO/IEC 17799 e le successive ISO 2700X si fondano sui tre principi di garanzia di Riservatezza, Integrità e Disponibilità informazione. Nella parte prima contiene le raccomandazioni per la gestione della sicurezza, divise in dieci aree di intervento e 6 fasi di analisi, mentre la parte seconda contiene le specifiche per la certificazione, costituite da ben 127 diversi controlli.

Il principale riferimento di ISO 17799 è la precedente ISO/IEC 13335, che introduce il concetto di analisi dei rischi preliminare alla gestione delle contromisure, che comprende pianificazione, realizzazione e verifica (audit).

Le 10 aree di intervento di ISO/IEC 17799 si distribuiscono tra 1. politica, 2. principi organizzativi, 3. controllo classificazione patrimonio, 4. personale, 5. fisica ambientale, 6. comunicazioni e operazioni, 7. accessi, 8. sviluppo manutenzione sistemi, 9. gestione continuativa, 10. controlli conformità. Le fasi di sviluppo del ISMS in ISO/IEC 17799 sono sei: I scopo, II politica, III valutazione rischio, IV gestione rischio, V controlli, VI dichiarazioni applicabilità.

L' adeguamento a ISO 9001:2000 di ISO/IEC 17799 è realizzato con l'applicazione del modello Plan Do Check Act di Deming, ossia pianificare scopo, politica, rischio, opzioni, controlli; attuare •

piano trattamento rischi, formazione, gestione operazioni e risorse, gestione incidenti; verificare monitoraggio, audit, rischio residuo, azioni ed eventi; agire su cambiamenti, azioni correttive prventive, comunicazione risultati.

Tra i contenuti di ISO 27799 possiamo citare al paragrafo 5.4 (Health information to be protected) l'identificazione delle informazioni da proteggere, ossia quelle personali, i dati pseudonimizzati, i dati statistici e di ricerca, le conoscenze mediche come ad esempio gli effetti collaterali dei farmaci, i dati degli operatori sanitari, le informazioni di rilevanza per la sanità pubblica, i risultati delle verifiche (audit), infine i dari di sicurezza del sistema, come quelli per l'accesso.

Al punto 6.4.4.3 di ISO 27799 si elencano le caratteristiche necessarie per l'analisi dei rischi, che non può essere compito di un singolo, ma deve derivare al consenso di posizioni diverse, prefigurando gli scenari peggiori possibili. Gli incidenti già accaduti possono non rappresentare il caso peggiore, per la cui definizione è necessario raccogliere contributi specialistici con ipotesi multiple. Tra le competenze necessarie si trovano a) la conoscenza medica e infermieristica dei processi, protocolli e percorsi, b) la conoscenza dei formati dei dati e delle possibilità di errore nel loro uso, c) i fattori ambientali esterni che influenzano i rischi, d) le caratteristiche degli strumenti informatici e dei dispositivi medici, e) la conoscenza delle storie di incidenti e degli attuali scenari, f) l'architettura dei sistemi e infine g) i programmi di cambiamento capaci di modificare i rischi.

La certificazione è descritta nel punto 6.6.2 di ISO 27799, che prevede l'autovalutazione (6.6.2.1 Self-assessment), l'audit di parte terza (6.6.2.3 Independent audit) ed infine la certificazione in base a ISO/IEC 27001 (• 6.6.2.4 Certification audit against ISO/IEC 27001)

Particolarmente interessanti per noi sono le implicazioni sanitarie raccolte nel capitolo 7 (Healthcare implications of ISO/IEC 17799). I punto 7.1.1 e 7.1.2 trattano del documento sulla sicurezza informatica. Il paragrafo 7.2.1 tratta dell'organizzazione interna per la sicurezza, il coordinamento, la segretezza, i contatti con autorità e altri soggetti. Al punto 7.2.2 sono invece affrontati i rapporti con soggetti terzi, i fornitori di servizi, che portano rischi specifici per la sicurezza. Il “patrimonio informativo” (asset) è trattato nel paragrafo 7.3 (Asset management), che individua le responsabilità e le modalità per identificare e classificare le informazioni sensibili. Al paragrafo 7.4 si parla di risorse umane, prima, durante e dopo il rapporto d'impiego.

Ad esempio, nel punto 7.4.3.1 in aggiunta alle indicazioni di ISO/IEC 17799 si raccomanda di considerare nella “terminazione del servizio” anche i meccanismi di rotazione nei turni, tipici del lavoro di tecnici e infermieri. Ancora, nel punto 7.5.1.3 si rileva come sia importante, in aggiunta alla prescrizione di ISO/IEC DIS 27799, tener conto di situazioni in cui il pubblico di pazienti ed accompagnatori è fisicamente presente in aree con grandi quantità di dati sensibili, come il laboratorio di analisi, il pronto soccorso, le guardiole infermieristiche vicine alle stanze di degenza.

Ai punti 7.5.5 e 7.6.7.2 si stabilisce che in aggiunta a quanto stabilito da ISO/IEC 17799 tutte le registrazioni di dati sanitari non più utilizzati siano sovrascritti o distrutti. Va posta attenzione a macchine informatiche o dispositivi medici mandati in riparazione o rimossi per fuori uso.

Il punto 7.6.1.2 ricorda l'importanza elevata dei momenti di cambiamento o riorganizzazione. In aggiunta a quanto stabilisce ISO/IEC 17799, si deve gestire ogni processo di rinnovo di attrezzature cercando di prevenire esplicitamente interruzioni improprie o alterazioni delle funzioni sanitarie.

Il successivo punto 7.6.1.3 tratta della divisione dei compiti. La separazione delle aree di

responsabilità riduce la possibilità di modifiche non autorizzate o cattivo uso delle informazioni mediche. I sistemi informatici dovrebbero garantire l'approvazione dei processi clinici da soggetti differenti se ciò è richiesto. Un esempio di questi casi è senz'altro quello del lavoro di équipe che si svolge nel laboratorio medico.

Al punto 7.6.5.1 si presenta l'obbligo di avere una copia di riserva (back up, v. anche il codice della privacy nelle misure minime) di tutte le informazioni sanitarie. La copia deve stare in un luogo fisicamente diverso ed i dati dovrebbero essere protetti con crittografia.

I punti 7.6.6, 7.6.6.1 e 7.6.6.2 di ISO/IEC DIS 27799 si occupano delle reti. Il rischio più importante è quello conseguente a interruzione delle comunicazioni in rete, le cui conseguenze assistenziali devono essere attentamente considerate. Il tema è ripreso anche al punto 7.10.1.

La posta elettronica costituisce argomento di ISO/IEC DIS 27799 al punto 7.6.8.3. I messaggi email dovrebbero essere criptati. Al punto 7.11.1.2 si discute invece il consenso alla trasmissione di dati.

La valutazione dei rischi informatici

Principio fondamentale delle norme ISO sulla sicurezza informatica è la precedenza della fase di valutazione dei rischi a quella di realizzazione delle misure di garanzia. Due gruppi di lavoro di CEN/TC 251, WGIII e WGIV, hanno prodotto uno standard che, seppur oggi superato da altre norme, costituisce un ottimo esempio schematico di valutazione dei rischi. ENV 12924: "Security categorisation and protection for healthcare information systems" definisce la sicurezza come un processo e attribuisce alle componenti meramente hardware e software di un sistema informatico una importanza molto scarsa. Al contrario, sono critici per la sicurezza gli elementi delle esigenze di riservatezza, integrità e disponibilità dei dati, l'ambiente del computer, le persone che lo utilizzano. ENV 12924 prevede che la classificazione della sicurezza e specificazione dei requisiti proceda in sei passi: • Passo 1. Valutare ACI (disponibilità -riservatezza integrità); • Passo 2. Individuare la categoria; • Passo 3. Individuare i requisiti di base; • Passo 4. Costruire il profilo di protezione: categoria più requisiti di base più requisiti di livello superiore; • Passo 5. Realizzazione dei requisiti; • Passo 6. Procedere con la sicurezza.

La valutazione ACI parte dalla disponibilità (availability) dei dati. Servono le risposte a semplici domande. La domanda 1 è: la non disponibilità delle informazioni può causare cattivo o prolungato trattamento? La domanda 2 è: se le informazioni non sono disponibili, ne risultano conseguenze finanziarie, legali o altro ? Bisogna considerare lo scenario peggiore e non tener conto di copie elettroniche o su carta. I risultati possono essere due: non critica oppure critica, rappresentati come A.n-c e A.c. La valutaizone di riservatezza C = confidentiality deriva dalle risposte alla domanda 1 (il sistema contiene, elabora o trasmette informazioni personali identificabili?), alla domanda 2 (svelare i dati sanitari a estranei può causare imbarazzo o pericolo, diretto o indiretto?) ed alla domanda 3 (svelare i dati sanitari a estranei può dare conseguenze per l'organizzazione sanitaria, danno finanziario, legale, commerciale o imbarazzo della struttura? Bisogna considerare attentamente i dati anche non identificati direttamente, ma identificabili mediante inferenza e considerare lo scenario peggiore non tener conto dei rimedi esistenti. I risultati possibili sono tre, non sensibile, sensibile e molto sensibile, con le sigle C.n-s, C.s e C-v-s .

Infine la caratteristica I = integrità deriva dalla domanda 1 (errori o mancanze possono causare

cattivo o prolungato trattamento?) e dalla domanda 2 (in caso di errori o mancanze, risultano conseguenze finanziarie, legali o altro?). Anche in questo caso bisogna considerare lo scenario peggiore e non tener conto di eventuali misure correttive. I risultati possono essere due, non critica oppure critica, con le sigle I.n-c e I.c.

La categoria di rischio risulta dalla combinazione dei risultati. I: A.nc, Cs, I.n-c; II. A.nc, Cs, I.c; III: A.c, Cs, I.c; IV: A.nc, C.v-s, I.n-c; V: A.nc, C.v-s, I.c; VI A.c, C.v-s, I.c.

Allo stesso modo ENV 12924 conduce la valutazione sull'ambiente ambiente fisico. Il profilo di ambiente fisico (PEA) può andare da 1 a 6 a seconda della risposta ad alcune alternative: accesso fisico, lontananza, staff presente a pubblico presente, sistema sorvegliato a pubblico assente. Analogamente la connessione fisica (PCA) si categorizza in tre livelli a seconda della presenza o meno di connessione in rete e della sua intermittenza o permanenza. La connessione logica (LCA) vede le alternative tra un solo dominio e più domini e tra una sola struttura sanitaria e più strutture.

Il profilo di protezione I, quello minimo, previsto in ENV 12924 comprende caratteristiche di sistema (password, gestione di log-on e log-out, privilegi, etc..), requisiti amministrativi (security manager, security policy, antivirus, manutenzione, documentazione), requisiti del personale (assunzione, gestione, addestramento, fine rapporto), requisiti fisici e ambientali (computer principale, furto, elettricità, aria, fuoco, acqua). Le categorie superiori richiedono profili di ordine superiore.

