PROTOCOLLO DI CYBERSECURITY

PER MEDICI E STUDI MEDICI

Protezione di dati sanitari, cartelle cliniche digitali, telemedicina e intelligenza artificiale

Applicabile a medici di base, specialisti, poliambulatori e studi medici di ogni dimensione

Centuria Foundation

centuriafoundation.pl

Versione 1.0 | 2025

Indice

1. Introduzione e Contesto Normativo

I medici e gli studi medici trattano la categoria di dati personali piu sensibile prevista dal GDPR: i dati relativi alla salute. Anamnesi, diagnosi, terapie, referti, immagini diagnostiche, note psicologiche. Una violazione informatica in ambito sanitario non e solo un danno operativo: e una violazione della privacy del paziente, un potenziale illecito penale e una lesione del rapporto fiduciario alla base della relazione terapeutica.

Questo protocollo fornisce linee guida operative, metodologie concrete e strumenti pratici per proteggere lo studio da minacce reali. L approccio e proporzionato alle risorse disponibili e applicabile a medici singoli, specialisti, poliambulatori e strutture di piccole e medie dimensioni.

1.1 Riferimenti Normativi

Norma / Regolamento	Rilevanza per il Medico
GDPR (Reg. UE 2016/679)	I dati sanitari sono "dati particolari" ex art. 9: protezione rafforzata. Misure tecniche adeguate obbligatorie. Notifica breach entro 72 ore al Garante.
D.Lgs. 196/2003 (Codice Privacy)	Base normativa italiana. Art. 75-94: disciplina specifica del trattamento dei dati sanitari.
Codice di Deontologia Medica	Artt. 10-11: segreto professionale e riservatezza, estesi all ambiente digitale e ai sistemi informatici.
D.Lgs. 502/1992 e s.m.i.	Organizzazione del servizio sanitario. Obblighi di riservatezza nelle strutture sanitarie.
Linee guida Garante Privacy	Provvedimento del 4 giugno 2020 e successive: indicazioni specifiche per il trattamento dati sanitari.
NIS2 (Dir. UE 2022/2555)	Strutture sanitarie di medie e grandi dimensioni rientrano tra i soggetti essenziali con obblighi di sicurezza rafforzati.
ISO/IEC 27001 / ISO 27799	ISO 27799: standard specifico per la sicurezza delle informazioni in ambito sanitario.

Attenzione: I Dati Sanitari sono Dati Particolari

Il GDPR classifica i dati sulla salute come "dati particolari" (art. 9): richiedono misure di protezione piu elevate rispetto ai dati personali ordinari.

Una violazione che espone dati sanitari puo configurare:

- Violazione del segreto professionale medico (reato penale, art. 622 c.p.)
- Illecito amministrativo GDPR fino a 20 milioni di euro o 4% del fatturato globale
- Responsabilita civile per danni patrimoniali e non patrimoniali al paziente
- Notifica obbligatoria al Garante entro 72 ore e ai pazienti coinvolti

La cybersecurity in ambito medico non e una questione tecnica: e un obbligo etico e giuridico.

2. Gestione di Password e Accessi

2.1 Politica delle Password

Negli studi medici le credenziali di accesso proteggono cartelle cliniche, referti, immagini diagnostiche e dati di pazienti vulnerabili. La gestione delle password e il primo livello di difesa e non puo essere approssimativa.

Parametro	Requisito
Lunghezza minima	16 caratteri (20+ per accessi a cartelle cliniche digitali e sistemi gestionali).
Composizione	Lettere maiuscole/minuscole, numeri e simboli. Mai parole di dizionario o termini medici comuni.
Unicita	Password diversa per ogni sistema: gestionale, email, cartella clinica, PACS, portali SSN.
Rotazione	Cambio ogni 12 mesi. Immediato se si sospetta una compromissione o al cambio di personale.
Account condivisi	Vietati. Ogni operatore deve avere credenziali personali per garantire la tracciabilita degli accessi.

Password Manager consigliati

Strumento	Caratteristiche	Livello
Bitwarden	Open source, cloud EU disponibile, piano business con gestione team. Audit pubblici.	Consigliato
1Password	Funzioni avanzate per team, Travel Mode, report sicurezza. Interfaccia eccellente.	Professionale
KeePassXC	Completamente offline. Massima privacy, nessun dato in cloud.	Avanzato

2.2 Gestione degli Accessi per Ruolo

Negli studi medici operano figure diverse: medici, infermieri, amministrativi, tecnici. Ognuno deve accedere solo ai dati necessari per il proprio ruolo (principio del minimo privilegio).

