TE.RI. – TERAPIA RIABILITATIVA S.R.L.

REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI

ai sensi del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018, e dei principi del Codice di Deontologia delle Professioni Sanitarie

Titolare del Trattamento	TE.RI. – Terapia Riabilitativa S.r.l. – Sig.ra **Mara Villani** (Legale Rappresentante) Via Renato Simoni, 29/31 00157 Roma PEC: terisrl@legalmail.it
DPO **(Responsabile della Protezione dei Dati)**	Avv. **Maurizio Belloni** dpo@centroteri.com Tel. +39 06.58230712
Versione	v. 1.0
Data di adozione	25 giugno 2026

Destinatari	Tutto il personale dipendente, i collaboratori, i consulenti, i tirocinanti e chiunque operi per conto di TE.RI. S.r.l. con accesso a dati personali.
Prossima revisione	Entro il 01 giugno 2027, o anticipatamente in caso di variazioni normative/organizzative significative

0.1 INDICE

- **PREMESSA** – Perché esiste questo documento e a chi si applica
- **SEZIONE I** – I principi fondamentali (Artt. 1–5)
- **SEZIONE II** – Regole operative per il trattamento dei dati (Artt. 6–13)
- **SEZIONE III** – Sicurezza informatica e gestione delle credenziali (Artt. 14–19)
- **SEZIONE IV** – Dati sanitari e attività domiciliare (Artt. 20–24)
- **SEZIONE V** – I diritti degli interessati (Artt. 25–28)
- **SEZIONE VI** – Violazioni dei dati, segnalazioni e sanzioni (Artt. 29–33)
- **SEZIONE VIII** – Disposizioni finali (Artt. 36–38)
- **ALLEGATO A** – Tabella riepilogativa dei comportamenti vietati
- **ALLEGATO B** – Dichiarazione di presa visione e accettazione



0.2 PREMESSA – Perché esiste questo documento e a chi si applica

TE.RI. – Terapia Riabilitativa S.r.l. (di seguito "la Struttura") tratta ogni giorno dati personali di pazienti, dipendenti, collaboratori e fornitori.

Tra questi, una parte significativa riguarda lo **stato di salute delle persone**: si tratta di informazioni tra le più delicate e protette dall'ordinamento giuridico.

Il presente **Regolamento Interno per la Protezione dei Dati Personali** (di seguito "Regolamento" o "Codice") nasce dall'obbligo giuridico di adottare misure organizzative adeguate ai sensi dell'art. 5, par. 2 GDPR (principio di *accountability* – responsabilizzazione), ma prima ancora dall'impegno etico della Struttura verso i propri pazienti e verso chi lavora al suo interno.

Il rispetto di questo documento non è facoltativo.

Chi opera per conto della Struttura – a prescindere dal tipo di contratto (dipendente, collaboratore, consulente, tirocinante, volontario) – è tenuto a conoscere e applicare le regole qui contenute **dal primo giorno di attività**.

⚠ ATTENZIONE – Le conseguenze della violazione.

Violare le regole di questo Codice può comportare:

provvedimento disciplinare, fino al licenziamento per giusta causa (art. 2104 c.c. e CCNL applicabile);

responsabilità civile per i danni causati alle persone coinvolte (art. 82 GDPR);

responsabilità penale per i reati previsti dagli artt. 167–172 del D.Lgs. 196/2003;

sanzione amministrativa fino a **€ 20.000.000** o al **4% del fatturato mondiale annuo** della Struttura (art. 83 GDPR).



0.3 SEZIONE I – I PRINCIPI FONDAMENTALI

Cosa significa questa sezione?

Il GDPR stabilisce sei principi base che devono guidare qualsiasi trattamento di dati personali.

Ogni regola operativa contenuta in questo Codice discende da uno o più di questi principi.

Conoscerli aiuta a capire il *perché* delle regole.

0.3.1 Art. 1 – LICEITÀ, CORRETTEZZA E TRASPARENZA

(art. 5, par. 1, lett. a) GDPR)

Ogni trattamento di dati personali deve avere una **base giuridica valida**: il consenso dell'interessato, un obbligo di legge, l'esecuzione di un contratto o un'altra condizione prevista dall'art. 6 (o dall'art. 9 per i dati sanitari) del GDPR.

