Raccomandazioni per Accreditamento ISO 15189 del laboratorio medico: processi della gestione dati e informazioni

Recommendations for Medical Laboratory ISO 15189 Accreditation: data and information management processes

Codifica di questo documento:

Flusso Operativo		**Elementi fondamentali del sistema qualità**	
Pre-esame Richiesta di esame A		Documenti e Registri L	
Prelievo B		Organizzazione M	
Trasporto del campione C		Personale N	
Accettazione e trattamento del campione D		Strumentazione O	
Esame Analisi E		Acquisti e gestione scorte P	
Revisione e flusso dei risultati F		Controllo del processo Q	#
Interpretazione di laboratorio G		Gestione delle informazioni R	#
Post-esame Trasmissione e archiviazione del risultato H		Gestione degli inconvenienti S	
Conservazione e smaltimento del campione I		Verifiche T	
		Miglioramento del processo U	
		Servizio e Soddisfazione V	
		Impianti e sicurezza Z	

Riferimenti normativi

- UNI EN ISO 15189:2023. Laboratori medici - Requisiti riguardanti la qualità e la competenza.
- UNI EN ISO 22367:2020. Laboratori medici - Applicazione della gestione del rischio ai laboratori medici
- EN ISO/IEC 27001:2023. Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)
- UNI CEI EN ISO/IEC 27000:2020. Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Panoramica e vocabolario
- UNI CEI EN ISO/IEC 27002:2023. Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni
- UNI EN ISO 27799:2017. Informatica medica - Gestione della sicurezza dell'informazione in materia di salute in riferimento alla UNI CEI ISO/IEC 27002
- ISO 17090-1:2021. Health informatics. Public key infrastructure. Part 1: Overview of digital certificate services
- ISO/TS 17975:2022. Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information.
- UNI CEI EN ISO/IEC 17025:2018. Requisiti generali per la competenza dei laboratori di prova e taratura

Indice

Introduzione: la revisione di ISO 15189

SIPMeL ha già affrontato il tema della gestione informatica nei laboratori medici con le Raccomandazioni 2017 del Gruppo di Studio Informatica.[1],[2] Si deve tornare sull'argomento alla luce della revisione della norma ISO per l'accreditamento dei laboratori medici.

La norma ISO 15189 revisionata è stata pubblicata il 6 dicembre 2022, quasi un anno dopo il termine previsto, e recepita da UNI in Italia poco tempo dopo.[3] Il processo di revisione è stato lungo e faticoso, iniziato già in ottobre 2018[4] ha attraversato molteplici versioni della bozza e altrettante votazioni. Dai vertici ISO e del Comitato tecnico competente (ISO/TC 212) sono state ricevute, tra le altre, alcune importanti direttive: usare ISO/IEC 17025:2017 come modello, incorporare ISO 22870 (la norma per i Point-of-care), stabilire collegamenti con ISO 15190 (salute e sicurezza), ISO 22367 (gestione dei rischi) e ISO/TS 20658 (fase preesame), ridurre i requisiti prescrittivi ma basarsi sul rischio per il paziente, prendere in considerazione altri documenti ISO pubblicati pertinenti, con l'obiettivo di evitare anche ripetizioni ridondanti, sincronizzando le clausole pertinenti in ISO 15190, ISO 22367, ISO TS 20658, ISO 17511 (taratura), ISO TS 20914 (incertezza di misura) e la serie di standard diagnostici molecolari sviluppato da ISO TC Il risultato è stato la presenza dei POCT in quasi tutti i capitoli e una appendice normativa di ISO 15189 sulla gestione dei POCT.

Tuttavia, le innovazioni chieste da ISO si sono scontrate nel processo di revisione con non poche resistenze, con il risultato della presenza nel testo finale di diversi compromessi, potenziali difficoltà per laboratori medici e ispettori di accreditamento.[5] Un particolare impegno a laboratori e ispettori è richiesto dalla disposizione di collegare ISO 15189 a numerosi altri documenti ISO pertinenti, al fine di evitare ridondanze.

In questa nota vengono presentati alcuni punti salienti di UNI EN ISO 15189:2023 nel capitolo 7 (Requisiti di processo), in particolare nella clausola 7.6 (Controllo della gestione dei dati e delle informazioni) i punti norma 7.6.1 Generalità, 7.6.2 Autorità e responsabilità per la gestione delle informazioni, 7.6.3 Gestione dei sistemi informativi, 7.6.4 Piani di inattività, 7.6.5 Gestione fuori sede.