Figura	Accesso consentito	Accesso vietato
Medico titolare	Cartelle cliniche complete, gestionali, referti, immagini	Accesso sistemi amministrativi non necessari
Medico sostituto/associato	Solo cartelle dei propri pazienti durante la sostituzione	Archivio completo dello studio
Infermiere / OSS	Dati necessari per la specifica prestazione	Diagnosi, note anamnestiche, terapie complete

Personale amministrativo	Dati demografici, prenotazioni, fatturazione	Dati clinici, diagnosi, terapie
Tecnico informatico	Accesso tecnico ai sistemi, mai ai dati	Cartelle cliniche e dati sanitari

Procedura di Revoca Accessi

Al termine di qualsiasi rapporto di lavoro o collaborazione:

1. Revocare immediatamente tutte le credenziali dell ex collaboratore
2. Cambiare le password dei sistemi a cui aveva accesso
3. Verificare i log di accesso degli ultimi 30 giorni per anomalie
4. Revocare eventuali token 2FA e sessioni attive
5. Documentare la revoca nel registro dei trattamenti GDPR

Non esiste un termine di grazia: la revoca va eseguita il giorno stesso della fine del rapporto.

3. Autenticazione a Due Fattori (2FA/MFA)

I sistemi sanitari sono bersagli prioritari degli attacchi informatici per il valore dei dati che contengono. L autenticazione a due fattori blocca l accesso non autorizzato anche in caso di furto delle credenziali.

3.1 Gerarchia dei Metodi 2FA

Metodo	Come funziona	Livello sicurezza
Chiave hardware (YubiKey)	Dispositivo USB/NFC fisico. Non phishabile. Standard FIDO2.	Massimo
App TOTP (Aegis, Authy)	Codice temporaneo ogni 30 secondi. Offline, indipendente da SMS.	Molto alto
SMS / Chiamata	Vulnerabile a SIM swapping. Accettabile solo dove non ci sono alternative.	Medio - evitare
Email di verifica	Dipende dalla sicurezza dell account email. Sconsigliato.	Basso - evitare

3.2 Dove il 2FA e obbligatorio in uno studio medico

- Email professionale (priorita assoluta)
- Cartella clinica digitale (EMR/EHR)
- PACS e sistemi di imaging diagnostico
- Portali SSN e fascicolo sanitario elettronico (FSE)
- Gestionale di prenotazione e fatturazione
- Cloud storage con documenti clinici
- Sistemi di telemedicina e videoconsulto
- VPN dello studio
- Password manager

Backup dei Codici 2FA: obbligatorio

Se si perde l accesso al secondo fattore si rischia di essere esclusi permanentemente dai sistemi clinici, con impatto diretto sulla cura dei pazienti.

Misure obbligatorie:
- Salvare i codici di recupero forniti al momento dell attivazione
- Stamparli e conservarli in cassaforte o armadio chiuso a chiave
- Non salvarli sul dispositivo usato per il 2FA
- Per app TOTP: backup cifrato del vault (Aegis supporta backup automatico cifrato)

4. Cartella Clinica Digitale e Sistemi Gestionali

La cartella clinica digitale (EMR - Electronic Medical Record) e il nucleo informativo piu sensibile di uno studio medico. La sua protezione richiede misure specifiche che vanno oltre la semplice password.

4.1 Requisiti Minimi per il Software Gestionale

Requisito	Dettaglio
Cifratura dei dati	Il database della cartella clinica deve essere cifrato at-rest. Verificare con il fornitore del software.
Log di accesso	Registro automatico di chi ha acceduto a quale cartella e quando. Obbligatorio per GDPR.
Backup automatico	Backup giornaliero automatico su supporto separato dal server principale.
Aggiornamenti	Il fornitore deve garantire aggiornamenti regolari di sicurezza. Software non aggiornato = vulnerabilita note.
DPA con il fornitore	Il fornitore del gestionale e un responsabile del trattamento ex GDPR: obbligatorio firmare il DPA.
Accesso remoto cifrato	Se il gestionale e accessibile da remoto: solo tramite VPN o connessione cifrata certificata.
Cancellazione sicura	Procedura documentata per la cancellazione sicura dei dati alla fine del rapporto con il fornitore.