In pratica: non si raccolgono dati senza un motivo legale chiaro.

Non si usano i dati per scopi diversi da quelli comunicati all'interessato.

L'interessato ha sempre diritto a sapere chi tratta i suoi dati e perché.

0.3.2 Art. 2 – LIMITAZIONE DELLA FINALITÀ

(art. 5, par. 1, lett. b) GDPR)

I dati personali sono raccolti per **finalità determinate, esplicite e legittime**.

Non possono essere riutilizzati per scopi incompatibili con quello originario.

In pratica: i dati sanitari dei pazienti raccolti per finalità terapeutiche **non possono** essere usati per scopi commerciali, di ricerca non autorizzata o per qualunque altro scopo non connesso alla cura e alla riabilitazione del paziente.

0.3.3 Art. 3 – MINIMIZZAZIONE DEI DATI

(art. 5, par. 1, lett. c) GDPR)

Si raccolgono e trattano **solo i dati strettamente necessari** per la finalità dichiarata.

È vietato raccogliere dati "per precauzione" o in eccesso rispetto alle reali necessità operative.

In pratica: (*esempio*) durante le visite domiciliari, si porta al domicilio del paziente **il minimo indispensabile** di documentazione.

Non si raccolgono informazioni aggiuntive che non servono per la seduta.

0.3.4 Art. 4 – ESATTEZZA

(art. 5, par. 1, lett. d) GDPR)

I dati trattati devono essere **esatti e aggiornati**.

Eventuali errori o dati obsoleti devono essere segnalati e corretti senza ritardo.

In pratica: se si riscontra un'inesattezza nei dati di un paziente o di un altro interessato, si segnala immediatamente al Referente interno.

Non si modifica autonomamente la documentazione senza autorizzazione.

0.3.5 Art. 5 – INTEGRITÀ E RISERVATEZZA

(art. 5, par. 1, lett. f) GDPR)

I dati personali devono essere protetti da **accessi non autorizzati, perdita, distruzione o divulgazione accidentale**, attraverso misure tecniche e organizzative adeguate.

In pratica, questo principio impone a tutto il personale di:

a) non divulgare informazioni sui pazienti a persone non autorizzate, nemmeno involontariamente;
b) non lasciare documenti contenenti dati personali incustoditi (scrivania, stampante, autovettura);
c) non condividere le proprie credenziali di accesso con nessuno;

d) adottare tutte le precauzioni necessarie per impedire accessi non autorizzati ai sistemi.

0.4 SEZIONE II – REGOLE OPERATIVE PER IL TRATTAMENTO DEI DATI

0.4.1 Art. 6 – CHI PUÒ TRATTARE I DATI E IN CHE MISURA (AUTORIZZAZIONE)

Il personale è autorizzato a trattare **solo i dati personali indicati nella propria lettera di incarico**, per le finalità e con gli strumenti ivi specificati.

Qualsiasi trattamento non espressamente autorizzato è vietato.

In caso di dubbio sull'ampiezza della propria autorizzazione, contattare preventivamente il Referente interno o il DPO prima di procedere.

0.4.2 Art. 7 – COME SI RACCOLGONO I DATI

In fase di raccolta, il personale deve:

Obbligo	Descrizione
✅ Informativa	Consegnare o illustrare l'informativa privacy (artt. 13–14 GDPR) **prima o al momento** della raccolta dei dati
✅ Consenso	Raccogliere il consenso scritto quando è la base giuridica del trattamento (es. finalità non sanitarie obbligatorie)
✅ Minimizzazione	Raccogliere **solo i dati necessari** per la finalità dichiarata
✅ Verifica identità	Verificare l'identità dell'interessato prima di fornire informazioni o accedere ai suoi dati



✅ Minori	Non raccogliere dati di minori senza il consenso del genitore/tutore, salvo urgenza sanitaria

0.4.3 Art. 8 – QUANDO SI POSSONO COMUNICARE I DATI A TERZI

La comunicazione di dati personali a soggetti terzi (familiari, colleghi di altre strutture, medici, autorità) è consentita **solo nei seguenti casi**:

1. Su richiesta e/o consenso **esplicito e documentato per iscritto** dell'interessato;
2. Per **adempiere a obblighi di legge** (es. segnalazioni obbligatorie alle autorità sanitarie);
3. Per la **continuità terapeutica**, nei limiti dello stretto necessario (es. ove necessario comunicazione al medico di base);
4. Su **richiesta dell'autorità giudiziaria o di pubblica sicurezza**, previa verifica della legittimità della richiesta.