1 SIPMeL. Raccomandazioni per la razionalizzazione e la convergenza della informatica di laboratorio nei Servizi Sanitari Regionali. 21 gennaio 2017. https://www.sipmel.it/it/lineeguida/approvate/110813

2 Pradella, M. Infrastruttura informatica per i Laboratori medici (LIS) del 2020: le raccomandazioni SIPMeL. Riv Ital Med Lab 13, 56–62 (2017). https://doi.org/10.1007/s13631-017-0142-1

3 UNI EN ISO 15189:2023. Laboratori medici - Requisiti riguardanti la qualità e la competenza. Data disponibilità: 02 marzo 2023

4 Pradella M. Requisiti dei laboratori medici, forensi, antidoping e alimentari: nuove ISO 15189 e ISO 17025. La Rivista Italiana della Medicina di Laboratorio 2019 dicembre;15(4):252-62. DOI: 10.23736/S1825-859X.19.00033-1

5 Pradella M. New ISO standards for medical biology laboratories, prescriptions and deviations. Volume 80, issue 5, September-October 2022. Annales de Biologie Clinique. 2022;80(5):451-453. doi:10.1684/abc.2022.1755

ISO 15189 7.6 gestione dei dati e delle informazioni

UNI EN ISO 15189:2023 al punto 7.6 (Controllo della gestione dei dati e delle informazioni) chiede che il laboratorio deve avere accesso ai dati e alle informazioni necessarie per svolgere le attività di laboratorio. Nel capitolo 6.4 (Attrezzatura) vengono compresi i sistemi informativi di laboratorio, ma il capitolo 7 puntualizza che al laboratorio non serve il possesso del sistema in sé, ma la possibilità di avere dati e informazioni, anche da sistemi informatici esterni. Non solo il termine "sistemi informativi di laboratorio" comprende la gestione di dati e informazioni contenuti in sistemi informatici e non informatici. Alcuni requisiti possono essere più applicabili ai sistemi informatici che a quelli non informatici.
Il punto 7.6 di ISO 15189 corrisponde ai punti di ISO 9001 7.4 Comunicazione e 7.6 Controllo della gestione dei dati e delle informazioni, ai punti di ISO 17025 7.11 Controllo della gestione dei dati e delle informazioni e 7.6 Controllo della gestione dei dati e delle informazioni, nonché a quelli di ISO 15189 edizione 2012 5.10 Gestione delle informazioni di laboratorio, 5.10.1 Generalità, 5.10.2 Autorità e responsabilità e 5.10.3 Gestione del sistema informative.
Ottemperando alle direttive dei vertici ISO, il documento 15189 rimanda per i rischi associati ai sistemi informativi di laboratorio computerizzati alla norma ISO 22367:2020, punto in appendice A.13, mentre i controlli di sicurezza delle informazioni, le strategie e le migliori pratiche per garantire la conservazione della riservatezza, dell'integrità e della disponibilità delle informazioni sono elencati nella norma ISO/IEC 27001:2022, Allegato A (Controlli di sicurezza delle informazioni).

UNI EN ISO 22367:2020 rischio informatico nei laboratori medici

ISO ha avviato il progetto ISO/AWI 22367 “Laboratori medici Applicazione della gestione del rischio ai laboratori medici”, la votazione è terminata il 7 settembre 2023 con 28 voti su 39, con cui si la raccomandazione di avviare una revisione anticipata di ISO 22367 per allinearla alla norma ISO 15189:2022, anticipata in quanto revisione sistematica avrebbe dovuto avvenire nel 2025.
ISO 22367 fornisce ai laboratori medici un quadro di riferimento per gestire i rischi associati agli esami di laboratorio, che abbraccia l'intera gamma dei servizi: processi di preesame, esame e post-esame, compresa la progettazione e lo sviluppo degli esami. I requisiti di ISO 22367 sono applicabili a tutti gli aspetti degli esami e dei servizi, compresa la trasmissione accurata dei risultati degli esami nella cartella clinica elettronica.[6],[7]
L’Allegato A (informativo) di ISO 22367:2020 (Attuazione della gestione del rischio all'interno del sistema di gestione della qualità) contiene al punto A.13 il tema del controllo dei sistemi informativi di laboratorio. Qui si elencano le problematiche relative ai rischi potenziali, che possono comprendere: identificare e rintracciare correttamente un paziente e tutto il personale interessato durante l'intero processo di esame; trasmettere e visualizzare correttamente e in modo leggibile e comprensibile le informazioni, come istruzioni per la richiesta di esami al prelevatore o al laboratorio, risultati degli esami, problemi relativi al campione o all'esame che possono influire sull'interpretazione. Ma anche tollerare e/o recuperare le interruzioni del sistema informativo del laboratorio (di cui a ISO 15189

[6] UNI EN ISO 22367:2020. Laboratori medici - Applicazione della gestione del rischio ai laboratori medici
[7] Pradella M. ISO 22367 e la gestione dei rischi nei laboratori medici ISO 22367:2020. La Rivista Italiana della Medicina di Laboratorio 2019 Settembre;15(3):237-8 DOI: 10.23736/S1825-859X.19.00024-0

7.6.4); integrità e affidabilità dei sistemi informatici intermediari (*middleware*); intrusione nei sistemi collegati a Internet (direttamente o indirettamente) per modificare o rubare i dati dei pazienti; cibersicurezza in generale.