4.2 Fascicolo Sanitario Elettronico (FSE) e Portali SSN

Il Fascicolo Sanitario Elettronico e i portali del Servizio Sanitario Nazionale sono sistemi istituzionali con requisiti di accesso specifici. L accesso da parte del medico deve avvenire nel rispetto delle indicazioni ministeriali.

- Usare le credenziali personali fornite dall ASL o dall ordine: mai condividerle
- Accedere al FSE solo da dispositivi professionali protetti e aggiornati
- Non lasciare sessioni aperte senza sorveglianza: blocco automatico entro 5 minuti
- Verificare periodicamente i log di accesso al proprio profilo FSE per rilevare accessi anomali
- In caso di sospetta compromissione: contattare immediatamente l ASL di riferimento

4.3 PACS e Imaging Diagnostico

I sistemi PACS (Picture Archiving and Communication System) contengono immagini diagnostiche (radiografie, TAC, risonanze) con elevata sensibilita. Sono spesso connessi in rete e rappresentano un vettore di attacco sottovalutato.

- Il server PACS non deve essere direttamente esposto a internet: accesso solo tramite VPN o rete interna
- Aggiornare regolarmente il software PACS: i protocolli DICOM hanno storicamente vulnerabilita note

- Accesso alle immagini diagnostiche: solo personale clinico autorizzato, con credenziali individuali
- Backup delle immagini: separato dal backup della cartella clinica, con verifica periodica

5. Email, Telemedicina e Comunicazioni con i Pazienti

Le comunicazioni con i pazienti in ambito medico hanno requisiti di riservatezza particolarmente elevati. Un referto inviato all indirizzo sbagliato, un messaggio intercettato, una cartella condivisa senza cifratura: ognuno di questi eventi e un data breach notificabile al Garante.

5.1 Email Professionale: Requisiti Minimi

Misura	Dettaglio
Dominio proprietario	Usare @nomestudio.it o @nomestudio.medico.it. Mai Gmail o Hotmail personale per comunicazioni cliniche.
SPF, DKIM, DMARC	Record DNS contro lo spoofing del dominio. Configurare con l amministratore di sistema.
Cifratura TLS	Verifica che il provider supporti TLS 1.2 o superiore per la trasmissione delle email.
2FA sull account	Obbligatorio. Vedi Sezione 3.
Archivio cifrato	Le email con dati clinici archiviate devono risiedere su storage cifrato.
PEC per atti formali	Usare la PEC certificata per comunicazioni ufficiali con ASL, ospedali, INPS, tribunali.

5.2 Telemedicina e Videoconsulto

La telemedicina ha avuto una crescita rapida. Le indicazioni del Ministero della Salute (Accordo Stato-Regioni 17 dicembre 2020) e le Linee Guida nazionali di telemedicina stabiliscono requisiti specifici per la gestione dei dati.

Requisito	Dettaglio	Strumenti conformi
Piattaforma certificata	Usare piattaforme che rispettino il GDPR e le linee guida ministeriali. Non usare videochiamante consumer per teleconsulti clinici.	Doxy.me, Whereby for Healthcare, soluzioni ASL
Consenso informato	Il paziente deve esprimere consenso esplicito alla telemedicina prima della seduta, documentato.	Modulo cartaceo o digitale firmato
Registrazione vietata	Non registrare le sessioni senza consenso esplicito scritto del paziente.	N/A
Identificazione paziente	Verificare l identita del paziente all inizio di ogni sessione remota.	Documento d identita via webcam
Documentazione	Redigere e salvare la nota clinica del teleconsulto come qualsiasi altra visita.	Gestionale clinico

Comunicazione dei Referti: Regole Operative

L invio di referti medici via email o messaggistica richiede misure specifiche:

- VIETATO inviare referti con dati clinici via WhatsApp personale
- VIETATO inviare referti non cifrati via email standard a meno che il paziente non abbia espresso consenso informato ai rischi
- CONSENTITO: email cifrata (ProtonMail, S/MIME) con consenso del paziente
- CONSENTITO: portale pazienti autenticato con accesso protetto da credenziali
- CONSENTITO: PEC del paziente per documentazione sanitaria ufficiale

In ogni caso: documentare la modalita di trasmissione nel registro dei trattamenti.

6. Dispositivi, Reti e Smart Working

Un medico che lavora da casa, accede alla cartella clinica da un tablet personale o usa la rete Wi-Fi di uno studio associato introduce rischi che richiedono misure specifiche.