🚫 **VIETATO – Regola assoluta:**

È vietato comunicare dati sanitari dei pazienti a familiari, conviventi o terzi **senza il consenso esplicito del paziente**, salvo i casi di legge (es. incapacità del paziente).
La comunicazione a colleghi avviene esclusivamente attraverso i canali ufficiali della Struttura e per necessità cliniche documentate.

0.4.4 Art. 9 – USO DEGLI STRUMENTI INFORMATICI AZIENDALI

Gli strumenti informatici aziendali (PC, software gestionale) sono riservati **esclusivamente alle attività lavorative**.

È VIETATO	**MOTIVAZIONE**
Usarli per finalità personali	Rischio di accesso non autorizzato a dati aziendali
Installare software non autorizzato	Rischio di malware e violazioni di sicurezza
Navigare su siti non pertinenti all'attività	Rischio di accesso a contenuti dannosi
Usare account e-mail personali per dati aziendali o di pazienti	Rischio di data breach
Memorizzare dati di pazienti su dispositivi personali non autorizzati (smartphone privati, chiavette USB, cloud personali)	Violazione dei principi di sicurezza e minimizzazione

A fine sessione di lavoro: disconnettersi dai sistemi e bloccare il PC (tasto Windows + L, o screensaver automatico).

0.4.5 Art. 10 – COMUNICAZIONI ELETTRONICHE E SOCIAL MEDIA

Il segreto professionale e la riservatezza si applicano **in qualsiasi forma di comunicazione**, inclusi messaggi, email e post sui social.

🚫 **ASSOLUTAMENTE VIETATO:**

a) Pubblicare o condividere su piattaforme social (Facebook, Instagram, TikTok, LinkedIn, ecc.) immagini, video o informazioni che permettano l'identificazione – anche indiretta – di un paziente;

b) Inviare dati sanitari tramite app di messaggistica (WhatsApp, Telegram, ecc.) senza autorizzazione del Referente interno Privacy;

c) Discutere di casi clinici in luoghi pubblici o in spazi condivisi dove altri possono sentire;

d) Condividere credenziali di accesso tramite e-mail, messaggi o altri canali non sicuri.

📌 **ESEMPIO CONCRETO – Cosa NON fare**

❌ Fotografare un documento clinico con il proprio smartphone e inviarlo via WhatsApp a un collega, **anche se il collega è un professionista sanitario della stessa struttura**, è vietato. Occorre usare i canali ufficiali (sistema gestionale, e-mail aziendale; pec).

❌ Pubblicare sui propri profili social una foto che ritragga – anche sullo sfondo – un paziente in terapia, anche senza mostrarne il volto, senza il suo consenso scritto esplicito.





0.4.6 Art. 11 – GESTIONE DELLA DOCUMENTAZIONE CARTACEA

Regola	Dettaglio
✅ Archiviazione sicura	Al termine di ogni sessione, riporre i documenti in archivi chiusi a chiave
🚫 No documenti incustoditi	Vietato lasciare documenti su scrivanie, stampanti o fotocopiatrici
✅ Distruzione sicura	Le stampe non necessarie vanno distrutte con il trita-documenti, non gettate nel cestino
🚫 No fotocopie non autorizzate	Vietato fotocopiare o fotografare documenti senza specifica autorizzazione
🚫 No uscita dalla sede	I documenti cartacei con dati sanitari non possono uscire dalla sede senza autorizzazione scritta del Referente interno Privacy e nel rispetto della Policy aziendale per il trasporto dei dati



0.4.7 Art. 12 – CONSERVAZIONE E CANCELLAZIONE DEI DATI

I dati personali non si conservano più a lungo del necessario (art. 5, par. 1, lett. e) GDPR).

Il personale è tenuto a:

a) rispettare i **termini di conservazione** indicati nel Registro delle Attività di Trattamento (RAT) e nelle procedure interne;
b) segnalare al Referente interno Privacy eventuali archivi o dati conservati oltre i termini previsti;
c) **non eliminare autonomamente** dati personali senza autorizzazione, salvo le procedure ordinarie di archiviazione.