La sicurezza degli strumenti utilizzati in medicina è una preoccupazione dei pazienti, dei medici, delle autorità di sorveglianza e dei produttori da tempo. La normazione si è spesa parecchio, producendo diversi riferimenti. Ad esempio, ISO/TC 210/WG 2 ha pubblicato recentemente ISO/DTR 16142 con il titolo Medical devices — Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices, che contiene una selezione degli standard da rispettare. Tra questi, alcuni riferimenti generali come ISO Guide 51, Guidelines for the inclusion of safety aspects in standards, ISO Guide 63, Guidance on the development of International Standards in the field of health care technology, ISO Guide 64, Guide for the inclusion of environmental aspects in product standards, IEC 60513, Fundamental aspects of safety standards for medical electrical equipment. ISO/DTR 16142 cita invece come riferimenti specifici ISO 14971 Medical devices — Application of risk management to medical devices, ISO 13485 Medical devices — Quality management systems — Requirements for regulatory purposes, ISO/TR 14969 Medical devices — Quality management systems — Guidance on the application of ISO 13485:2003, ISO 14155 series Clinical investigations of medical devices for human subjects.

Non deve sorprendere la pluralità di riferimenti sullo stesso argomento. Anche ISO 9000, lo standard per i sistemi qualità che tutti conoscono, si declina per l'applicazione pratica in diverse norme: 9001 per gestione qualità, 9004 per miglioramento, 10005 per la pianificazione, 10006 per i progetti, 10007 per le configurazioni, 19011 per verifiche-audit, 10001 e 10003 per il trattamento dei clienti, 10014 per i riflessi economici della qualità. Parimenti, ad ISO 17025 per i laboratori di prova si affiancano 17001 per imparzialità, 17021 per audit, Guide 53 per certificazione di prodotto. Ad ISO 15189 per i laboratori medici seguono 22869 come linee guida applicative, 15190 per la sicurezza, 15198 per il controllo di qualità, 22367 per la gestione dei rischi, 20776 per gli antibiogrammi, 17583 per gli anticoagulanti, 15895 per i laboratori di “service”, 22870 per i point-of-care-testing.

Sorprende invece un po' che tra nella sicurezza dei dispositivi medici poco fosse dedicato all'informatica. Tanto che nel 2005 in ambito CEN fu proposto un nuovo tema di ricerca intitolato NWIP "Health informatics-Assuring patient safety of health informatics products" (CEN/TR) che rilevava appunto come l'informatica fosse fuori dal controllo per i dispositivi medici, mentre si registrava la diffusione di sistemi di supporto alla diagnosi, la pressione di fattori economici (tempo) e legali sulole attività sanitarie e la transizione a pratiche "paperless", con rischio di corruzione e perdita di dati. L'uso di strumenti informatici può avere effetti indesiderati avversi, anche letali, esattamente come le altre attività. Come riferimenti generali per questo progetto si potevano citare EN 61508-4:2001, Functional safety of electrical/electronic/programmable electronic safety-related systems -Part 4: Definitions and abbreviations (IEC 61508-4:1998 + Corrigendum 1999) ed anche ISO/IEC Guide 51:1999, Safety aspects — Guidelines for their inclusion in standards.

Il progetto è stato sviluppato fino ad arrivare a documenti consolidati, tra cui CEN/TS 15260: Health informatics - Classification of safety risks from health informatics products (oct 2006). CEN 15269 applica il principio di analisi dei rischi e assegnazione ad una classe. Gli esempi applicativi, riportati nell'allegato, si riferiscono a sistemi come la prescrizione elettronica, l'etichettatura con codice a barre, la ricerca sulle malattie sessualmente trasmesse, le ambulanze. In particolare, il codice a barre interessa i laboratori medici.

Contemporaneamente ISO lavorava allo sviluppo di una norma dello stesso tipo. Nasceva così ISO/DTS 25238 -2006 Classification of Safety Risks from Health Software, con gli stessi principi e la stessa struttura del documento.

La classificazione dei rischi di 15269 e 25238 si basa su due dimensioni. Le categorie delle conseguenze sono cinque, vanno da "minor" (danno di un singolo paziente con recupero in breve tempo) a "catastrofico" (danno mortale o con invalidità permanente di molti pazienti). Le categorie delle probabilità sono ancora cinque, da "molto bassa" (trascurabile) a "molto alta" (certo o quasi certo). La griglia bidimensionale contiene 25 celle che identificano cinque classi di rischio, A B C D E (Tabella XXX).

Tabella XXX. Griglia per la classificazione del rischio (ISO DTS 25238, CEN TS 15260)

Probabilità	***Conseguenze***				
	Catastrofiche	Maggiori	Considerevoli	Significative	Minori
Molto alta	A	A	B	B	C
Alta	A	B	B	C	C
Media	B	B	C	D	D
Bassa	B	C	D	D	E
Molto bassa	C	C	D	E	E

Ad esempio, il già citato sistema di codice a basse (appendice B.2 Bar code tracking system), usato comunemente per identificare i campioni in laboratorio, se produce un errore comporta la non

disponibilità di informazioni necessarie al clinico. Ma si pensa che un clinico appena competente ritardi le sue decisioni fino al recupero delle informazioni, anche con mezzi alternativi. Quindi, le possibili conseguenze gravi sono bilanciate dalla bassa probabilità di verificarsi. Un caso simile verrebbe quindi inserito in classe C.

L'appendice C.3 di ISO/DTS 25238 contiene la descrizione dei gruppi di controlli applicabili nele diverse situazioni di rischio. Si tratta di un lungo elenco di misure, che va oltre lo scopo di questo capitolo.

ISO ha in sviluppo altre norme per la sicurezza informatica. ISO/NWIP/DTS #29321 Health Informatics (Application of Risk Management to the Manufacture of Health Software), ISO/NWIP/DTR #29322 (Health Informatics: Guidance on Risk Evaluation and Management in the Deployment and Use of Health Software) e ISO/TR 27809:2007 (Health informatics — Measures for ensuring patient safety of health software). Queste direttive si applicano al software sanitario, un settore in grande crescita.

Nella norma ISO/DTS o DTR #27809 (Health Informatics: Measures for Ensuring Patient Safety of Health Software, in inchiesta pubblica nel 2006) è interessante esaminare il contenuto del punto 8, dedicato alle misure da applicare per il controllo dei programmi software. Sono comprese, oltre a misure generali, la documentazione, l'evidenza clinica, la reportistica degli incidenti. Sono inoltre richiamati il sistema qualità, il controllo del progetto e la gestione dei rischi. Ciò a dimostrare la circolarità dei concetti e l'omogeneità dei diversi approcci per la sicurezza informatica.

CLSI AUTO11: IT Security

Il Clinical and Laboratory Standards Institute (CLSI) fornisce un fondamentale strumento di lavoro con il documento AUTO11-P—IT Security of In Vitro Diagnostic Instruments and Software Systems.

L'approccio CLSI, a differenza di ISO, è decisamente orientato all'individuazione pragmatica di misure per la sicurezza. Inoltre, è specificamente tagliato sulle esigenze dei laboratori di analisi cliniche. L'originalità principale è costituita dalla distinzione precisa dei compiti degli utenti e dei fornitori dei sistemi.

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.

i

Tabella XXX. Contenuto di CLSI AUTO11: IT Security

3 Delineation of Vendor and HCO Responsibilities 4 Technical Design Guidelines Related to Regulatory Requirements

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

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
5 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 HCO
5.6 Preventive Actions (software patches, virus definitions)
6 Applicability to Device Classes

Proviamo a richiamare qui una selezione delle raccomandazioni più interessanti di CLSI AUTO11 2006.

Il paragrafo 4.1 riguarda l'autorizzazione all'accesso dell'applicativo. Riguarda sia il personale del laboratorio che quello dell'assistenza tecnica, che agisce oggi in collegamento remoto. Va comunicata all'organizzazione che acquista il sistema e va differenziata a seconda del ruolo dell'operatore (amministratore, manutenzione, supervisore, operatore), con attenzione alle situazioni che coinvolgono operatori diversi per cambio turno o per il completamento di processi a più fasi.

In particolare, 4.1.1 prevede l'identificazione unica dell'operatore, 4.1.2 contiene i meccanismi di autenticazione: password, biometria, dispositivi (card o chiave), domanda/risposta (chiave e password), 4.1.3 contiene la gestione della password, la disattivazione al termine del servizio, la data di scadenza. 4.1.4 riguarda creazione e modifica della password, che dovrebbe rispettare alcuni criteri: lunghezza almeno otto caratteri, almeno un carattere alfabetico ed uno numerico, sensibilità al maiuscolo, controllo storico delle password precedenti. E' inoltre raccomandato di evitare nomi comuni, collegati a date di nascita o numeri di telefono, a disposizioni di caratteri nella tastiera, al nome di login. 4.1.5 contiene raccomandazioni su protezione e controllo delle password, che non devono essere trascritte in alcun modo, usate per funzioni diverse, condivise tra operatori. Va evitato l'abuso delle funzioni di recupero della password o di automatismi per l'inserimento. Le password compromesse vanno sostituite subito, comunque tutte vanno cambiate periodicamente, l'utente va bloccato in caso di ripetuti tentativi di accesso. Al punto 4.1.6 si prevede la procedura di accesso d'emergenza, in caso di evento catastrofico, che va notificata dal venditore e incorporata nelle procedure dell'organizzazione sanitaria, che individua i soggetti che la custodiscono ed i luoghi in cui viene tenuta. Infine 4.1.7 prevede l'interruzione automatica della connessione (Automatic Logoff) dopo alcuni minuti di inattività, 4.1.8 la registrazione degli accessi locali e remoti, 4.1.9 il controllo degli accessi al sistema operativo.

Il paragrafo 4.2 tratta della prevenzione delle intrusioni attraverso vie non ordinarie, ossia dispositivi hardware, di rete o altre porte d'ingresso. Tra questi (4.2.1) i programmi per sviluppo di applicazioni, le connessioni di rete (4.2.2, barriere e firewalls), le protezioni del BIOS (4.2.3) e altro. Da segnalare (4.2.5) l'autenticazione delle fonti di dati mediante meccanismi punto-a-punto o infrastrutture di chiave pubblica (firma digitale) e la criptazione dei dati in trasmissione (4.2.6). Quest'ultima funzione manca nelle principali specifiche di trasmissione dei dati (CLSI/NCCLS

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

document LIS2— Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems [già ASTM 1394], CLSI/NCCLS document POCT1—Point-of-Care Connectivity, and HL7). La trasmissione si può avvalere di crittografia, protocolli di sicurezza (come https) o di carico sicuro (secure payload), così come di connessioni fisiche sicure (i tradizionali cavi seriali). Per assicurare l'integrità dei dati (4.2.7) può utilizzare uno SHA-1 hash, una checksum (CRC minimo 16-bit), o una firma digitale. L'accesso fisico (lettori CD e chiave USB) va limitato (4.2.8) e le macchine vanno protette dai furti (4.2.9)

Per la protezione dai programmi maligni (4.3 Protection From Malicious Software) è elencabile una lunga serie di strumenti, firewalls, rilevatori di intrusione, antivirus, aggiornamenti dei programmi (patches) e notifiche degli incidenti. Esiste una guida FDA per i produttori, ritrovabile all'indirizzo http://www.fda.gov/cdrh/comp/guidance/1553.pdf. Particolare attenzione va posta durante trasporto e installazione dei sistemi (4.3.3) e l'uso dei computer per altre funzioni (4.3.5).