NOTA cibersicurezza
La cibersicurezza nei sistemi informatici sanitari è diventata popolare grazie ad alcuni recenti fatti di cronaca. Anche la sicurezza dei sistemi informatici intermediari (middleware) è un aspetto ancora poco curato nei laboratori, che hanno dedicato invece molte risorse ad aspetti prevalentemente formali come la firma digitale.

ISO/IEC 27001, ISO/IEC 27002, ISO 27799 e controlli di sicurezza delle informazioni[8]

ISO 27001 anche è norma europea (EN), ma non ancora accolta da UNI tra le norme italiane, dove restano al momento le edizioni precedenti.[9]
ISO 27001 contiene requisiti per la creazione, l'attuazione, il mantenimento e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni, influenzata dalle esigenze e dagli obiettivi dell'organizzazione, dai requisiti di sicurezza, dai processi organizzativi utilizzati e dalle dimensioni e dalla struttura dell'organizzazione fattori destinati a cambiare nel tempo. Deriva da ISO/IEC 27000, panoramica e vocabolario dei sistemi di gestione della sicurezza delle informazioni,[10] capostipite della famiglia di norme sui sistemi di gestione della sicurezza delle informazioni, che oggi contiene ben 25 standard. Tra questi, ISO 27002, che fornisce un insieme di controlli generici per la sicurezza delle informazioni,[11] e ISO 27799, che definisce le linee guida per l'attuazione in informatica sanitaria della ISO/IEC 27002. [12] La norma si applica a tutti gli aspetti delle informazioni riguardanti la salute, in qualsiasi forma (parole e numeri, registrazioni sonore, disegni, video e immagini mediche), indipendentemente dal mezzo usato per la memorizzazione (stampa, scrittura su carta o archiviazione elettronica) e qualsiasi tipo di trasmissione dei dati (a mano, tramite fax, su reti di computer o per posta). ISO 27799 è in questo momento sottoposta a revisione come ISO/AWI 27799.[13]
La ISO 27799:2016 (la versione attuale) si basa sulla ISO/IEC 27002:2013 e deve essere rivista per allinearsi alla ISO/IEC 27002:2022. Esistono differenze significative tra il contenuto tecnico della versione precedente e di quella attuale della ISO/IEC 27002. La ISO/IEC 27002:2022 ha una struttura

[8] EN ISO/IEC 27001:2023. Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022)
[9] UNI CEI EN ISO/IEC 27001:2017. Tecnologie Informatiche - Tecniche di sicurezza - Sistemi di gestione della sicurezza dell'informazione – Requisiti.
[10] UNI CEI EN ISO/IEC 27000:2020. Tecnologie informatiche - Tecniche di sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Panoramica e vocabolario
[11] UNI CEI EN ISO/IEC 27002:2023. Sicurezza delle informazioni, cybersecurity e protezione della privacy - Controlli di sicurezza delle informazioni
[12] UNI EN ISO 27799:2017. Informatica medica - Gestione della sicurezza dell'informazione in materia di salute in riferimento alla UNI CEI ISO/IEC 27002
[13] ISO/AWI 27799. Health informatics. Information security management in health using ISO/IEC 27002. https://www.iso.org/standard/84647.html

completamente diversa dalla precedente. In particolare, la nuova versione ha 4 clausole sui controlli (organizzativi, delle persone, fisici e tecnologici), mentre la versione 2013 ne aveva 14. Il numero totale dei controlli è cambiato, passando da 1 a 2. Il numero totale di controlli è passato da 114 a 93 e l'ordine è cambiato in modo significativo.
ISO 27799 assorbirà anche il documento ISO/TS 14441:2013, un progetto avviato nel 2010 da Alessandra Pastorino di UNINFO, dedicato a sistemi di cartella clinica elettronica presso il punto di assistenza clinica.[14]

NOTA ISO 27001 e ISO 27799
Laboratori e ispettori possono chiedersi come dimostrare evidenza di conformità al punto ISO 15189 7.6.1. Non è escluso che si faccia riferimento direttamente alla norma collegata ISO 27001, nonché alle sue declinazioni, quella applicativa ISO 27002 e quella sanitaria ISO 27799. La citata raccomandazione SIPMeL[15] dava indicazione al punto 5.1.5.3 come ideale la certificazione ISO 27001, rilasciata oggi in Italia da organismi di certificazione di sistemi di gestione per la sicurezza delle informazioni accreditati secondo le norme ISO/IEC 17021-1 e ISO/IEC 27006.[16]