0.4.8 Art. 13 – RISERVATEZZA E SEGRETO PROFESSIONALE

Il personale sanitario è tenuto al rispetto del **segreto professionale** (art. 622 c.p.) e delle norme deontologiche della propria professione.

L'obbligo di riservatezza:

a) riguarda **qualsiasi informazione** di cui il professionista è venuto a conoscenza nell'esercizio delle proprie funzioni;
b) si estende a **ogni forma di comunicazione**: scritta, orale, informatica;
c) **permane dopo la cessazione** del rapporto di lavoro o di collaborazione;
d) si applica anche **nei confronti di colleghi non coinvolti** nel trattamento del paziente.

0.5 SEZIONE III – SICUREZZA INFORMATICA E GESTIONE DELLE CREDENZIALI

0.5.1 Art. 14 – CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione (User ID e password) sono **strettamente personali e non cedibili a nessuno, per nessun motivo**.

Regole obbligatorie:

Obbligo	Dettaglio
Cambio al primo accesso	Modificare la password assegnata prima di iniziare a lavorare
Complessità della password	Almeno 8 caratteri, con lettere maiuscole, minuscole, numeri e caratteri speciali
Password vietate	Nome, cognome, data di nascita, nome del paziente, sequenze ovvie (es. "12345678", "password")
Rinnovo periodico	Ogni 6 mesi per dati comuni; ogni 3 mesi per dati sanitari
Non comunicare la password	A nessuno: né colleghi, né superiori, né amministratori di sistema
Custodia sicura	Conservare la password in luogo sicuro

Segnalazione immediata	Comunicare subito al Referente interno Privacy e all'Amministratore di Sistema qualsiasi sospetto di uso non autorizzato delle proprie credenziali

0.5.2 Art. 15 – USO SICURO DEL PC E DEI DISPOSITIVI

Obbligo	Dettaglio
✅ Screensaver automatico	Attivare il blocco automatico dopo 5 minuti di inattività
✅ Blocco manuale	Bloccare sempre il PC quando ci si allontana dalla postazione, anche brevemente
🚫 No sessioni aperte incustodite	Non lasciare il PC con sessioni aperte contenenti dati personali
🚫 No USB personali	Non collegare dispositivi USB personali non autorizzati al PC aziendale

✅ Segnalazione anomalie	Comunicare immediatamente all'Amministratore di Sistema qualsiasi comportamento anomalo del sistema
🚫 No phishing	Non aprire allegati da mittenti sconosciuti; non cliccare su link sospetti

0.5.3 Art. 16 – GESTIONE DELLA POSTA ELETTRONICA AZIENDALE

a) La casella e-mail aziendale è riservata a **sole comunicazioni professionali**;
b) Prima di inviare documenti con dati personali, verificare che il **destinatario sia corretto** e che il canale sia adeguato (per dati sanitari, preferire il sistema gestionale o canali quali email verificata o pec);
c) Non inviare dati sanitari a indirizzi e-mail personali del paziente senza il suo consenso esplicito;
d) **In caso di invio erroneo:** segnalare immediatamente al Referente interno Privacy e al DPO;
e) Non usare la casella aziendale per iscriversi a servizi o siti non correlati all'attività lavorativa.

0.5.4 Art. 17 – BACKUP E PROTEZIONE DEI DATI

Il personale collabora alle procedure di backup indicate dall'Amministratore di Sistema:

a) salvare i documenti di lavoro **nelle cartelle indicate**, non in locale sul PC, per garantirne l'inclusione nel backup automatico;
b) non cancellare file o cartelle di rete senza autorizzazione;
c) segnalare immediatamente all'Amministratore di Sistema qualsiasi perdita o danneggiamento di dati.

0.5.5 Art. 18 – PROTEZIONE DA VIRUS E ATTACCHI INFORMATICI

Il personale è la **prima linea di difesa** contro gli attacchi informatici.

a) 🚫 Non disabilitare o aggirare i sistemi di protezione (antivirus, firewall);
b) ✅ Aggiornare il sistema operativo e i software quando richiesto;
c) ✅ Prestare massima attenzione alle e-mail di phishing;
d) ✅ Segnalare immediatamente all'Amministratore di Sistema qualsiasi sospetto di infezione da virus o ransomware.