Fondamentale un'attività continua di sorveglianza e registrazione (4.4 Security Monitoring) che comprende (4.4.2) il Security Incident Reporting, la verifica di integrità dei dati (4.4.3) e dei programmmi applicativi (4.4.4), in cui si prevede firma digitale o equivalenti per i programmi software e per le copie di sicurezza dei dati (backup).

Un rischio tipicamente trascurato nei laboratori è quello della perdita di dati. Il paragrafo 4.5 di AUTO11 si occupa di questo, prescrivendo (4.5.1) il Data Backup, l'eliminazione dei singoli punti critici (4.5.2 Eliminate Single Points of Failure), ad esempio mediante ridondanza e sistemi di alimentazione in continuità, la gestione dei guasti (4.5.3 Fail Open).

Un computer che in caso di malfunzionamento impedisce l'accesso ai dati si dice che “fails closed”. Al contrario, quello che “fails open” permette l'accesso ai dati durante i guasti. Negli scenari medici, il secondo tipo è di gran lunga preferibile, per i rischi intuitivamente connessi alla mera mancanza di dati.

CEN EN 13606 EHRcom

La cultura della sicurezza si va diffondendo nella normativa tecnica informatica. Lo standard CEN EN 13606 “Electronic Healthcare Record Communication” (EHRcom) è basato sul precedente pre-standard (ENV 13606) e include molti concetti da openEHR. EHRcom diventa uno standard in cinque parti, costituite da 1. The Reference Model, 2. Archetype Interchange Specification, 3. Reference Archetypes and Term Lists, 4. Security Features, e 5. Exchange Models.

Come si vede , la parte EN 13606-4 (Electronic health record communication -Part 4: Security

requirements and distribution rules) è dedicata alla sicurezza.

Un esempio interessante di applicazione è rappresentato da EN 14484 - International transfer of personal health data (July 2003), in applicazione della direttiva EU sulla protezione dei dati personali. Nel paragrafo 9 sono contenute le politiche di sicurezza, distinte in tredici principi. Il principio 10 riguarda la sicurezza dei trattamenti, che prevede crittografia e firma digitale (entrambi) per la trasmissione tra stati diversi di dati sanitari. In particolare, sono specificate diverse linee guida, tra cui la numero due richiede la criptazione in trasmissione (cifrotesto), la numero tre

richiede integrità e autenticazione della fonte dei dati, la numero quattro autenticazione dell'accesso ai dati in lettura (Figura XXX).

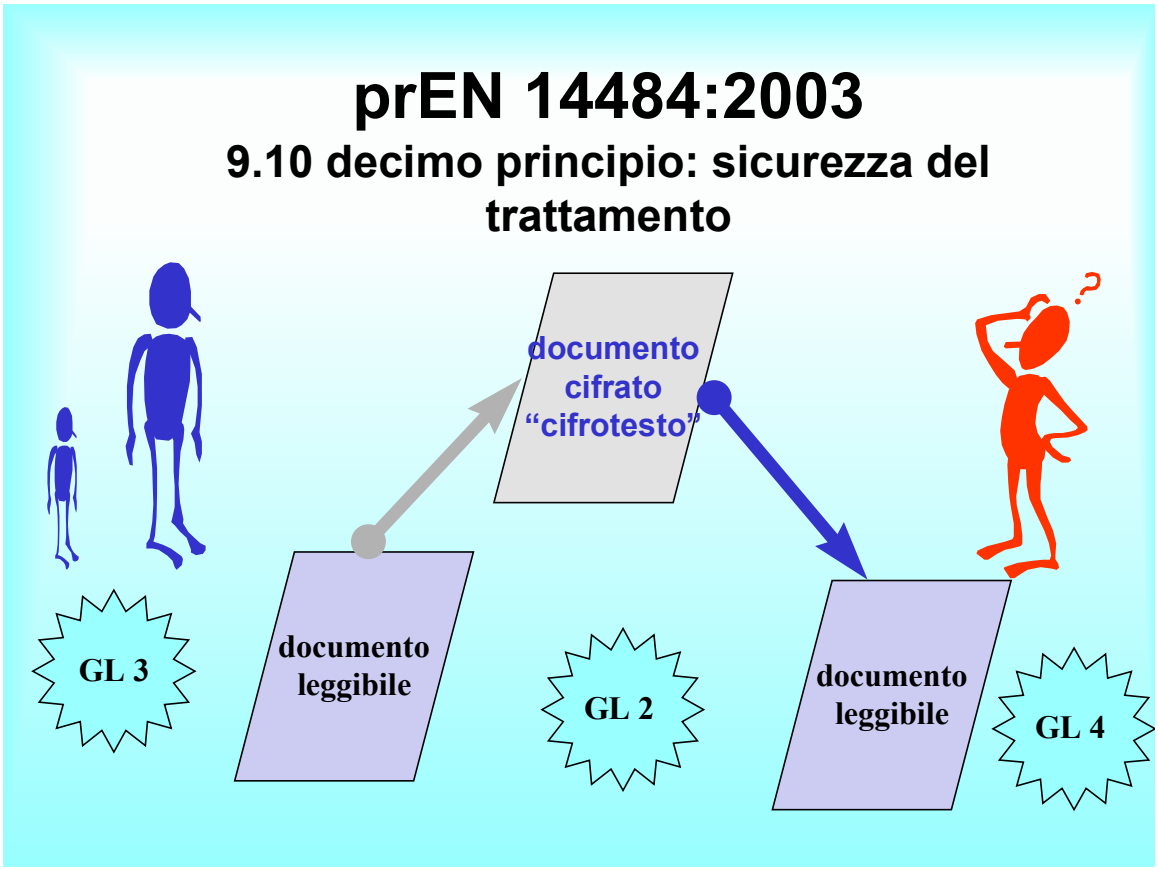


Figura XXX. Linee guida del decimo principio di EN 14484:2003 sulla sicurezza nel trasferimento dei dati.

STANDARD ISO 17090:2008

Fin dal 2005 ISO ha iniziato la revisione della precedente versione 2002 del pacchetto di norme tecniche sulla firma digitale. In inchiesta pubblica già nel 2006, sono state pubblicate in versione definitiva nel febbraio 2008.

Il pacchetto è in tre parti: Part 1: Overview of digital certificate services, Part 2: Certificate profile, • Part 3: Policy management of certification authority. A noi interessano le prime due.

ISO 17090-1:2008 definisce i concetti di base per l'uso di certificati digitali in campo sanitario e fornisce uno schema di interoperabilità per stabilire i requisiti di un certificato digitale in grado di garantire la comunicazione di informazioni sanitarie. Esso individua inoltre le principali parti interessate alla comunicazione di informazioni in materia di salute, così come i principali servizi di

sicurezza richiesti per la comunicazione in cui di richiedono i certificati digitali.

ISO 17090-1:2008 dà una breve introduzione alla crittografia a chiave pubblica e gli elementi di base necessari per la distribuzione di certificati digitali in materia di assistenza sanitaria. Essa inoltre introduce diversi tipi di certificato digitale, certificati di identità e associati certificati di attributo per utilizzatori, certificati di autorità di certificazione (CA), gerarchie di CA e strutture di transizione.

ISO 17090-2:2008 specifica i profili dei certificati necessari per lo scambio di informazioni sanitarie all'interno di una singola organizzazione, tra le diverse organizzazioni e tra i confini giurisdizionali. Dettaglia l'uso di certificati digitali nel settore sanitario e si concentra, in particolare, su specifici problemi sanitari in materia di profili dei certificati.

ISO 17090-3:2008 si occupa di gestione delle problematiche di attuazione e utilizzo di certificati digitali in sanità. Esso definisce struttura e requisiti minimi per il certificato di politiche (CPS) e una struttura per la pratica di certificazione associata. Questa parte è basata sulle raccomandazioni della informativa IETF / RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework e individua i principi necessari in una politica di sicurezza sanitaria per le comunicazioni in tratte transfrontaliere. Inoltre, essa definisce i livelli minimi di sicurezza richiesti, concentrandosi sugli aspetti peculiari delle cure sanitarie.

ISO 17090-1 qundi fornisce i concetti generali dei servizi di certificato digitale basati sulla crittografia. La crittografia (3.2.9) è la disciplina che incorpora principi e metodi per la trasformazione dei dati per nascondere il loro contenuto informatico, impedire la loro modifica e/o il loro utilizzo non autorizzato [ISO 7498-2:1989]. Applica algoritmi crittografici o “cipher” (3.2.10). La decrittazione (3.2.13) è il processo di ottenere da un cifrotesto i dati originali corrispondenti. [ISO/IEC 2382-8:1989]. Un cifrotesto (3.2.7) è costituito da dati prodotti con l'uso della cifratura (3.2.15), il cui contenuto semantico non è disponibile [da ISO 7498-2:1989]. La firma digitale (3.2.14) è invece un pacchetto di dati aggiunti oppure una trasformazione dell'unità di dati che permette al destinatario di provare la fonte e l'integrità dell'unità di dati e proteggere dalla contraffazione.

Con la crittografia simmetrica si usa una chiave segreta per criptare un testo e la stessa chiave per decifrarlo. Questo tipo di criptosistema è largamente usato per avere riservatezza.

La crittografia asimmetrica (3.2.3) invece usa chiavi diverse per cifratura e decifratura.

La crittografia a chiave pubblica è stata descritta per la prima volta da Whitfield Diffie e Martin Hellman nel 1976. L'approccio si avvale di due chiavi diverse, una pubblica e l'altra privata. Chiunque con la chiave pubblica può cifrare un messaggio, ma non decifrare. Solo la persona con la chiave privata può decifrare il messaggio. Non è possibile dedurre la chiave privata dalla conoscenza della chiave pubblica da sola e la chiave pubblica può quindi essere resa nota senza preoccupazioni per la riservatezza.

L'algoritmo asimmetrico RSA che prende il nome dai tre inventori (Rivest, Shamir e Adelman) è utilizzato da solo o in combinazione con la crittografia simmetrica. In tali sistemi ibridi, l'algoritmo asimmetrico è utilizzato per proteggere la chiave segreta del crittosistema simmetrico.

I sistemi asimmetrici sono in grado di aggiungere valore alla crittografia simmetrica o alle reti

private virtuali consentendo agli utenti di essere autenticati, l'integrità della comunicazione ed il controllo di accesso.

Alcuni algoritmi a chiave pubblica come RSA si usano per recuperare un messaggio e sono quindi adatti per la protezione di riservatezza. Questo algoritmo può essere usato anche nella direzione inversa, in cui un testo cifrato con la chiave privata può essere decifrato usando la chiave pubblica. Questo metodo non è adatto per la protezione di riservatezza, ma per l'autenticazione. Solo il possessore della chiave privata potrebbe produrre un crittogramma che può essere decifrato usando la chiave privata corrispondente. Questa caratteristica è quindi utile per autenticare l'origine dei messaggi da parte di chi fosse in possesso della chiave privata (Figura XXX).