In ISO 27799:2016 i laboratori sono menzionati in particolare nel punto 11.1.6 (Aree di consegna e carico), dove si segnalano circostanze distinte in cui il pubblico (soggetti in cura e loro accompagnatori) è fisicamente ammesso in aree con grandi quantità di informazioni sensibili (ad esempio, esami di laboratorio in cui il flusso di lavoro può imporre la raccolta di informazioni dai soggetti in cura nella stessa area in cui si stanno elaborando i dati di soggetti precedenti). Le aree fisiche dell'assistenza sanitaria che raccolgono informazioni sulla salute attraverso interviste e che contengono sistemi in cui i dati vengono visualizzati su schermo dovrebbero quindi essere soggette a un controllo supplementare. Nell'allegato B (Piano d'azione pratico per l'attuazione di ISO/IEC 27002 in ambito sanitario) al punto B.4.4 (Valutazione dei rischi per le informazioni sanitarie) si evidenzia che l'assistenza sanitaria comporta rischi relativamente elevati, soprattutto in aree come i laboratori, i reparti di emergenza e le sale operatorie, sconsigliando di attribuire basso rischio a tali aree.
Il contenuto di ISO/IEC 27001:2022 sta prevalentemente nell'Allegato A (normativo), dove si trova il riferimento ai controlli di sicurezza delle informazioni, organizzato in una lunga tabella di 7 pagine con una sezione dedicata a Controlli organizzativi (37 controlli), Controlli sulle persone (8 controlli), Controlli fisici (14 controlli), Controlli tecnologici (34 controlli).

NOTA firma digitale
ISO 27001 non cita in nessun punto la tecnica di infrastruttura di chiave pubblica (PKI) ovvero

[14] UNI CEN ISO/TS 14441:2014. Informatica sanitaria - Requisiti di sicurezza e privacy delle cartelle cliniche elettroniche per la valutazione dei criteri conformità
[15] SIPMeL. Raccomandazioni per la razionalizzazione e la convergenza della informatica di laboratorio nei Servizi Sanitari Regionali. 21 gennaio 2017. https://www.sipmel.it/it/lineeguida/approvate/110813
[16] Accredia. Sistemi di gestione per la sicurezza delle informazioni. https://www.accredia.it/servizio-accreditato/sistemi-di-gestione-per-la-sicurezza-delle-informazioni/

lo strumento informatico alla base della cosiddetta "firma digitale". Se ne deduce che la "firma digitale" non ha alcun ruolo nella sicurezza informatica, mentre può essere utilizzata in ambiti diversi. Infatti, lo strumento con PKI non impedisce l'accesso ai documenti con informazioni sanitarie, ma garantisce solo l'autenticazione della firma stessa. Peraltro, nemmeno ISO 15189 richiede la firma dei documenti, ma l'individuazione degli autori di ciascun intervento, sia esso il prelievo, l'esecuzione dell'esame o la verifica e rilascio dei singoli risultati, quest'ultima eseguibile anche da un sistema automatico.
ISO 17090, pubblicata con revisione nel 2021 e ora avviata nuovamente alla revisione con le norme collegate nella stessa famiglia,[17] destina infatti lo strumento "firma digitale" a informazioni sanitarie riguardanti i singoli cittadini scambiate tramite posta elettronica, accesso remoto a database, scambio elettronico di dati e altre applicazioni. L'interoperabilità della tecnologia dei certificati digitali è importante per lo scambio di informazioni, ad esempio, tra un ospedale e un medico della comunità che lavora con lo stesso paziente.
Per quanto riguarda gli obiettivi di salvaguardia della sfera privata e della riservatezza, pur enunciati nell'introduzione al documento ISO 17090, si attendono chiarimenti.

La gestione informatica del consenso

Tema particolarmente delicato è quello del consenso del paziente, trattato da UNI EN ISO 15189:2023 al punto 7.2.4.3. Il laboratorio deve ottenere il consenso informato del paziente per tutte le procedure eseguite su di esso, anche se per la maggior parte delle procedure di laboratorio ordinarie, il consenso può essere "dedotto" quando il paziente si sottopone volontariamente alla procedura di prelievo, ad esempio la puntura venosa. Le procedure speciali, come quelle più invasive o quelle che comportano un maggior rischio di complicazioni, possono richiedere una spiegazione più dettagliata e, in alcuni casi, un consenso documentato e registrato. Se non è possibile ottenere il consenso in situazioni di emergenza, il laboratorio può eseguire le procedure necessarie, purché siano nell'interesse del paziente.

NOTA progetto UNINFO su consenso

Può essere utile segnalare su questo tema il progetto UNINFO 1611110 sulla gestione informatica del consenso, già sottoposto a inchiesta pubblica.[18] Il documento prodotto dal progetto, ispirato a ISO/TS 17975,[19] contiene una panoramica sullo stato dell'arte inerente al consenso al trattamento dei dati in ambito sanitario, a supporto delle organizzazioni sanitarie per favorire lo sviluppo di sistemi software modulari, inclusi sistemi software di gestione dei consensi, aderenti ai principali standard internazionali di informatica medica in grado di interoperare nel rispetto della legislazione vigente in materia di protezione dei dati personali, con i concetti fondamentali, i riferimenti alle norme tecniche e le azioni utili per ottenere un consenso in ambito sanitario italiano. Nel progetto è trattata anche la fattispecie del cosiddetto

[17] ISO 17090-1:2021. Health informatics. Public key infrastructure. Part 1: Overview of digital certificate services
[18] Codice Progetto UNI1611110. Informatica Medica - Sistema di gestione del consenso in ambito sanitario – Panoramica
[19] ISO/TS 17975:2022(en) - Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information.