6.1 Configurazione Minima dei Dispositivi

Misura	Dettaglio
Cifratura del disco	BitLocker (Windows) o FileVault (Mac) abilitati su tutti i PC dello studio.
PIN/password dispositivo	Minimo 8 caratteri alfanumerici. Blocco automatico entro 3 minuti di inattivita.
Antivirus/EDR aggiornato	Soluzione antivirus attiva e aggiornata su tutti i PC. Scansione automatica schedulata.
Aggiornamenti OS	Aggiornamenti automatici abilitati. Nessun sistema operativo fuori supporto (es. Windows 7/8).
Separazione uso	I PC dello studio non devono essere usati per navigazione personale, giochi o download non professionali.
Blocco USB	Nei PC con cartelle cliniche: valutare il blocco delle porte USB per prevenire esfiltrazione dati.

6.2 VPN: Obbligatoria per il Lavoro Remoto

Qualsiasi accesso a dati clinici fuori dall ambulatorio deve avvenire tramite VPN. Le reti Wi-Fi pubbliche o domestiche non offrono le garanzie di sicurezza necessarie per i dati sanitari.

- VPN aziendale (WireGuard, OpenVPN) o servizio business verificato: mai VPN gratuite
- La VPN deve essere attiva prima di accedere a qualsiasi sistema clinico da remoto
- Provider VPN consigliati con no-log policy certificata: ProtonVPN Business, Mullvad for Teams
- Il router dello studio deve essere aggiornato e protetto da password sicura (non quella di default)

6.3 Dispositivi Mobili e Tablet

Regole per Smartphone e Tablet in Ambito Clinico

Se si usano dispositivi mobili per accedere a dati clinici o comunicare con i pazienti:

- Dispositivo dedicato allo studio: preferibile a BYOD
- Cifratura del dispositivo abilitata (default su iOS, verificare su Android)
- PIN alfanumerico minimo 8 caratteri, blocco entro 1 minuto
- App cliniche solo da store ufficiali: verificare che rispettino il GDPR
- Cancellazione remota configurata: in caso di smarrimento, attivare immediatamente
- Le foto scattate con lo smartphone professionale non devono finire nel rullino personale
- Non installare app di terze parti non verificate sullo stesso dispositivo usato per i dati clinici

7. Archiviazione Cloud e Strategia di Backup

I dati sanitari archiviati in cloud sono soggetti a requisiti GDPR particolarmente stringenti. La scelta del provider e la configurazione del backup non sono decisioni tecniche: sono decisioni di compliance.

7.1 Criteri Obbligatori per il Cloud Sanitario

Criterio	Requisito specifico per dati sanitari
Server in UE	Obbligatorio per GDPR art. 9. I dati sanitari non possono essere trasferiti fuori UE senza garanzie adeguate.
Cifratura end-to-end	Preferibile la cifratura lato client: il provider non deve poter leggere i dati. Minimo AES-256 at-rest.
DPA specifico per dati sanitari	Il DPA deve esplicitare il trattamento di dati ex art. 9 GDPR. Non accettare DPA generici.
Certificazioni	Cercare provider con certificazione ISO 27001 e, dove disponibile, ISO 27799 (sanita).
Audit log	Log di accesso ai file con possibilita di esportazione per audit Garante.
Right to erasure	Il provider deve garantire cancellazione certificata dei dati su richiesta.

Provider valutati per uso clinico

Provider	Note per uso sanitario	Valutazione
Microsoft 365 Business	Compliance pack disponibile, server EU, BAA (Business Associate Agreement) disponibile per ambienti healthcare.	Accettabile con BAA
Google Workspace Enterprise	DPA disponibile, server EU. Per dati sanitari: necessario piano Enterprise con BAA.	Con cautela + BAA
Nextcloud Healthcare	Self-hosted o provider certificato. Piena conformita GDPR, zero dipendenza da terze parti.	Ottimo per sanita
Tresorit	Cifratura end-to-end lato client, server in UE, DPA solido. Ottima per studi piccoli.	Consigliato

7.2 Strategia di Backup per Dati Clinici

Regola 3-2-1 applicata ai Dati Sanitari
3 copie dei dati clinici (originale + 2 backup)
2 supporti diversi (es. server locale cifrato + cloud EU cifrato)
1 copia off-site fisicamente separata dalla sede dello studio

Frequenza per dati clinici:
- Backup incrementale automatico: ogni giorno (al termine dell orario clinico)
- Backup completo: settimanale
- Test di ripristino: ogni 3 mesi con verifica dell integrita dei dati
- Retention: conservare i backup secondo gli obblighi di legge
  (cartelle cliniche: minimo 10 anni dal termine del trattamento, art. 22 D.Lgs. 502/92)

I backup devono essere cifrati. Un backup non cifrato e un dato esposto.