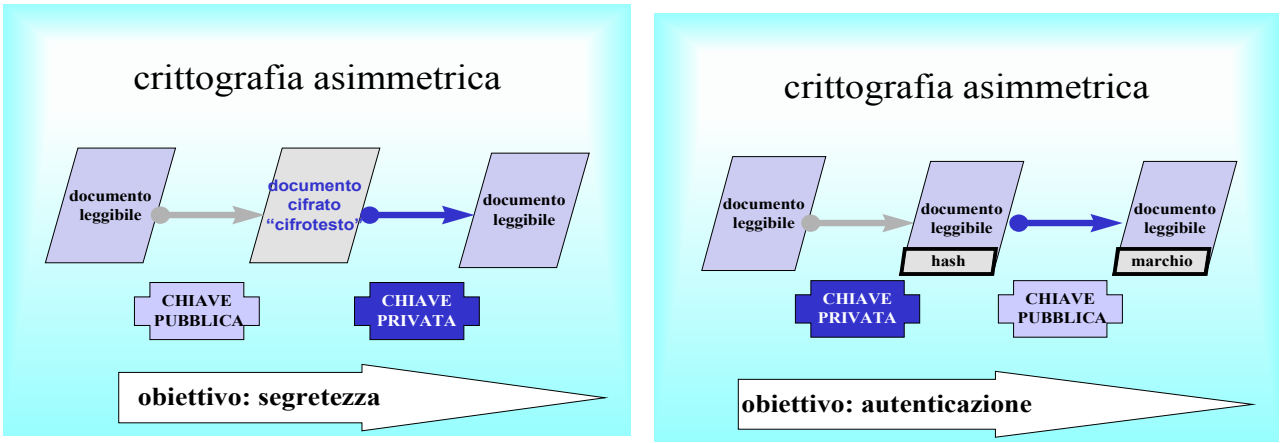


Figura XXX. Usi della crittografia asimmetrica per segretezza e autenticazione.

Un certificato digitale è una struttura software di dati che lega la chiave pubblica di un'entità e uno o più attributi relativi all'identità di tale entità. L'entità può essere una persona, una unità organizzativa, un'applicazione, un server o un dispositivo hardware. Lo scopo di un certificato digitale è quello di fornire un certo livello di fiducia che la chiave pubblica appartiene alla entità identificata e l'entità che possiede la chiave privata corrispondente.

I profili specifici per la sanità dei certificati digitali basati su International Standard X.509 e IETF/RFC 3280 sono quindi di vario tipo. Si distinguono i certificati "radice" per le autorità di certificazione, quelli subordinati e quelli "ponte" tra una autorità e l'altra. Quelli di "entità finale" sono invece attribuiti a individui, organizzazioni e dispositivi. Gli idividui possono essere sia professionisti sanitari registrati (iscritti ad un'Ordine) che non registrati, pazienti o consumatori, dipendenti di organizzaizoni di supporto (ditte di servizi o assistenza).

ISO/DTS N266:2002 (Health informatics – Security requirements for archiving and backup – – Part 1: Archiving of health records) fornisce un interessante esempio di applicazione dell'infrastruttura di chiave pubblica per un uso diverso dalla comunicazione, quello degli archivi. ISO/DTS N266 riconosce nel paragrafo 6.17 il "marchio" dei documenti elettronici del paziente, affermando che essi dovrebbero essere contrassegnati con la firma elettronica. L'integrità dei dati marchiati è verificata dalla "firma", tipicamente quella di un professionista sanitario, con un marchio personale

che contiene informazioni sul ruolo professionale, sia quello individuale (es. specialista) che quello attribuito dalla organizzazione (es. assistente di Medicina Interna). Il marchio deve contenere un "timbro" temporale. ISO/DTS N266 prevede però anche al punto 6.18 la firma istituzionale come . . "firma" dell'organizzazione, tipicamente utilizzata come "firma" dell'archivio. Se utilizzata per una verifica esterna assume la veste di archivio "notarile". Essa inoltre può sostituire la firma professionale.

Nella Appendice A8 di ISO/DTS N266 si rappresenta l'esempio di un archivio con firma digitale sottoposto a conversione strutturale, da formato HL7 a formato XML. Il nuovo documento incorpora quello vecchio e la sua firma ma anche il marchio della persona o del programma che effettua la conversione.

Un esempio di applicazione di firma digitale istituzionale è descritto da Takeda e collaboratori (Takeda H et al. Healthcare public key infrastructure (HPKI) and non-profit organization (NPO): essential for healthcare data exchange. Int J Med Inform 2004;73:311-6) della Osaka University. Takeda inserisce i risultati di laboratorio in contenitori multi-uso con firma digitale, inoltre accantona l'idea di firmare ciascun singolo rapporto.

http://www.interlex.it/forum10/relazioni/46mc.htm

http://www.interlex.it/forum10/relazioni/13ricchiuto.htm

http://www.interlex.it/docdigit/codicepa5.htm

http://www.interlex.it/docdigit/nuovoreg2.htm

http://www.interlex.it/docdigit/corrado9.htm

http://www.interlex.it/forum10/relazioni/28neirotti.htm

http://www.interlex.it/docdigit/confuse.htm

Una descrizione completa della normativa italiana sulla firma digitale va oltre gli scopi di questo capitolo. Tuttavia, va detto che l'Italia si è posta all'avanguardia nell'uso legale della firma digitale, essendo il primo paese ad avere attribuito piena validità giuridica ai documenti elettronici. Fin dal 1997 l'articolo 15 della L. 59/97 stabilisce infatti che "gli atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge".

La normativa pre-direttiva sulla firma digitale, la firma elettronica e la conservazione del documento elettronico, prevedeva un'unica tipologia di certificato, di certificatore e di firma digitale. Con il recepimento della Direttiva 1999/93/CE e l'emanazione del D. lgs n. 10/02 e del DPR 7 aprile 2003 n. 137, il quadro normativo di riferimento ha subito una profonda trasformazione; in particolare, l'articolo 6 del decreto di recepimento ha modificato l'articolo 10 del DPR n. 445/00, stabilendo che il documento informatico (da intendersi, ai sensi del Testo unico del 2000, come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti e, quindi, non recante alcuna sottoscrizione elettronica), ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile. Con l'entrata in vigore del Codice dell'amministrazione digitale (gennaio 2006), attraverso il Decreto legislativo 7 marzo 2005, n. 82, il valore probatorio del documento informatico

ha subito una ulteriore modifica, difatti con il comma 2 dell'articolo 21, come modificato dal D.Lgs. 4 aprile 2006, n. 159, è stabilito che "Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria. ". Il citato decreto legislativo rivede anche le tipologie di firma elettronica previste contemplando tre tipologie di firma:

- firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
- firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
- firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le norme continuano a contemplare due tipologie di certificato (qualificato e non qualificato) e tre di certificatore (che rilascia certificati qualificati: accreditato o notificato; che rilascia certificati non qualificati). Istanze e dichiarazioni inviate per via telematica da e verso la PA sono valide se sottoscritte mediante firma digitale basata su un certificato qualificato rilasciato da un certificatore accreditato e generata mediante un dispositivo sicuro per la creazione di firme elettroniche.

Con la pubblicazione del DPCM del 13 gennaio 2004 (G. U. 27 aprile 2004, n. 98) sono state emanate le regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione, anche temporale, dei documenti informatici. Il provvedimento disciplina la formazione della documentazione amministrativa tramite il supporto informatico, con particolare attenzione per la generazione, apposizione e verifica delle firme digitali. Viene quindi portato a compimento il recepimento della Direttiva europea 1999/93/CE. Con l'entrata in vigore di queste regole tecniche viene abrogato il DPCM 8 febbraio 1999.

Sulla gazzetta ufficiale n. 51 del 3 marzo 2005 sono state infine pubblicate le "Regole per il riconoscimento e la verifica del documento informatico", attraverso la Deliberazione CNIPA n.4 del 17 febbraio 2005, emanate ai sensi del comma 4 dell'articolo 40 del DPCM 13 gennaio 2004.

Queste ulteriori regole sono fondamentali per garantire l'interoperabilità della firma digitale, cioè la possibilità di verificare qualunque firma digitale con qualsiasi software di verifica purché conformi alle medesime regole. Per tale ragione il rispetto delle stesse è obbligatorio da parte dei certificatori accreditati.

http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Firma_digitale/

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

http://www.genghinieassociati.it/italiano/Presentazioni/chisiamo.htm

http://www.corriere.it/Primo_Piano/Economia/2006/06_Giugno/26/notaio.shtml

http://www.pki.org.tw/pkiforum2005/d_file/02_Riccardo%20Genghini.pdf genghiniESclumpsy

Per riepilogare, la protezione del documento dalla falsificazione si ricollega ad alcuni articoli del codice civile, sia il documento cartaceo che digitale (Tabella XXX).

Tabella XXX. Relazione tra codice civile e protezione dei documenti

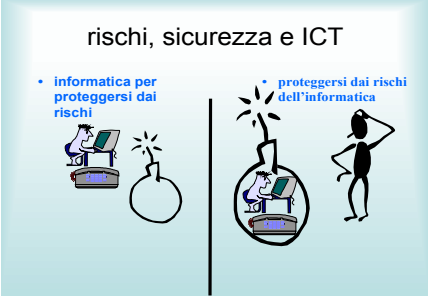
livello sicurezza	documento cartaceo	Documento elettronico
minimo	Codice civile Art. 2712 Riproduzioni meccaniche	Idem, D. lgs n. 10/02 e del DPR 7 aprile 2003 n. 137
intermedio	Codice civile Art. 2702 Efficacia della scrittura privata. Sottoscrizione.	Direttiva 1999/93/CE 13 dicembre 1999 (G.U. delle Comunità europee L. 13 del 13 dicembre 1999). Comma 2 art. 5. Firma elettronica "leggera". D.Lgs. 4 aprile 2006, n. 159
elevato	Codice civile Art. 2703 Sottoscrizione autenticata	DPCM 13 gennaio 2004. (GU n. 98 del 27 aprile 2004) Firma digitale (elettronica "forte")

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

correzione, verifica e validazione dei risultati

Dopo aver preso in considerazione i rischi generati dall'informatica per la sicurezza dei pazienti, ora è il turno dell'impiego dell'informatica per proteggere il paziente da altri rischi.



il ciclo richiesta-risposta

L'immagine tradizionale del ciclo operativo di un laboratorio medico, chiamato anche ciclo diagnostico o schema di Lundberg, ha la classica forma circolare chiusa, che parte dal cervello del medico, formulante il quesito diagnostico, passa dal prelievo e dalla fase analitica,

In ogni passaggio di questo ciclo potremmo aprire un capitolo informatico: la prescrizione computer assistita (CPOE), la comunicazione nel sistema informatico ospedaliero (HL7) e del laboratorio (CLSI AUTO3), la comunicazione tra strumenti analitici e sistema informatico (CLSI LIS01 ISO18812) ed infine il recapito dei risultati ancora nel sistema informatico sanitario (WEB).