"consenso implicito", corrispondente al "consenso dedotto" della norma ISO.[20] Il documento UNINFO ricorda però che anche nei casi di "consenso implicito" o "dedotto", il laboratorio non è sottratto (art.26 del 317 Regolamento Europeo) a tutti gli obblighi e adempimenti previsti dal regolamento e dalla legge per i titolari o contitolari del trattamento dei dati.[21]

ISO 15189:2023 7.6.2 Autorità e responsabilità 7.6.3 Gestione dei sistemi informativi

Il laboratorio deve garantire che siano specificate le autorità e le responsabilità per la gestione dei sistemi informativi, compresa la manutenzione e la modifica dei sistemi informativi che possono influire sull'assistenza ai pazienti. Il laboratorio è il responsabile ultimo dei sistemi informativi del laboratorio.
Il punto ISO 15189:2023 7.6.3 Gestione dei sistemi informativi (lettera a) chiede che i sistemi utilizzati per la raccolta, l'elaborazione, la registrazione, la creazione di rapporti, l'archiviazione o il recupero dei dati e delle informazioni sugli esami devono essere validati dal fornitore e verificati dal laboratorio prima della loro introduzione. Qualsiasi modifica al sistema, compresa la configurazione del software di laboratorio o le modifiche al software commerciale, deve essere autorizzata, documentata e validata prima dell'attuazione. Validazione e verifica includono, ove applicabile, il corretto funzionamento delle interfacce tra il sistema informativo di laboratorio e altri sistemi, quali le apparecchiature di laboratorio, i sistemi di amministrazione dei pazienti in ospedale e i sistemi di assistenza primaria. Il software commerciale disponibile sul mercato, utilizzato nell'ambito del campo di applicazione previsto, può essere considerato sufficientemente convalidato (ad esempio, programmi di elaborazione testi e fogli di calcolo e programmi informatici di gestione della qualità, i cosiddetti strumenti di produttività individuale).

NOTA manutenzione sistemi informatici
Mantenere la continuità della responsabilità in occasione di interventi di manutenzione informatica o modifiche al sistema non è affatto scontato. Può essere un punto qualificante del capitolato e del contratto di acquisto.

ISO 15189:2023 al punto 7.6.3 (Gestione dei sistemi informativi) (alle successive lettere da b a e) chiede la documentazione prontamente disponibile per gli utenti autorizzati, compresa quella per il funzionamento quotidiano del sistema; che si tenga in conto la cibersicurezza, per proteggere il sistema da accessi non autorizzati e salvaguardare i dati da manomissioni o perdite; un ambiente conforme alle specifiche del fornitore o, nel caso di sistemi non computerizzati, in condizioni tali da salvaguardare l'accuratezza della registrazione e della trascrizione manuale; una manutenzione che garantisca l'integrità dei dati e delle informazioni e registri i guasti del sistema e le relative azioni immediate e correttive. I calcoli e i trasferimenti di dati devono essere controllati in modo appropriato e sistematico.

[20] Pradella M. Nuove norme tecniche nazionali e internazionali per l'informatica del laboratorio medico: un quadro generale. La Rivista Italiana della Medicina di Laboratorio 2022 dicembre;18(4):233-40. DOI: 10.23736/S1825-859X.23.00170-6

[21] Regolamento UE 2016 679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Arricchito con riferimenti ai Considerando Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018

CLSI AUTO11 Sicurezza informatica degli strumenti IVD e dei sistemi informatici

ISO 15189 enuncia una serie di principi validi e, seguendo le direttive dei vertici ISO, non entra nei dettagli esecutivi. I laboratori hanno quindi bisogno di supporto, linee guida autorevoli e riconosciute a livello internazionale, per ottenere i risultati richiesti. Altrimenti devono improvvisare. ISO non cita qui la linea guida CLSI AUTO11 sulla sicurezza informatica[22], in questo momento in revisione, che tuttavia risponde perfettamente allo scopo. In altri documenti ISO sono invece citate le linee guida CLSI. Ad esempio, ISO 11073-90101 (POCT), ISO 17822:2020 (amplificazione acidi nucleici), ISO 18113-1:2022 (documentazione diagnostici) e molti altri, in tutto 42 standard.