8. Uso dell Intelligenza Artificiale in Ambito Medico

L AI generativa trova applicazione crescente in medicina: sintesi di note cliniche, supporto alla diagnosi differenziale, redazione di lettere di dimissione, ricerca bibliografica. I rischi per la privacy dei pazienti sono pero reali e richiedono un protocollo esplicito.

8.1 Il Rischio Fondamentale: i Dati del Paziente

Inserire dati clinici identificativi in uno strumento AI cloud equivale a trasmetterli a un server esterno fuori dal proprio controllo. Questo puo violare:

- Il GDPR: i dati sanitari richiedono base giuridica specifica per ogni trattamento
- Il segreto professionale medico: art. 11 Codice Deontologico
- Il consenso informato del paziente: che non copre la condivisione con sistemi AI terzi

Regola Fondamentale: AI e Dati del Paziente

Non inserire MAI in sistemi AI generativi cloud:

- Nome, cognome, data di nascita o codice fiscale del paziente
- Diagnosi, sintomi, terapie o anamnesi specifiche
- Risultati di esami, referti, immagini diagnostiche
- Note cliniche, lettere di dimissione, piani terapeutici
- Qualsiasi dato che consenta di risalire all identita del paziente

L AI puo essere usata per:

- Ricerca bibliografica su patologie generali (senza dati paziente)
- Bozze generiche di documenti amministrativi
- Sintesi di linee guida cliniche pubbliche
- Formattazione e revisione di testi anonimi

8.2 Valutazione degli Strumenti AI per Uso Clinico

Strumento	Note per uso sanitario	Valutazione
AI mediche certificate (es. Nuance DAX, AWS HealthScribe)	Progettate specificamente per la sanita. Conformita HIPAA/GDPR, DPA dedicati, cifratura.	Accettabile con DPA
Microsoft Copilot M365 Enterprise	Con piano Healthcare: BAA disponibile, dati non usati per training, server EU.	Accettabile in Enterprise
LLM locali (Ollama, LM Studio)	Modello eseguito sul dispositivo locale. Nessun dato esce. Massima privacy.	Ottimo per uso clinico
ChatGPT / Gemini gratuiti	Dati possono essere usati per training. ASSOLUTAMENTE NON per dati clinici reali.	VIETATO in ambito clinico

8.3 Procedura di Anonimizzazione

Se si usa l AI per elaborare contenuti clinici, l anonimizzazione preventiva e obbligatoria:

1. Sostituire nome e cognome con identificatori (es. Paziente M, 67 anni)
2. Rimuovere data di nascita esatta: usare fascia d eta (es. 65-70 anni)

3. Eliminare codice fiscale, numero di tessera sanitaria, indirizzo
4. Generalizzare la localizzazione geografica (es. 'nord Italia' invece di citta)
5. Rimuovere date specifiche di ricovero o visita se non necessarie
6. Verificare che il testo anonimizzato non contenga dettagli che consentano la re-identificazione
7. Documentare l uso dello strumento AI nel registro delle attivita dello studio

9. Risposta agli Incidenti di Sicurezza

In ambito sanitario un incidente informatico puo avere conseguenze immediate sulla cura dei pazienti, non solo sulla privacy. Un ransomware che blocca le cartelle cliniche puo rendere impossibile l erogazione delle cure. Il piano di risposta va preparato a mente fredda.

9.1 Classificazione degli Incidenti in Ambito Sanitario

Livello	Esempi in ambito medico	Azione immediata
CRITICO	Ransomware su cartelle cliniche, data breach con dati pazienti esposti, accesso abusivo confermato	Isolare sistemi, attivare backup cartaceo emergenza, notifica Garante entro 72h, valutare impatto clinico
ALTO	Sospetto accesso non autorizzato alle cartelle, phishing cliccato, dispositivo clinico smarrito	Cambiare credenziali, revocare sessioni, analizzare log accessi, valutare notifica Garante
MEDIO	Email sospetta ricevuta, tentativo di login bloccato, vulnerabilita software rilevata	Documentare, applicare contromisure, aggiornare software, verificare backup

9.2 Piano di Continuita Clinica in Caso di Attacco

A differenza di altri contesti professionali, in ambito medico un sistema informatico bloccato puo impedire l erogazione delle cure. E necessario avere un piano di continuita operativa.