Da qualche tempo circola però un inquietante interrogativo, espresso originariamente con il motto "The Request-Report Cycle: Are the wheels coming off?" da Jonathan Kay di Oxford, nel convegno CPD4IT 'Getting ahead of the IT Curve", 18 October 2004.

Jonathan Kay descrive una realtà di cambiamenti ineluttabili fuori dal nostro controllo, conseguenti alla crescita di alcune forme di discontinuità nelle cure mediche. Nuovi modelli assistenza, riduzione delle ore di lavoro, passaggio di mansioni da medici a infermieri, presenza di clinici con meno esperienza ma più accreditamento formale e necessità di apprendimento continuo, passaggio di meccanismi decisionali dall'arbitrio dei clinici agli schemi dei protocolli, di cui solo alcuni basati su evidenza. Infine, si fanno decisamente più esami per paziente e per anno. La trasmissione dei

risultati presenta sempre di più alcuni aspetti critici, rappresentati da correttezza del recapito (alla persona giusta nel tempo giusto?), responsabilità dei risultati, mezzo di trasmissione, tempestività e suo controllo, correttezza dell'interpretazione. L'informazione prodotta dai laboratori è sempre di più una combinazione di risultati e conoscenza, l'accesso varia dalla tradizionale carta al computer al browser per intranet. Ci si interroga sulla convenienza di un meccanismo tipo “spedizione” (push) o “scarico” (pull), specie quando per la rotazione del personale si mette a repentaglio la continuità assistenziale. Ci si chiede come gestire i fenomeni di “escalation”, sia quelli dovuto all'aggravamento delle condizioni del paziente (si pensi all'emocoltura positiva) che alla necessità talvolta di prendere contatto col medico curante invece dell'infermiera di turno. In un contesto in cui si diffondono rapidamente strumenti come i dispositivi mobili di comunicazione.

Laura C. Hanson, MD, MPH; Mary Ersek, PhD, RN. Meeting Palliative Care Needs in Post–Acute Care Settings "To Help Them Live Until They Die" JAMA. 2006;295:681-686.

Jonathan Kay. Clin Chem Lab Med 2006;44(6):719–723

Una rappresentazione realistica e moderna delle attività svolte nei laboratori medici secondo lo standard stato dell'arte è fornita dalla “CAP Checklists”, ossia quello che la COMMISSION ON LABORATORY ACCREDITATION del LABORATORY ACCREDITATION PROGRAM del College of America Pathologists (www.cap.org) ha elaborato per guidare le visite ispettive nei laboratori.

Nelle checklists sono previsti diversi casi di trasmissione dei risultati non “deragliata” rispetto al tradizionale ciclo richiesta-risposta. Ad esempio, MIC.15000 prevede “preliminary reports” per i risultati degli esami colturali (anche dal miscroscopico diretto o dalla prima lettura delle piastre) quando sono clinicamente significativi, seguiti poi dai risultati completi e definitivi.

La notifica immediata è invece obbligata da MIC.15150, quanto i risultati superano i limiti di allarme importanti per le pronte decisioni nella gestione del paziente. Anche l'operatore al banco deve essere familiare con i limiti di allarme. Lo stesso è prescritto da MIC.15200, che aggiunge la necessità di documentare eventuali difficoltà nella trasmissione e le misure prese per evitare il ripetersi del problema. Il registro delle notifiche comunque contiene data, ora, operatore responsabile, persona che raccoglie la segnalazione, risultato dell'esame. GEN.41320, che contiene il medesimo concetto, aggiunge che i limiti di allarme vanno definiti in concertazione con i clinici a cui sono destinati.

Esistono alcuni casi particolari considerati nelle CAP checklists. MIC.22100 prevede uno striscio colorato col gram dei campioni respiratori (espettorato) per decidere se proseguire con l'esame colturale. A seguire, MIC.22110 stabilisce che il campione non accettabile venga immediatamente riferito al clinico che può nel caso disporre una nuova raccolta. MIC.22510 contiene la prassi di riferire i risultati positivi dell'esame microscopico del liquido cefalo-rachidiano, come fosse un risultato di allarme. Lo stesso dice MIC.22620 per le emocolture, senza attendere l'identificazione del microorganismo, MIC.22710 per il gram sui campioni delle ferite e MIC.31200 per i bacilli acido-alcol resistenti entro 24 ore dall'accettazione.

ISO 15189 afferma nelle definizioni introduttive che i servizi di laboratorio medico comprendono funzioni per validazione, interpretazione e trasmissione dei risultati nonché consulenza.

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Il punto 4.2 della norma (Quality management system) contiene l'affermazione 4.2.4 che il manuale di qualità contiene alla lettera (p) le procedure di validazione dei risultati.

Purtroppo, la nozione di validazione qui introdotta, con le migliori intenzioni, non appare conforme alle definizioni delle norme di riferimento. Ciò comporta alcuni inconvenienti pratici di importanza non trascurabile.

Validazione secondo ISO 9000 (ma anche secondo la precedente ISO 8402 ed una serie di norme correlate) è la conferma con evidenza oggettiva che siano soddisfatti requisiti per l'uso specificatamente previsto. **Verifica** invece è la conferma con evidenza oggettiva che siano soddisfatti requisiti previsti, generalmente nella fase di sviluppo.

Sembrano la stessa cosa, ma non lo sono affatto. La validazione comporta una relazione con gli utilizzatori del prodotto o servizio, nel nostro caso un collegamento alla storia clinica ed alle conseguenze assistenziali nello specifico caso del risultato di laboratorio. La verifica comporta solo un confronto con criteri interni prestabiliti. Con un aforisma si dice validazione “fare la cosa giusta” mentre verifica sarebbe “fare la cosa in modo giusto”.

Medical devices The FDA (21 CFR) has validation and verification requirements for medical devices. . See guidance: [2] and ISO 13485

Clinical laboratory medicine: ISO 15198:2004 Clinical laboratory medicine --In vitro diagnostic medical devices -- Validation of user quality control procedures by the manufacturer

Quality Management and Quality Assurance -Vocabulary-ISO 8402:1994 (reference only, obsoleted by [8] ANSI/ISO/ASQ Q9000-2000 (U.S. version ISO 9000:2000);

– [2] FDA Medical Device Quality Systems Manual -The Quality Systems regulation

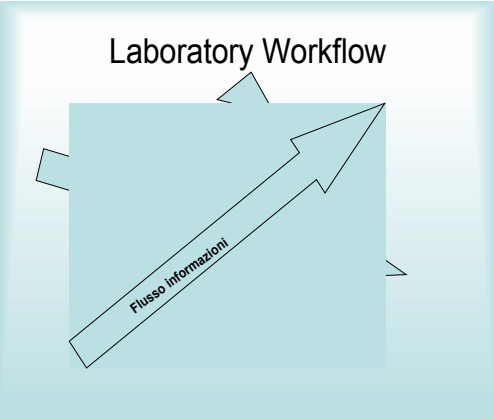
ISO 15189 prevede al punto 3.9 le procedure post-esame o fase post-analitica. Si tratta dei processi che seguono l'esame vero e proprio e comprendono la revisione sistematica, la formattazione e l'interpretazione, l'autorizzazione per il rilascio e la trasmissione dei risultati, nonché infine la conservazione dei campioni per eventuali altri esami o riesami.

Il flusso operativo del laboratorio secondo CLSI GP26 – Laboratory Workflow contiene nella fase analitica la revisione e l'interpretazione di laboratorio del risultato analitico. CLSI AUTO10-P Vol. 26 No. 4 Autoverification of Clinical Laboratory Test Results; Proposed Guideline indica la posizione nel flusso delle attività di verifica, collocandole sia nella fase di esame che in quella post-esame.

In definitiva, dallo studio di queste linee guida ricaviamo che mentre il flusso dei campioni nel laboratorio medico è monotonico, quello delle informazioni può assumere diverse direzioni (Figura XXX).

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*



.

CLSI AUTO10-P Autoverification of Clinical Laboratory Test Results; Proposed Guideline fornisce una chiara rappresentazione del processo di revisione e correzione dei risultati. Ripropone la differenziazione, mai abbastanza evidenziata, tra verifica e validazione. Testualmente, per AUTO10 la **verifica** di un risultato è un processo conosciuto con una varietà di nomi, come ad esempio verifica, accettazione o rilascio dei risultati del personale di laboratorio, in modo tale che i risultati stessi siano resi disponibili o accessibili ai curanti esterni al laboratorio, come ad esempio medici, infermieri, etc .; NOTA: implica che i risultati siano stati esaminati e soddisfino i criteri di qualità stabiliti dal laboratorio e possano essere utilizzati per il trattamento e la gestione dei pazienti. **Autoverifica** (verifica automatica dei risultati) sono le azioni automatizzate eseguite da un sistema di computer connessi con l'emissione dei risultati degli esami per la cartella clinica, utilizzando criteri e logiche stabilite, documentate e provate dal personale medico del laboratorio; NOTA: I criteri possono essere semplici o complessi e coinvolgono molti diversi parametri. Il sistema offre i più alti livelli di consistenza e la capacità di gestire complessi algoritmi in un modo molto efficiente.

Che sia manuale o automatica, AUTO10 dà per scontato che una verifica ci sia. Il College of American Pathologists (CAP), riferimento indiscutibile per le prassi professionali, riporta nelle "Checklists" alcuni interessanti concetti. Innanzitutto, tra gli obiettivi dedicati alla sicurezza del paziente ("CAP PATIENT SAFETY GOALS") include tra gli altri "...il miglioramento della verifica e della comunicazione delle informazioni "salvavita" (neoplasie, valori critici), ... migliorare l'identificazione, la comunicazione e la correzione degli errori...". Non bastasse, il CAP raccomanda che l'ispettore ponga particolare attenzione ai punti collegati agli obiettivi di sicurezza del paziente.

Un'approfondimento esaustivo del tema degli errori in laboratorio va oltre gli scopi di questo capitolo. Tuttavia possiamo ricordare, ricavandoli da una vasta letteratura, alcuni dati significativi. Si stimano gli errori in "unità per milione" (ppm) al livello di 700 ppm per le attività analitiche comuni, 7000 circa per la microbiologia, 500 per la trasmissione dei risultati. Dei 500 ppm, solo 41 ppm avrebbe effetti significativi sulle cure mediche. Altri stimano 1100 ppm su pazienti ambulatoriali.

La cosa interessante è che questi valori, pur bassi, sono tutti superiori alla soglia di 3 ppm nota come "6 sigma", ossia la soglia psicologica di percezione di affidabilità di un servizio.

• Nevalainen D, Berte L, Kraft C, Leigh E, Picaso L, Morgan T. Evaluating laboratory performance on quality indicators with the six sigma scale. Arch Pathol Lab Med. 2000;124:516-9

• Witte DL, VanNess SA, Angstadt DS, Pennell BJ. Errors, mistakes, blunders, outliers, or unacceptable results: how many? Clin Chem. 1997 Aug;43(8 Pt 1):1352-6.