CLSI AUTO11 descrive requisiti tecnici e operativi e procedure di attuazione tecnica relative alla sicurezza dei sistemi diagnostici in vitro (IVD) (dispositivi, strumenti analitici, sistemi di gestione dei dati, ecc.). I destinatari sono i fabbricanti di dispositivi medici e di sistemi IVD (MDM), gli utenti (ad esempio, il personale di laboratorio) e la direzione informatica delle organizzazioni sanitarie (HDO). Questa suddivisione delle responsabilità tra soggetti è forse il contributo più rilevante di CLSI AUTO11.

Il documento CLSI AUTO11 contiene i capitoli Linee guida di progettazione tecnica relative ai requisiti normativi, Requisiti di processo e operativi e Applicabilità dei requisiti alle classi di sistemi diagnostici in vitro (rispettivamente 3, 4 e 5). Nel capitolo 5 si danno dettagli, distinguendo tutti i sistemi diagnostici in vitro (IVD, 5.1), IVD che supportano credenziali utente (5.2), IVD che gestiscono informazioni sanitarie protette (5.3), IVD che supportano connessioni di rete (5.4), IVD che supportano applicazioni in nuvola informatica (5.5), IVD che supportano applicazioni mobili (5.6). La sicurezza informatica è diventata molto più importante dalla pubblicazione della precedente edizione di questo standard nel 2014. Il settore ha riconosciuto che uno sforzo congiunto e processi armonizzati a livello globale rappresentano il modo migliore per mitigare il rischio di cibersicurezza e ridurre al minimo l'effetto degli attacchi di sicurezza informatica. Nell'era dei dispositivi esterni funzionanti in remoto e del loro accesso ai sistemi IVD, anche questi dispositivi esterni remoti sono entrati nel mirino della cibersicurezza. Un altro aspetto importante sono i sistemi basati su nuvola, che aggiungono ulteriori requisiti di sicurezza informatica

[22] CLSI. Information Technology Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard—Second Edition. CLSI document AUTO11-A2. Wayne, PA: Clinical and Laboratory Standards Institute; 2014

ISO 15189:2023 7.6.4 Piani di fermo impianto, 7.6.5 Gestione fuori sede

Il laboratorio deve disporre di processi pianificati per mantenere le operazioni in caso di guasto o durante i tempi di inattività dei sistemi informativi che influiscono sulle attività del laboratorio. Ciò include selezione automatica e presentazione dei risultati.

NOTA fermi impianto informatico

Non sarà facile per i laboratori adeguarsi a questo requisito. Il mercato offre sistemi con tolleranza ai guasti (fault tolerant), si può pensare alla ridondanza (più sistemi in parallelo), a un piano di contingenza che preveda, in casi estremi, l'utilizzo di supporti cartacei.

Questo requisito corrisponde al punto 3.2.7 Procedura di accesso di emergenza di CLSI AUTO11, dove di prevede che MDM del sistema IVD e HDO adotteranno misure ragionevoli e appropriate per stabilire, validare, attuare e documentare una procedura di accesso di emergenza che garantisca alle persone autorizzate l'accesso ai sistemi IVD critici durante un disastro. MDM deve fornire un meccanismo di accesso di emergenza a HDO. HDO deve poi incorporare il meccanismo nella sua procedura corrispondente. MDM e HDO devono notificare tutti gli aggiornamenti che riguardano il meccanismo di accesso di emergenza. HDO sarà responsabile dell'aggiornamento delle procedure organizzative interessate.
La procedura di accesso di emergenza può richiedere l'uso di meccanismi e procedure separati dalle azioni eseguite per il normale accesso degli utenti al sistema IVD. Ad esempio, se MDM introduce una credenziale utente per l'accesso di emergenza con una parola chiave, HDO dovrà proteggere tale parola e allo stesso tempo attuare procedure che consentano l'accesso e l'uso della parola in caso di disastri o emergenze.
Le persone autorizzate dovranno sempre avere a disposizione una copia aggiornata della procedura di accesso di emergenza, ma conservata in condizioni di sicurezza. Ulteriori copie devono essere conservate in un luogo sicuro fuori sede, come definito in un piano di ripristino d'emergenza separato.
Il punto 3.9.4 di CLSI AUTO11 concerne il recupero di emergenza dalla nuvola. Il recupero di emergenza per i sistemi IVD basati su nuvola è completamente fuori dalle mani dell'HDO e deve essere gestito efficacemente dall'MDM. MDM deve definire un accordo sul livello di servizio con HDO che rifletta un progetto con valori accettabili per le caratteristiche di operatività e guasto.
L'accordo sul livello di servizio deve inoltre delineare i meccanismi di allarme accettabili, le procedure di intensificazione e le procedure di accesso ai dati di HDO a scopo di ripristino.
Quando i sistemi informativi del laboratorio sono gestiti e mantenuti fuori sede o tramite un fornitore esterno (ISO 15189 punto 7.6.5 Gestione fuori sede), il laboratorio deve garantire che il fornitore o l'operatore del sistema si conformi a tutti i requisiti applicabili del presente documento. Quindi lo standard ISO deve essere una delle fonti per la stesura dei capitolati o dei contratti di acquisto.