🛡 **COME RICONOSCERE UN'E-MAIL DI PHISHING:**

Prestare attenzione alle e-mail che: provengono da indirizzi sospetti o con dominio errato (es. "asl-roma@gmail.com"); richiedono con urgenza di cliccare un link o inserire le credenziali; contengono errori grammaticali o di formattazione insoliti; hanno allegati inattesi (.exe, .zip, macro Office); richiedono il trasferimento di denaro o dati bancari.

In caso di dubbio: NON cliccare, NON rispondere.

Art. 19 – DISPOSITIVI MOBILI E LAVORO DA REMOTO (ove presenti)

Regola	Dettaglio
✅ PIN/password	I dispositivi mobili aziendali devono essere protetti da PIN o password (**attualmente non ve ne sono**)
✅ Cifratura	I dispositivi mobili contenenti dati personali devono essere cifrati
✅ VPN obbligatoria	In caso di connessione remota ai sistemi aziendali, usare sempre la VPN aziendale (**attualmente non vi è alcuna procedura in tal senso**)
🚫 No Wi-Fi pubblico	Vietato connettersi ai sistemi aziendali tramite reti Wi-Fi pubbliche non protette (bar, alberghi, stazioni)

✅ Furto/smarrimento	In caso di furto o smarrimento: segnalare immediatamente al Referente interno e all'Amministratore di Sistema per la cancellazione remota dei dati

0.6 SEZIONE IV – DATI SANITARI E ATTIVITÀ DOMICILIARE

Perché questa sezione è particolarmente importante?

I dati relativi alla salute sono **categorie particolari di dati** (art. 9 GDPR):
godono di una tutela rafforzata perché la loro divulgazione può causare danni gravi e irreversibili alle persone.

Il personale sanitario che opera anche al domicilio del paziente è esposto a rischi aggiuntivi che richiedono attenzioni specifiche.

0.6.1 Art. 20 – TRATTAMENTO DEI DATI SANITARI – OBBLIGHI SPECIFICI

Il personale sanitario autorizzato è tenuto a:

a) accedere alle cartelle cliniche **solo in relazione alla propria specifica attività terapeutica**;
b) 🚫 **non consultare** cartelle cliniche di pazienti non in carico, anche se tecnicamente accessibili dal sistema;
c) trattare i dati sanitari con la massima riservatezza, **anche nei confronti di colleghi non coinvolti** nel trattamento;
d) non discutere di casi clinici in **aree comuni** (sale d'attesa, corridoi,) o in presenza di persone non autorizzate;

e) garantire che le comunicazioni sulla salute dei pazienti avvengano in **locali idonei** a garantire la privacy (colloqui privati, non ad alta voce in reception);

f) trattare i dati sanitari **in forma anonima** ove possibile, separando i dati identificativi da quelli clinici.

0.6.2 Art. 21 – REGOLE SPECIFICHE PER IL PERSONALE CHE EFFETTUA VISITE DOMICILIARI

(Fisioterapisti, logopedisti, psicologi, assistenti sociali, logoterapisti)

0.6.2.1 21.1 – Documentazione cartacea in mobilità

Regola	Dettaglio
☑ Minimizzazione	Portare al domicilio **solo i documenti strettamente necessari** per la seduta
☑ Custodia	Conservare i documenti in una cartella/borsa chiusa, non visibile a terzi, **mai incustodita**

🚫 No documenti in auto	**Vietato** lasciare documenti con dati sanitari nell'autovettura, nemmeno per brevi periodi, nemmeno nel bagagliaio
✅ Al termine della visita	Riporre immediatamente tutta la documentazione nella cartella chiusa
✅ Al rientro in sede	Consegnare o riporre la documentazione negli archivi sicuri

0.6.2.2 <u>21.2 – In caso di furto o smarrimento</u>

1. Presentare **immediatamente** denuncia alle autorità di pubblica sicurezza;
2. ⚠ **OBBLIGO ASSOLUTO:** notificare l'accaduto al Titolare e al DPO **entro la stessa giornata lavorativa**, fornendo ogni dettaglio (tipo di documenti sottratti, pazienti coinvolti, luogo e ora dell'evento);
3. **Non tentare di gestire autonomamente l'incidente:** il Titolare ha l'obbligo di notifica al Garante **entro 72 ore** dalla scoperta della violazione (art. 33 GDPR).