• Nutting PA, Main DS, Fischer PM, et al. Problems in laboratory testing in primary care. JAMA. 1996;275:635-639

Desjarlais F. Intérêt de la validation informatique finale des rapports de biochimie générale. Annales de biologie clinique du Québec. 2000;38:7 -13

Non ci sono molti dati sull'impatto delle attività di verifica sul carico di lavoro ed i tempi di risposta del laboratorio. Una di queste (SPEEDING ACCURATE DIAGNOSIS BY IMPROVING LABORATORY TURNAROUND TIME AND RESULT QUALITY. Uettwiller-Geiger, D. · Clinical Chemistry Department, John T. Mather Memorial Hospital · Port Jefferson, NY. www.matherhospital.org/NPSFPoster.html) ha rilevato il tempo della verifica post-analitica è superiore alla somma dei tempi analitici e pre-esame.

Dal complesso delle CAP Checklists si ricavano alcuni principi cardinali per la gestione degli errori in laboratorio: • verifica (no "validazione"), • verifica manuale e autoverifica, • divisione delle mansioni (operatore, supervisore tecnico, supervisore generale), • selezione e flusso parallelo, ciclo in 24 ore. Nelle liste si trovano diversi punti collagati a verifica e correzioni, riassunti nella tabella XXX.

Tabella XXX. CAP checklists per gestione errori

• detect and correct clerical and analytical errors CHM.10800
• unusual or inconsistent results MIC.21950 GEN.20364
• revised reports, revised and original data, multiple sequential corrections GEN.41308 GEN.41310 GEN.41312
• calculations reviewed GEN.43450
• absurd values GEN.43600
• specimen quality GEN.43750
• result entries verified GEN.43825
• results falling outside the AMR limits CHM.15400
• who may use the computer system GEN.43150
• individuals who have entered and/or modified patient data GEN.43800
• technical supervisors GEN.53500
• general supervisor GEN.53700
• organizational chart GEN.54000
• competency of each person GEN.55500
• identity of the analyst GEN.41306
• 24 hours review CHM.10900
• autoverification GEN.43850 GEN.43875 GEN.43878 GEN.43881 GEN.43884 GEN.43887 GEN.43890 GEN.43893

GEN.20364 richiede il monitoraggio delle variabili post-analitiche, che comprendono l'esattezza della trasmissione tra interfacce elettroniche.

GEN.43600 richiede la disponibilità di tabelle per catturare valori assurdi, con registrazione del processo di verifica.

GEN.43825 richiede la verifica dei dati inseriti manualmente ed automaticamente prima dell'accettazione finale. Un esempio di verifica è il confronto con intervalli analitici e valori critici, da parte di operatori autorizzati, eventualmente diversi da chi ha fatto l'esame.

Anche CHM.10800 richiede un meccanismo per trovare gli errori e consentirne la correzione. Tipicamente la revisione è fatta da da un supervisore o da un patologo, ma non è obbligatoria su tutti i risultati prodotti. Aiuta anche l'uso selettivo dei delta-checks, ossia del confronto con i dati precedenti per lo stesso paziente. Gli errori vanno corretti tutti, anche quelli rilevati dagli utenti.

REFERENCE: Dufour D, et al. The clinical significance of delta checks. Am J Clin Pathol. 1998;110:531.

MIC.21950 si riferisce alla rilevazione di risultati microbiologici insoliti o inconsistenti. Ad esempio, E. coli resistente all'impienem, Klebsiella sensibile all'ampicillina, Proteus mirabilis invece resistente all'ampicillina, stafilococco resistente alla vancomicina.

GEN.41308 dispone che tutti i risultati vengano corretti in tutti i rapporti previsti (carta, video, trasmissioni, etc..). Si possono trascurare gli errori tipografici minori senza valore clinico. Deve essere chiaro il risultato corretto rispetto al precedente errato.

Per GEN.41310 i risultati originali devono restare accessibili per confronto, mentre per GEN.41312 eventuali correzioni multiple devono essere riportate in sequenza.

GEN.43450 richiama l'attenzione sui calcoli, disponendo che vengano rivisti uno per uno almeno una volta l'anno o dopo una variazione nel sistema.

GEN.43750 si preoccupa che vengano consentiti commenti sulla qualità del campione, quando significativa (emolizzato, lipemico, scarso, etc..).

Per CHM.15400 i risultati non compresi nell'intervallo analitico (analytical method range, AMR), senza diluizione, concentrazione o pretrattamento, vanno ripetuti prima della trasmissione. A meno che non siano riportati come inferiore al limite o superiore al limite e ci sia evidenza che non siano effetto di errori di diluizione o di “effetto gancio” immunologico. CHM.15500 aggiunge la necessità di stabilire protocolli di diluizione o concentrazione se l'intervallo clinico supera quello analitico.

GEN.43150 identifica la necessità di documentare chi usa il sistema informatico per inserire dati dei pazienti. GEN.43800 conferma quest'obbligo, estendendolo ai casi di inserimento multiplo ed ai meccanismi di autoverifica nonché ai point-of-care, dove chi esegue può non essere chi inserisce.

GEN.41306 introduce l'identificazione del tecnico che esegue o completa l'esame nonché la sua data. GEN.53500 aggiunge al primo operatore un supervisore tecnico, con le responsabilità definite da CLIA-88. GEN.53700 aggiunge ai primi due un supervisore generale, con le opportune caratteristiche. GEN.54000 infine prevede un organigramma che descriva le relazioni tra proprietà o direzione, supervisione generale, supervisione tecnica. Per GEN.55500 si devono verificare le

competenze dei singoli operatori.

La suddivisione dei compiti di verifica disegnata dal CAP si articola dunque su tre livelli: tecnico esecutore (stazione analitica, GEN.41306) che usa allarmi strumentali, controllo di qualità interno, limiti di allarme / delta check; supervisore tecnico (settore, GEN.53500), che si avvale di segnali da dal tecnico esecutore, risultati complessivi delle serie, risultati interlaboratorio; supervisore generale (intero laboratorio, GEN 53700) che lavora con segnali da supervisore tecnico, risultati complessivi del paziente, protocolli clinici. Questo schema ha un ovvio inconveniente: se applicato in modo rigido, può allungare molto i tempi di risposta. Il CAP introduce così come correttivo la regola delle 24 ore (CHM.10900). Per CHM 10900, in assenza dei supervisori, il risultato viene rilasciato senza indugi, riservandosi la verifica (eventuale, non per tutti i dati) nell'arco delle successive 24 ore (Figura XXX).

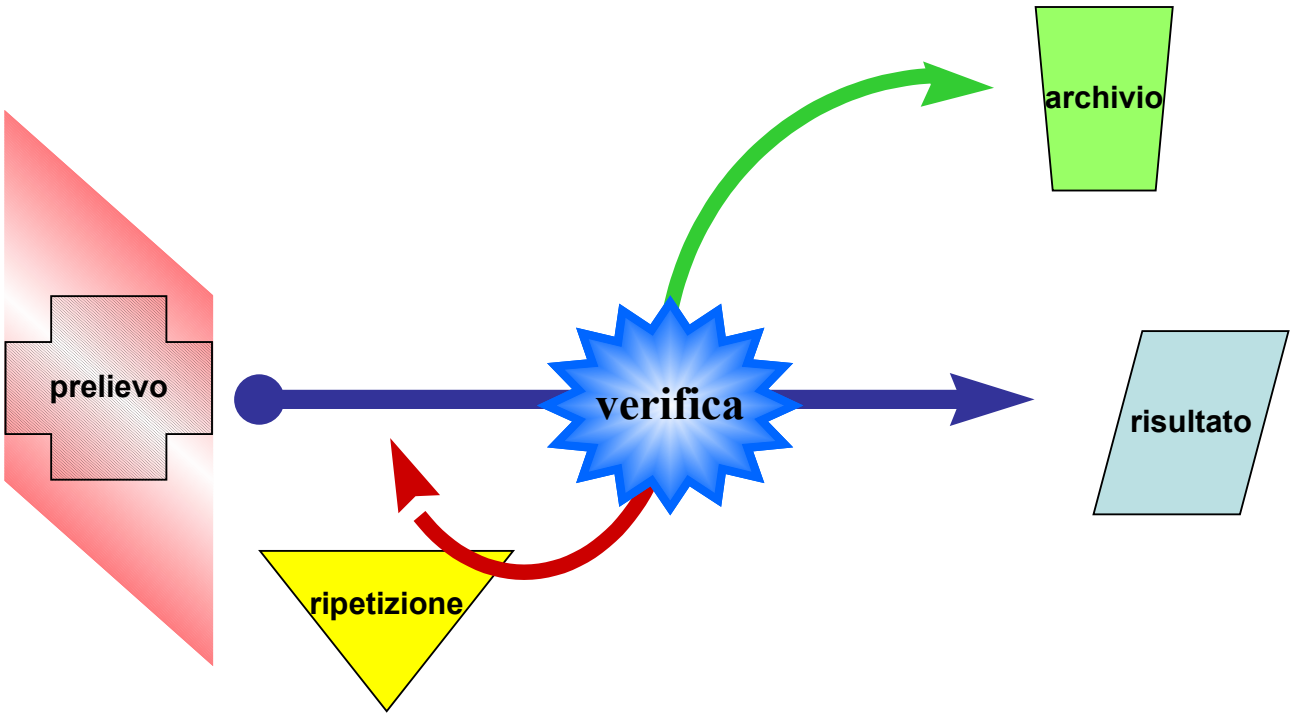


Figura XXX: flusso dei risultati degli esami di laboratorio

Middleware per autoverifica - ISO - EN 12967

Oggi il numero 12967 significa la stessa cosa per ISO e CEN. ISO 12967-3 è stato preparato da CEN (come EN 12967-3) ed è stato sottoposto per l'approvazione, secondo una procedura speciale veloce (“fast-track procedure”), dal Technical Committee ISO/TC 215, Health informatics, in parallelo con la sua approvazione dagli organismi centrali ISO.