Conclusioni e raccomandazioni

Tutto sommato, il capitolo 7.6 di ISO 15189 rispetta abbastanza le direttive ISO di ridurre i requisiti prescrittivi ma basarsi sul rischio per il paziente, prendere in considerazione altri documenti ISO pubblicati pertinenti, con l'obiettivo di evitare anche ripetizioni ridondanti. Il risultato è un testo composto di proposizioni molto appropriate, ma povero di collegamenti alle attività pratiche necessarie per ottenere la conformità ai requisiti.
Alcune indicazioni sono ritrovabili in altri documenti ISO (22367, 27001, 27799). Ma non sembrano sufficienti. Almeno il documento CLSI AUTO11 sulla sicurezza informatica avrebbe meritato una citazione esplicita, come fanno altri documenti ISO per altre linee guida CLSI. In tutto il testo di ISO 15189:2022 viene citato solo CLSI GP36 per la gestione dei disastri.
Nella sua "Introduzione" ISO 15189 afferma come obiettivo la promozione del benessere dei pazienti e la soddisfazione degli utenti del laboratorio attraverso la fiducia nella qualità e nella competenza dei laboratori medici. Nello stesso capitolo di afferma che ISO 15189 vale sia per tutte le discipline di laboratorio medico, ma può essere applicato ad altri servizi sanitari, come diagnostica per immagini, fisioterapia respiratoria, fisiochinesiterapia, banche del sangue e servizi trasfusionali. Non solo: facilita la cooperazione tra i laboratori medici e gli altri servizi sanitari, favorisce lo scambio di informazioni e l'armonizzazione di metodi e procedure. Infine, facilita la comparabilità dei risultati degli esami dei pazienti tra diversi laboratori medici. I vantaggi della norma vengono perciò prima della sua applicazione per confermare o riconoscere la competenza dei laboratori medici da parte degli utenti del laboratorio, delle autorità di regolamentazione e degli enti di accreditamento, come dichiarato nel capitolo 1 "campo di applicazione".

Si possono quindi esprimere le seguenti Raccomandazioni:

1. Si raccomanda ai laboratori di avvicinarsi ai requisiti di ISO 15189:2022 anche prima di avviare un percorso di accreditamento con un organismo che operi in conformità alla norma ISO/IEC 17011.	1. Laboratories are recommended to approach the requirements of ISO 15189:2022 even before starting an accreditation process with a body operating in accordance with ISO/IEC 17011.
2. Si può altresì raccomandare di considerare i requisiti di ISO 9001 come utile predisposizione ai requisiti di ISO 15189 in tutti i capitoli, non solo nel capitolo 8 "Sistema di gestione".	2. It is also recommended to consider the requirements of ISO 9001 as a useful predisposition to the requirements of ISO 15189 in all chapters, not only in Chapter 8 'Management System'.
3. Per evitare le insidie dei testi normativi in lingua inglese, si raccomanda di utilizzare le versioni tradotte o le raccomandazioni nazionali in lingua italiana (ISO 15189 7.3.6 lettera b).	3. In order to avoid the pitfalls of English-language regulatory texts, it is recommended to use the translated versions or national recommendations in Italian (ISO 15189 7.3.6 letter b).
4. Si raccomanda ai laboratori di avvicinarsi ai requisiti di ISO 15189:2022 anche prima di avviare un percorso di accreditamento con un organismo che operi in conformità alla norma ISO/IEC 17011.	4. Laboratories are recommended to approach the requirements of ISO 15189:2022 even before starting an accreditation process with a body operating in accordance with ISO/IEC 17011.