📌 Art. 22 – UTILIZZO DI DISPOSITIVI ELETTRONICI DURANTE LE VISITE DOMICILIARI

L'utilizzo di tablet o smartphone per consultare o aggiornare cartelle cliniche durante le visite domiciliari è soggetto a condizioni rigorose:

Condizione	Dettaglio
✅ Dispositivo autorizzato	Aziendale o formalmente autorizzato dal Titolare
✅ Cifratura e PIN	Il dispositivo deve essere cifrato e protetto da PIN/password
✅ VPN	La connessione al sistema gestionale avviene tramite VPN aziendale (**la Struttura attualmente non dispone di VPN**)
🚫 No fotografie	Vietato fotografare documenti clinici con dispositivi personali non autorizzati

✅ Furto/smarrimento	Segnalare immediatamente al Referente interno Privacy e all'Amministratore di Sistema per l'attivazione della cancellazione remota

0.6.3 Art. 23 – COMUNICAZIONI CON IL PAZIENTE E I FAMILIARI

Situazione	Regola
Paziente adulto capace	Fornire informazioni sanitarie **esclusivamente al paziente,** salvo suo consenso esplicito a coinvolgere i familiari
Paziente minore	Rivolgersi ai genitori o al tutore legale, rispettando comunque il diritto del minore all'informazione adeguata alla propria età
Paziente con capacità ridotta	Seguire le indicazioni del tutore/amministratore di sostegno, documentando ogni comunicazione rilevante in cartella

🚫 Familiari non indicati	Non fornire informazioni cliniche a familiari che il paziente non abbia espressamente indicato come destinatari

0.6.4 Art. 24 – RISERVATEZZA NELL'AMBIENTE DOMICILIARE

L'accesso al domicilio del paziente comporta la conoscenza di informazioni aggiuntive (condizioni abitative, dinamiche familiari, situazione economica) che – pur non rientrando nella cartella clinica – fanno parte della sfera **strettamente privata** della persona.

Il personale è tenuto a:

a) trattare con **assoluta riservatezza** tutte le informazioni acquisite durante le visite domiciliari, anche quelle non strettamente sanitarie;
b) non divulgare a terzi informazioni sulle condizioni abitative, familiari o economiche del paziente;
c) segnalare al Referente interno Privacy eventuali **situazioni di rischio** per il paziente (abusi, trascuratezza) secondo le procedure previste dalla normativa sanitaria vigente.

0.7 SEZIONE V – I DIRITTI DEGLI INTERESSATI

Chi sono gli "interessati"?

Sono tutte le persone fisiche i cui dati personali vengono trattati dalla Struttura: pazienti, dipendenti, collaboratori, familiari, fornitori, ecc.

0.7.1 Art. 25 – CATALOGO DEI DIRITTI DEGLI INTERESSATI

Il GDPR (artt. 15–22) riconosce alle persone i seguenti diritti:

Diritto	Cosa significa in concreto
Diritto di accesso (art. 15)	L'interessato può chiedere conferma del trattamento dei propri dati, ottenerne copia e conoscere finalità, destinatari, tempi di conservazione e diritti esercitabili
Diritto di rettifica (art. 16)	L'interessato può chiedere la correzione di dati inesatti e l'integrazione di dati incompleti

Diritto alla cancellazione (art. 17)	L'interessato può chiedere la cancellazione dei propri dati quando, ad esempio, non sono più necessari alle finalità o ha revocato il consenso. **Attenzione:** non si applica ai dati sanitari conservati per obbligo di legge
Diritto alla limitazione (art. 18)	L'interessato può chiedere che i propri dati non vengano ulteriormente trattati in determinate circostanze (es. se ne contesta l'esattezza)
Diritto alla portabilità (art. 20)	L'interessato può richiedere i propri dati in formato strutturato e leggibile per trasmetterli a un altro titolare (es. cambio di struttura sanitaria)
Diritto di opposizione (art. 21)	L'interessato può opporsi al trattamento basato sul legittimo interesse del Titolare

Diritto di non essere sottoposto a decisioni automatizzate (art. 22)	L'interessato ha il diritto di non essere soggetto a decisioni basate esclusivamente su trattamenti automatizzati che producano effetti giuridici significativi

0.7.2 Art. 26 – COSA FARE QUANDO UN PAZIENTE O UN ALTRO INTERESSATO ESERCITA UN DIRITTO

In caso di richiesta di esercizio di un diritto (anche verbale), il personale deve:

1. **Ricevere la richiesta** (anche verbale);
2. **Trasmetterla immediatamente** al Referente interno e al DPO (dpo@centroteri.com) – non rispondere autonomamente;
3. **Non opporre rifiuti** senza autorizzazione del DPO o del Referente interno Privacy;
4. **Verificare l'identità** del richiedente prima di fornire qualsiasi informazione.