Piano di Continuita Clinica (Business Continuity)

Preparare in anticipo:

1. Stampe periodiche di backup cartaceo delle cartelle dei pazienti in cura attiva
2. Lista aggiornata dei pazienti con terapie croniche critiche (sempre accessibile offline)
3. Contatti di emergenza dei pazienti fragili in formato cartaceo
4. Procedure operative di emergenza per la gestione delle visite senza sistema informatico
5. Accordo con tecnico informatico di fiducia reperibile in emergenza

In caso di ransomware: NON PAGARE il riscatto. Contattare il CSIRT Italia.

Il pagamento non garantisce il recupero dei dati e finanzia attivita criminali.

9.3 Procedura di Notifica Data Breach Sanitario

8. CONTENIMENTO: Isolare i sistemi coinvolti dalla rete
9. VALUTAZIONE: Determinare quanti pazienti sono coinvolti e quali dati sono stati esposti
10. NOTIFICA GARANTE: Obbligatoria entro 72 ore se i dati sanitari di pazienti sono coinvolti
11. NOTIFICA PAZIENTI: Obbligatoria se il breach comporta rischio elevato per i diritti dei pazienti
12. DOCUMENTAZIONE: Registro dell incidente con tutte le azioni intraprese
13. ANALISI CAUSE: Identificare e rimuovere la causa della violazione
14. RIPRISTINO: Ripristinare da backup verificati e puliti
15. REVISIONE PROTOCOLLO: Aggiornare le misure di sicurezza per prevenire ricorrenze

Contatti Utili in Caso di Incidente

Garante per la Protezione dei Dati Personali: www.garanteprivacy.it
Notifica data breach online: https://www.garanteprivacy.it/notifica-data-breach
CSIRT Italia (supporto tecnico): https://www.csirt.gov.it | Tel: 06 54 79 99 56
Polizia Postale: https://www.commissariatodips.it
Ordine dei Medici (segnalazione): contattare l OMCeO provinciale di riferimento

Conservare questi contatti in forma stampata: in caso di ransomware
i sistemi digitali potrebbero non essere accessibili.

10. Checklist di Implementazione per Priorita

Questa checklist e progettata per essere stampata e usata operativamente. Ogni voce va spuntata solo dopo aver verificato l effettiva implementazione, non la sola intenzione. Conservare copia firmata per audit GDPR.

Come usare questa checklist

Priorita 1 (entro 30 giorni): misure essenziali, costo zero o minimo, impatto immediato.
Priorita 2 (entro 90 giorni): misure strutturali che richiedono configurazione o acquisto.
Priorita 3 (entro 6 mesi): misure avanzate per uno studio maturo nella sicurezza.

Ogni voce include la verifica da completare prima di spuntarla.
Il campo 'Data' documenta quando la misura e stata implementata.

Priorita 1 — Azioni immediate (entro 30 giorni)

	Azione	Come verificare	Completato
[ ]	Installare un password manager e creare la Master Password	Vault operativo, prima password generata	Data: _____
[ ]	Attivare 2FA sull account email professionale con app TOTP (non SMS)	Login 2FA testato da dispositivo diverso	Data: _____
[ ]	Salvare i codici di recupero 2FA stampati in cassaforte o armadio chiuso	Copia cartacea in luogo fisicamente sicuro	Data: _____
[ ]	Verificare che ogni operatore abbia credenziali personali: vietati account condivisi	Lista utenti con credenziali individuali	Data: _____
[ ]	Verificare PIN alfanumerico minimo 8 caratteri su tutti i dispositivi dello studio	Blocco schermo testato su ogni dispositivo	Data: _____
[ ]	Abilitare aggiornamenti automatici OS su tutti i PC e dispositivi dello studio	Aggiornamenti automatici attivi in impostazioni	Data: _____
[ ]	Verificare che il DPA con il fornitore del gestionale clinico sia firmato	Copia firmata del DPA archiviata	Data: _____
[ ]	Comunicare al team: nessun dato identificativo dei pazienti negli strumenti AI cloud	Comunicazione scritta ricevuta e firmata dal team	Data: _____