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

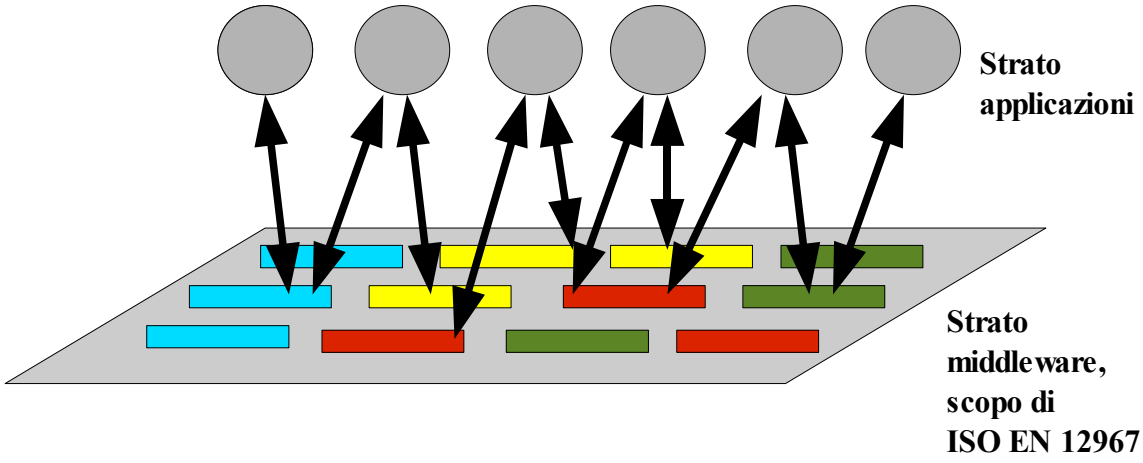


Figura XXX: architettura del middleware, da ISO EN 12967, modificata

ISO EN 12967 ha un titolo semplice (Health informatics — Service Architecture, abbreviato HISA) ed è diviso in tre parti: - Part 1 Punto di vista aziendale, con le caratteristiche generali dell'architettura le specifiche metodologiche ed i criteri di conformità; - Part 2 Punto di vista informativo, dove si trova la semantica fondamentale del modello informatico realizzato con il middleware per integrare i dati comuni dell'organizzazione; - Part 3 Punto di vista computazionale, con i servizi che devono essere forniti dal middleware per permettere l'accesso ai dati comuni come pure l'esecuzione delle logiche che sostengono i processi aziendali.

Middleware è uno strato di architettura informatica che integra i dati comuni ed i processi logici, distinto dalle applicazioni individuali ed accessibile in tutto il sistema informatico (Figura XXX).

I riferimenti generali del middleware si trovano in ISO/IEC 23004-1:2007 (Information technology -- Multimedia Middleware -- Part 1: Architecture) e negli altri documenti della serie ISO 23003 (fino a ISO/IEC 23004-7:2008, Information technology -- Multimedia Middleware -- Part 7: System integrity management).

Possiamo avere un'idea del contenuto di questi standard: in ISO EN 12967-3:2006 (Health informatics -Service architecture -Part 3: Computational viewpoint) si riconoscono due principali paragrafi, 5 principi metodologici e 6 caratteristiche generali del modello. Nel paragrafo 5 troviamo argomenti come 5.1 Clusters di oggetti, 5.2 linguaggio computazionale, 5.3 oggetti computazionali e interfacce, 5.4 interazioni. Nel successivo invece si trattano 6.1 i due tipi di oggetti computazionali, i dettagli di 6.2.2 “Add” basic methods, 6.2.3 “Update” basic methods, 6.2.4 “Delete” basic methods, 6.2.5 “Detail” basic methods, 6.2.6 “List” basic methods, le interfacce (6.3 General purpose interface). Le interfacce sono poi approfondite in 6.4 (The complex interfaces of the workflow related computational objects) e in particolare in 6.4.2 (“Subject of Care Workflow”), 6.4.3 (“Clinical Information workflow”), 6.4.4 (“Activity Management workflow”).

Esempi elementari ma concreti di logiche di middleware si trovano nel materiale pubblicato come AACC's Middleware Library (indirizzo aggiornato: http://apps.aacc.org/labrules/index.cfm). Tra gli esempi nella AACC's Middleware library troviamo la gestione delle discrepanze tra risultati di TSH e Free T4, regole di ematologia per identificare il campione che necessita di esame microscopico,

regole per il confronto longitudinale mediante Delta Check.

Autoverifica nelle liste di riscontro del College of American Pathologists

Una importante applicazione di tecniche informatiche nella verifica dei risultati è appunto la verifica automatica (autoverifica), puntualmente trattata nelle liste di riscontro (Checklists) del College of American Pathologists (CAP), usate per le visite ispettive nell'accreditamento dei laboratori medici.

L'argomento è stato introdotto nelle Checklists nel 2005, formando un intero capitolo. Autoverifica è definita come il processo in cui i risultati dei pazienti sono generati dagli strumenti collegati e mandati al sistema informatico (LIS), dove sono confrontati con parametri di accettabilità definiti dal laboratorio. Se i risultati ricadono all'interno di questi parametri definiti, essi sono automaticamente rilasciati per la trasmissione senza altri interventi degli operatori, mentre se cadono al di fuori sono trattenuti per il riesame da parte del personale del laboratorio. Il processo è innanzitutto investigato dalla regola GEN.43850 che prevede “politiche” di autoverifica, firmate dal direttore,

1) Davis GM. Autoverification of the peripheral blood count. Lab Med. 1994;25:528-531; 2) Davis GM. Autoverification of macroscopic urinalysis. Lab Med. 1999;30:56-60;

3) Nicoli M, et al. The use of the Sysmex Co. data processing software program (PC-DPS) for the automatic validation of haematological data. Clin Chem. 2000;46:A133;

4) NCCLS. Laboratory automation: communications with automated clinical laboratory systems, instruments, devices, and information systems; proposed standard AUTO3-P. Wayne, PA: NCCLS, 1998;

5) Duco DJ. Autoverification in a laboratory information system. Lab Med. 2002;33:21-25.

La regola GEN.43878 poi stabilisce che l'autoverifica sia collegata al controllo di qualità interno. Il computer verifica i risultati del controllo prima dell'autoverifica, che viene disabilitata manualmente se il controllo di qualità non fornisce risultati accettabili. La regola GEN.43881 cerca la presenza di intervalli appropriati di valori di accettabilità per trovare i valori assurdi, impossibili o critici che richiedono interventi manuali (ripetizioni, diluizioni, telefonate, etc..). Secondo GEN.43884 i risultati, prima dell'autoverifica, devono essere controllati per la presenza di allarmi. La presenza di un allarme non impedisce in assoluto l'autoverifica, ma allarmi non riconosciuti comportano il blocco del risultato per la revisione manuale. La regola GEN.43890 prevede l'utilizzo dei criteri di delta checks, ossia dei confronti con risultati precedenti, gli stessi utilizzati manualmente.

GEN.43875 richiede poi la documentazione della validazione iniziale dell'autoverifica. GEN.43887 prevede che nel sistema informatico venga tenuta traccia dell'autoverifica con data e ora. Per GEN.43893, infine, serve una procedura per la rapida sospensione dell'autoverifica in caso di problemi con i metodi di analisi, gli strumenti o lo stesso programma di autoverifica.

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Altri Riferimenti per autoverifica

L'autoverifica ha diversi riconoscimenti ufficiali. Oltre alle regole CAP citate, negli USA anche FDA prevede criteri per l'autoverifica. Lo Stato della California fece una legge, Assembly Bill 2156 del 18 settembre 2006, applicato il 1 gennaio 2007. La legge è inserita nel Business and Professions Code (BPC) 1209.5 e autorizza i laboratori ad unsare l'autoverifica per rilasciare i risultati degli esami. Questa legge cancella il precedente regolamento vecchio di 30 anni Department of Health Services 17CCR 1050 (h)) che richiedeva che tutti i risultati di laboratorio siano revisionati criticamente da un addetto con adatta qualifica prima di essere comunicati.

In letteratura si trovano alcuni resoconti di imprese per l'installazione in laboratori medici di sistemi di autoverifica. Richard S. Seaberg, MT(ASCP), Administrative Director North Shore, University Hospital Long Island Jewish Medical Center, racconta la propria esperienza in diversi interventi:

http://www.clinchem.org/cgi/content/full/46/5/751

Richard S. Seaberg1, Robert O. Stallone1,a and Bernard E. Statland2. (Clinical Chemistry. 2000;46:751-756.) The Role of Total Laboratory Automation in a Consolidated Laboratory Network.

http://www.aacc.org/SiteCollectionDocuments/Divisions/lis/presentations/AACCAutoverificationPresentationRev4.pdf

http://www.aacc.org/SiteCollectionDocuments/Divisions/lis/presentations/TheWhysandHistory.pdf

I benefici riconosciuti dell'autoverifica vanno da alleviare gli effetti della carenza di personale, all'aumentare le capacità di espandere i servizi del laboratorio, favorendo lo sviluppo professionale e l'addestramento incrociato del personale, al ridurre i tempi di risposta, migliorando l'affidabilità dei risultati, consentendo agli operatori di concentrarsi sui risultati sospetti.

Realizzare un sistema di autoverifica non è affatto facile. Siamo nelle mani del fornitore informatico o di terze parti in contratto con questo. Sviluppare e mantenere le regole può essere difficile, gli algoritmi più complessi (anatomia, microbiologia, settori speciali come coagulazione e metodi molecolari) non possono essere inseriti. E' necessario un controllo continuo, perché alcuni risultati con problemi possono sempre passare: in questi casi bisogna intervenire con correzioni al sistema, da notificare agli utenti (reparti, medici, infermieri).

Autoverifica e Reflex Testing sono meccanismi molto vicini. Gli esami riflessi sono aggiuntivi rispetto alla richiesta iniziale, si rendono necessari in base ai risultati di altri esami. Il transito del risultato in autoverifica avviene di solito prima del reflex testing, anche per mantenere il tempo di risposta.

Nel processo di autoverifica possono essere considerati diversi fattori: pre-analitici, regole mediche, orario di prelievo, dati analitici. Bisogna decidere dove realizzarla: nel sistema del laboratorio, nella stazione di lavoro strumentale, in un “buffer” a sé stante, con approcci ibridi.

Nel seminari on-line del 08 marzo 2005 e del 06 gennaio 2004 su www.aacc.org l'autoverifica è stata messa in relazione alla qualità dei risultati, negli interventi di Michael Astion (Developing a Patient Safety Culture in the Clinical Laboratory) e di Robin Felder (Laboratory Reporting for the Future: Linking Autoverification to the Electronic Medical Record).

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Altri contributi si pssono trovare in http://www.aacc.org/members/divisions/lis/Res_Center/articles/Pages/default.aspx. Tra questi, è di particolare interesse quello di Michael W. Fowler della Oklahoma Christian University (Autoverification:The How) (http://www.aacc.org/SiteCollectionDocuments/Divisions/lis/presentations/TheHow.pdf).

Fowler descrive bene il lavoro di realizzazione di un sistema di autoverifica, che coinvolge subito il personale mediante sedute di brainstorming ed affina progressivamente le regole mediante prove e correzioni.

Il semplice calcolo del delta check non è operazione da sottovalutare, come descrive Fowler. Il calcolo della "variazione di riferimento" (reference change value, RCV) si avvale di variabilità analitica (CVA) e variabilità individuale (CVI), combinati nell'equazione:

$RCV = 2^{½} \times Z \times (CVA^2 + CVI^2)^{½}$

dove Z è la probabilità o livello di significatività, Z= 2.58 at 99% (alta probabilità), Z = 1.96 at 95% (probabilità signficativa). Ma non è facile conoscere CVA e CVI.

Nel settembre 2006 a San Diego (CA, USA) tutta la tematica dell'autoverifica venne rivista da William E. Neeley (The Next Generation of Autoverification: Looking Beyond the Horizon). L'anno dopo, il 21 maggio 2007 a Baltimora ancora si è parlato di autoverifica (Autoverification & Data Management). Tutto lascia pensare che si tratti ormai di una pratica saldamente inserita nelle attività informatiche dei laboratori.