5. Si può altresì raccomandare di considerare i requisiti di ISO 9001 come utile predisposizione ai 26 requisiti di ISO 15189 in tutti i capitoli, non solo nel capitolo 8 “Sistema di gestione”.	5. It can also be recommended to consider the requirements of ISO 9001 as a useful predisposition to the 26 requirements of ISO 15189 in all chapters, not only in Chapter 8 'Management System'.
6. Si può raccomandare che la sicurezza informatica non si limiti ai risultati degli esami ma comprenda l’intero processo di esame fin dalla richiesta e non trascuri le componenti dei sistemi informatici intermediari (*middleware*).	6. It can be recommended that computer security should not be limited to examination results but should encompass the entire examination process right from the application and should not neglect the components of intermediary computer systems (middleware).
7. Si può raccomandare che i controlli di sicurezza dei sistemi informatici siano applicati in modo sistematico, preferibilmente certificando formalmente il sistema in riferimento alla norma ISO 27001, di cui si riportano alcuni esempi di controlli nella Tabella 1.	7. It may be recommended that computer system security controls be applied systematically, preferably by formally certifying the system with reference to ISO 27001, examples of which are given in Table 1.
8. Si può raccomandare che venga garantita la continuità della responsabilità di gestione del sistema informatico, senza interruzioni, nemmeno per interventi di manutenzione o modifiche al sistema stesso, fissando opportune regole nei capitolati o contratti di acquisto.	8. It may be recommended that continuity of responsibility for the management of the computer system be guaranteed, without interruptions, not even for maintenance work or changes to the system itself, by setting appropriate rules in the specifications or purchase contracts.
9. Si può raccomandare che il laboratorio utilizzi la linea guida CLSI AUTO11, recentemente rinnovata, per organizzare il proprio sistema di sicurezza informatica, in un contesto reale dove agiscono soggetti diversi, come produttori di sistemi, informatici delle aziende sanitarie e operatori di laboratorio.	9. It can be recommended that the laboratory uses the recently renewed CLSI AUTO11 guideline to organize its computer security system, in a real context where different actors, such as system manufacturers, health company IT staff and laboratory operators, are involved.
10. Si può raccomandare che per garantire la continuità assistenziale il sistema informatico abbia caratteristiche tali da superare qualsiasi inconveniente, sia come soluzioni tecnologiche che come procedure, anche in questo caso suggerite da CLSI AUTO11.	10. It can be recommended that in order to guarantee continuity of care, the IT system should have features that overcome any inconvenience, both in terms of technological solutions and procedures, again suggested by CLSI AUTO11.
11. Si può raccomandare che la gestione informatica fuori sede, anche nella nuvola, venga regolamentata strettamente nei contratti in modo che non vengano aggirati i requisiti fissati da ISO 15189.	11. It can be recommended that off-site IT management, including in the cloud, be strictly regulated in contracts so that the requirements of ISO 15189 are not circumvented.

Tabella 1. Esempi selezionati di controlli richiesti da ISO 27001 per la sicurezza informatica

5 Controlli organizzativi 5.3 Segregazione dei compiti: i compiti e le aree di responsabilità in conflitto devono essere separati. 5.5 Contatti con le autorità: l'organizzazione deve stabilire e mantenere contatti con le autorità competenti. 5.6 Contatti con gruppi di interesse speciale: l'organizzazione deve stabilire e mantenere contatti con gruppi di interesse speciale o altri forum di sicurezza specializzati e associazioni professionali. 5.23 Sicurezza delle informazioni per l'utilizzo dei servizi in nuvola: i processi per l'acquisizione, l'utilizzo, la gestione e l'uscita dai servizi in nuvola devono essere stabiliti in conformità ai requisiti di sicurezza delle informazioni dell'organizzazione. 5.35 Revisione indipendente della sicurezza delle informazioni: l'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione, comprese le persone, i processi e le tecnologie, devono essere riesaminati in modo indipendente a intervalli pianificati o quando si verificano cambiamenti significativi.
6 Controlli sulle persone 6.4 Processo disciplinare: deve essere formalizzato e comunicato un processo disciplinare per intraprendere azioni contro il personale e le altre parti interessate che hanno commesso una violazione della politica di sicurezza delle informazioni. 6.7 Lavoro a distanza: le misure di sicurezza devono essere implementate quando il personale lavora in remoto per proteggere le informazioni a cui si accede, che vengono elaborate o archiviate al di fuori dei locali dell'organizzazione.
7 Controlli fisici 7.7 Scrivania libera e schermo libero: devono essere definite e applicate in modo appropriato le regole di ordine della scrivania per i documenti e i supporti di memorizzazione rimovibili e le regole di chiarezza dello schermo per le strutture di elaborazione delle informazioni. 7.14 Smaltimento o riutilizzo sicuro delle apparecchiature: le apparecchiature contenenti supporti di memorizzazione devono essere verificate per garantire che tutti i dati sensibili e il software con licenza siano stati rimossi o sovrascritti in modo sicuro prima dello smaltimento o del riutilizzo.
8 Controlli tecnologici 8.4 Accesso al codice sorgente: l'accesso in lettura e scrittura al codice sorgente, agli strumenti di sviluppo e alle librerie software deve essere gestito in modo appropriato. 8.14 Ridondanza delle strutture di elaborazione delle informazioni: le strutture di elaborazione delle informazioni devono essere implementate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità. 8.24 Uso della crittografia: devono essere definite e attuate regole per l'uso efficace della crittografia, compresa la gestione delle chiavi crittografiche. 8.30 Sviluppo in esternalizzazione: l'organizzazione deve dirigere, monitorare e rivedere le attività relative allo sviluppo di sistemi in esternalizzazione. 8.34 Protezione dei sistemi informativi durante le prove di audit: le prove di audit e le altre attività di garanzia che comportano la valutazione dei sistemi operativi devono essere pianificati e concordati tra il valutatore e la direzione competente.