Priorita 2 — Azioni strutturali (entro 90 giorni)

	Azione	Come verificare	Completato
[	Attivare 2FA su cartella clinica digitale, PACS,	Lista sistemi con	Data:

]	portali SSN e FSE	2FA abilitato	_____
[ ]	Verificare che il gestionale clinico cifri il database at-rest	Conferma scritta dal fornitore del software	Data: _____
[ ]	Implementare backup 3-2-1 con backup giornaliero automatico cifrato	Schema backup documentato e automatizzato	Data: _____
[ ]	Eseguire primo test di ripristino dal backup: cartelle recuperabili con integrita	File ripristinato verificato, esito documentato	Data: _____
[ ]	Installare e configurare VPN per accesso remoto ai sistemi clinici	VPN testata da postazione remota su cartella reale	Data: _____
[ ]	Attivare cifratura disco (BitLocker/FileVault) su tutti i PC dello studio	Cifratura attiva verificata nelle impostazioni	Data: _____
[ ]	Formare il team su phishing, gestione credenziali e uso sicuro dei dispositivi	Sessione completata, partecipanti documentati	Data: _____
[ ]	Definire e distribuire la policy GDPR per il trattamento dei dati sanitari	Policy firmata da tutto il personale	Data: _____

Priorita 3 — Azioni avanzate (entro 6 mesi)

	Azione	Come verificare	Completato
[ ]	Configurare SPF, DKIM e DMARC sul dominio email dello studio	Test su mxtoolbox.com con risultato PASS	Data: _____
[ ]	Implementare sistema MDM per la gestione centralizzata dei dispositivi mobili	Tutti i dispositivi mobili clinici registrati nel MDM	Data: _____
[ ]	Verificare che la piattaforma di telemedicina rispetti GDPR e linee guida ministeriali	DPA firmato con il provider telemedicina	Data: _____
[ ]	Formalizzare policy di uso dell AI con lista strumenti approvati e procedura anonimizzazione	Policy firmata da tutto il personale clinico	Data: _____
[ ]	Preparare piano di continuita clinica: procedure operative senza sistemi informatici	Documento stampato accessibile in emergenza	Data: _____
[ ]	Condurre simulazione di risposta a incidente (ransomware su cartelle cliniche)	Simulazione completata, lezioni apprese	Data: _____

		documentate	
[ ]	Verificare e aggiornare il registro dei trattamenti GDPR con tutti i sistemi attuali	Registro completo, aggiornato, archiviato	Data: _____
[ ]	Valutare chiavi hardware YubiKey per accessi ai sistemi piu critici	Chiavi configurate e testate sui sistemi critici	Data: _____

Responsabile sicurezza: _____ Data ultima revisione: _____

11. Appendice: Risorse e Riferimenti

11.1 Fonti Normative

- GDPR: eur-lex.europa.eu (Regolamento UE 2016/679)
- Codice Privacy IT: normattiva.it (D.Lgs. 196/2003)
- Garante Privacy - dati sanitari: garanteprivacy.it/temi/sanita
- Linee guida telemedicina: salute.gov.it (Accordo Stato-Regioni 17/12/2020)
- Codice Deontologico Medico: fnomceo.it
- NIS2: eur-lex.europa.eu (Direttiva UE 2022/2555)

11.2 Standard Tecnici

- ISO/IEC 27001:2022: iso.org/standard/82875.html
- ISO 27799 (sanita): iso.org/standard/62777.html
- NIST Cybersecurity Framework: nist.gov/cyberframework
- ENISA - Healthcare Cybersecurity: enisa.europa.eu/publications
- Have I Been Pwned: haveibeenpwned.com

11.3 Strumenti Citati

- Bitwarden: bitwarden.com | KeePassXC: keepassxc.org
- Aegis Authenticator: getaegis.app | YubiKey: yubico.com
- ProtonMail / ProtonDrive: proton.me | Tresorit: tresorit.com
- ProtonVPN: protonvpn.com | Mullvad: mullvad.net
- Nextcloud: nextcloud.com | Signal: signal.org
- Ollama (AI locale): ollama.ai
- CSIRT Italia: csirt.gov.it | Garante notifiche breach: garanteprivacy.it

11.4 Log delle Revisioni

Versione	Data	Note
1.0	2025	Prima pubblicazione. Centuria Foundation — centuriafoundation.pl

Centuria Foundation

centuriafoundation.pl