La linea guida CLSI per l'autoverifica, AUTO10-A

Clinical and Laboratory Standards Institute (CLSI). Autoverification of Clinical Laboratory Test Results; Approved Guideline. CLSI document AUTO10-A (ISBN 1-56238-620-4). Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2006.

Il Sottocomitato per la Verifica Automatica dei risultati del laboratorio medico è composto da William Neeley, Detroit, Gerald Davis, Ann Arbor, Michigan, Randy R. Davis, Bear, Delaware, Bill Marquardt, South Burlington, Karen L. Nickel, Oakland, California, Curtis A. Parvin, St. Louis, William L. Roberts, Salt Lake City, Utah, Richard S. Seaberg, Manhasset, New York, David R. Velasquez, Burlingame. Funzionano da advisors Michael W. Fowler, Oklahoma City, Peter Myles George, Christchurch, New Zealand.

Scopo della linea guida è fornire ai laboratoristi uno strumento di logica booleana di base e complessa, per sviluppare algoritmi che possono essere utilizzati per decisioni sulla verifica dei risultati basate sui dati medici disponibili. Logica booleana di base può essere definita come una dichiarazione con le parole "E" o "O" nella creazione di una frase logica (o regola). La logica booleana complessa consiste di diverse dichiarazioni combinato con "E" o "O" che permettono di un'analisi precisa di un particolare situazione.

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

Auto-verifica è un processo mediante il quale i computer eseguono automaticamente azioni definite su un sottoinsieme dei risultati di laboratorio senza la necessità di intervento manuale di un

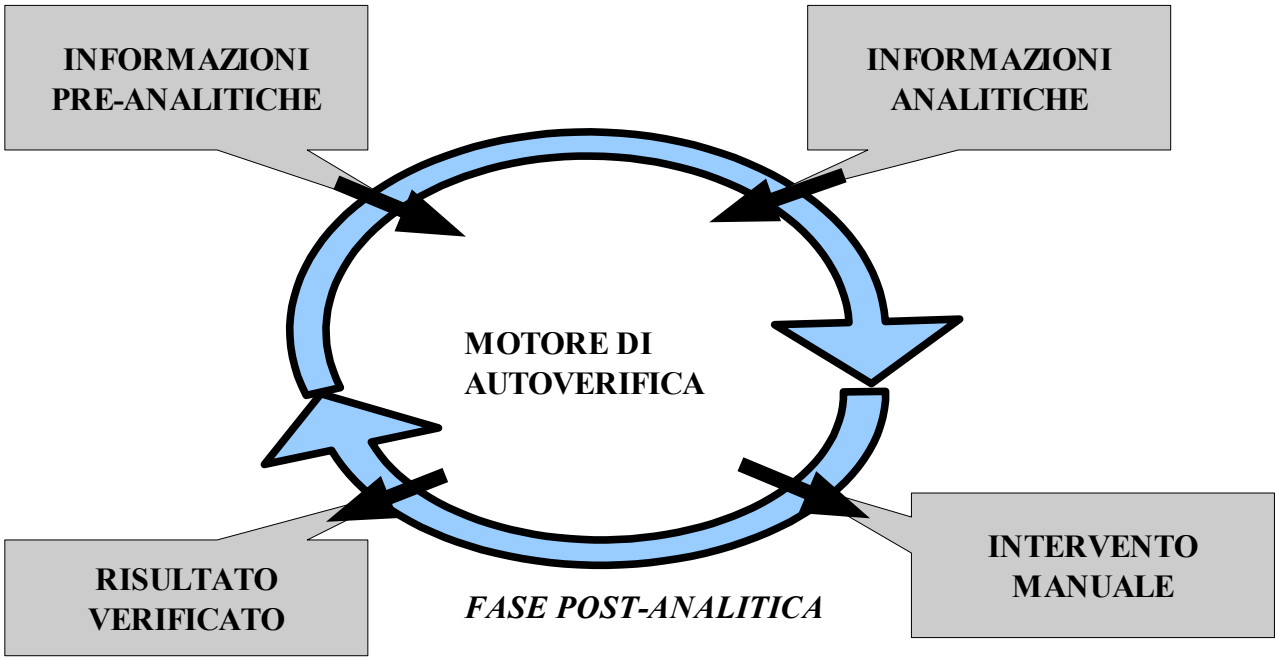


Figura XXX: il processo di autoverifica (modificato da CLSI AUTO10-A)

laboratorista. L'azione potrebbe essere la verifica immediata di un risultato, la ripetizione, un'altro esame (reflex), aggiunta di commenti, o proposte di misure manuali incluso (ma non limitate a) la revisione manuale del risultato. AUTO 10 fa riferimento a standard come ISO 14971:2000, Medical devices – Application of risk management to medical devices; AAMI/ANSI SW68:2001, Medical device software – Software life cycle processes.

AUTO 10 contiene un elenco dettagliato (sezione 4) degli elementi da considerare nell'auto-verifica, distinti in fase preanalitica (dati del paziente, della cartella elettronica, della farmacia), fase analitica (campione, strumento e risultato) e post-analitica (precedenti, altri esami, altri prelievi). Le decisioni sono basate su algoritmi che prevedono la comparazione con intervalli di riferimento, intervalli analitici, valori di allarme, valori decisionali. I risultati ripetuti vengono riconosciuti. Il delta check, ossia il confronto con risultati precedenti, ha limiti di accettabilità in asssoluto o percentuali. Il delta check dà la possibilità al tecnico di indagare su errori casuali come lo scambio di campioni, errori di trascrizione o strumentali. Le decisioni sono personalizzare in funzione del medico richiedente

La comunicazione dei risultati è regolamentata negli USA per legge (Federal law 42 CFR 493.1109), dove si stabilisce di consegnarli al medico o al laboratorio richiedente al più presto, correttamente e con riservatezza, adottando procedure particolari per i risultati di panico.

Per ottenere massima efficienza dall'auto-verifica, la distribuzione dei risultati è anch'essa automatizzata, nel modo adatto alle condizioni locali del laboratorio. E' però importante avere una conferma di ritorno o una firma digitale dal destinatario. Il tecnico documenta i casi in cui risulta impossibile comunicare col medico richiedente (4.3.2.2). Il meccanismo di auto-verifica può essere disattivato selettivamente per un esame, una combinazione di esami o uno strumento (4.4).

Medicina di laboratorio: parte generale. *Burlina Angelo; Galzigna Lauro*. Prezzo € 154,94 1996, 2 voll., 950 p., ill. *Piccin-Nuova Libraria* (collana **Trattato di medicina di laboratorio**)

SEZIONE I capitolo 12 **ABC del LIS. Introdurre il computer nel laboratorio clinico** *FR. Elevitch e R.D. Aller.* **Aggiornamento 2008** *Marco Pradella*

La sezione 5 di AUTO 10 è dedicata alla normativa, che comprende la responsabilità sulle politiche e le procedure di auto-verifica, la supervisione ed i meccanismi di delega.

Anche l'auto-verifica, come le altre attività di laboratorio, viene sottoposta a controllo di qualità, usando campioni di prova e documentando i casi trattenuti per la revisione manuale. Gli algoritmi vengono provati con modalità elettroniche.

L'auto-verifica non deve modificare i contenuti obbligatori della risposta con i risultati degli esami ed il trattamento dei risultati in archivio.

Con gli algoritmi di auto-verifica è più facile rispondere ai requisiti normativi (negli USA, Clinical Laboratory Improvement Amendments, CLIA), perché documentano l'aderenza a politiche e procedure scritte. Negli USA la legge federale rende il direttore del laboratorio responsabile della qualità del servizio (42 CFR 493.1407 [1] and [6]), ma alcuni stati ancora escludono esplicitamente l'uso dell'auto-verifica.

CLSI AUTO10 elenca in dettaglio le caratteristiche importanti degli algoritmi di autoverifica (5.1.1): inclusione di informazioni importanti generate dagli strumenti; presentazione al tecnico delle azioni correttive previste e documentazione di quelle eseguite; documentazione delle calibrazioni, dei problemi emersi e dei rimedi adottati; allarme su indici del controllo di qualità analitico (numero, frequenza e valutazione dei risultati) (5.1.1.3) e persino la documentazione delle azioni correttive del controllo di qualità; documentazione delle comparazioni dei risultati con criteri multipli (età, sesso, diagnosi, altri risultati e dati) in modo da evidenziare quelli inconsistenti (5.1.1.4) nonché delle azioni intraprese per i risultati segnalati; gestione delle priorità, in modo che i risultato più urgenti vengano presentati prima al tecnico (5.1.1.5) e vengano rilevati i casi di ritardo nonché documentate le relative azioni correttive; registrazione del tecnico responsabile e dell'addetto allo strumento, se disponibile, che può essere la stessa persona (5.1.1.6), a cui vengono assegnate le revisioni manuali, mentre i risultati auto-verificati sono identificati come tali ma anche per questi si conserva l'identità dell'esecutore.

La sezione 6 di CLSI AUTO10 è dedicata alla validazione degli algoritmi e prende in considerazione la logica, la raccolta dei dati, gli aggiornamenti di algoritmo e programma software, gli strumenti di validazione e la rivalidazione periodica.

Sono previste due fasi per la validazione. La prima si avvale di risultati simulati per tracciare la logica e verificare i calcoli. La seconda si avvale invece di casi clinici reali. Per la validazione servono un piano, le attività previste dal piano ed un rapporto finale. La tabella XXX riporta alcuni esempi di campioni necessari per validare la logica dell'algoritmo di auto-verifica:

Tabella XXX. Esempi di campioni necessari per validare l'auto-verifica (da CLSI AUTO10)

• campioni con risultati nei limiti di riferimento
• campioni con risultati superiori all'intervallo di riferimento
• campioni con risultati inferiori all'intervallo di riferimento
• campioni con risultati nell'intervallo dei valori critici
• campioni con risultati sia inferiori che superiori all'intervallo di misura analitica

- campioni con indici di interferenza
- campioni con calcoli da inserire nei risultati

Oltre ai campioni selezionati, si raccomanda di fare la revisione totale di pacchetti di risultati consistenti, ad esempio quelli di un interno turno. Questo metodo può catturare i casi problematici con bassa probabilità, purtroppo solo dopo che sono avvenuti. La documentazione di queste prove comprende il risultato atteso, quello ottenuto e tutte le indagini o le misure prese per i risultati non attesi.

Occorre garantire l'integrità dei dati, ossia la corrispondenza tra quello che esce dall'analizzatore e quello che compare nei risultati dei pazienti (6.2). Tutto il processo di validazione va ripetuto quando di modifica l'algoritmo interno (6.3), il programma sofware dell'analizzatore, del sistema informatico del laboratorio o del middleware (6.4). Per fare queste validazioni è utile avere un programma software in grado di simulare risultati analitici in diversi scenari.

Anche se non è cambiato nulla, si deve programmare una scaletta di rivalidazioni periodiche (6.6). Queste rivalidazioni possono avvalersi anche dei risultati riportati nel periodo trascorso.

La statistica dei risultati del monitoraggio delle prestazioni del sistema di auto-verifica serve per aggiustare continuamente le regole ed i limiti applicati.

i 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.