Tempi di risposta: Il Titolare fornisce riscontro **entro 30 giorni** dalla ricezione, prorogabili di ulteriori 60 giorni in casi complessi (con comunicazione della proroga entro i primi 30 giorni).

0.7.3 Art. 27 – INFORMATIVA AGLI INTERESSATI

Il personale addetto all'accettazione e al front-office è tenuto a consegnare l'**informativa privacy** (art. 13 GDPR) a ogni nuovo paziente, **prima o al momento della raccolta dei suoi dati**. L'avvenuta consegna deve essere documentata con la firma del paziente o del tutore legale.

0.7.4 Art. 28 – GESTIONE DEL CONSENSO

Nei casi in cui il trattamento richieda il consenso dell'interessato (es. comunicazione dei dati a terzi non prevista da obblighi di legge, utilizzo per motivi di ricerca,), il personale deve:

1. raccogliere il consenso **in forma scritta, specifica, informata e non ambigua**, prima di procedere al trattamento;
2. **conservare la documentazione del consenso** in modo da poterla esibire al Garante su richiesta;
3. informare l'interessato del diritto di **revocare il consenso** in qualsiasi momento, senza che ciò pregiudichi la liceità del trattamento precedente;
4. **cessare immediatamente** il trattamento basato sul consenso in caso di revoca.

0.8 SEZIONE VI – VIOLAZIONI DEI DATI, SEGNALAZIONI E SANZIONI

0.8.1 Art. 29 – COSA FARE IN CASO DI VIOLAZIONE DEI DATI (DATA BREACH)

Una **violazione dei dati personali** (data breach) è qualsiasi evento che comporti – accidentalmente o illecitamente – la **distruzione, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato** a dati personali.



⚠ REGOLA ASSOLUTA: SEGNALARE SUBITO

Chiunque rilevi o sospetti un data breach deve:

1. **Segnalare immediatamente** – anche verbalmente – al Referente interno e al DPO (dpo@centroteri.com), seguita da **conferma scritta entro poche ore**;
2. **Non tentare di gestire autonomamente** la violazione né di "nasconderla": la mancata segnalazione è essa stessa una **violazione disciplinare grave**;
3. Fornire al Titolare tutte le informazioni utili: natura della violazione, dati coinvolti, numero approssimativo di interessati, cause, misure già adottate.

Il Titolare, con il supporto del DPO, valuta se notificare la violazione al **Garante entro 72 ore** (art. 33 GDPR) e, se il rischio per gli interessati è elevato, se comunicarlo **direttamente agli interessati** (art. 34 GDPR).

0.8.2 Art. 30 – ESEMPI DI COMPORTAMENTI CHE COSTITUISCONO UN DATA BREACH

Tipo	Esempi concreti
Riservatezza	Furto o smarrimento di documenti cartacei con dati sanitari - Invio di dati sanitari a destinatario errato - Accesso non autorizzato a cartelle cliniche - Pubblicazione di dati su social media - Comunicazione non autorizzata a familiari.

Disponibilità	Cancellazione accidentale di dati - Guasto hardware con perdita di dati non recuperabili - Attacco ransomware con cifratura dei dati - Interruzione del sistema senza backup
Integrità	Modifica non autorizzata di dati in cartella clinica - Corruzione di file da malware - Alterazione di documentazione sanitaria

0.8.3 Art. 31 – SEGNALAZIONE DI COMPORTAMENTI SCORRETTI – WHISTLEBLOWING

Il personale che venga a conoscenza di comportamenti di colleghi o superiori che violino il presente Regolamento, la normativa privacy o le procedure interne è **incoraggiato a segnalarlo** al DPO (dpo@centroteri.com) o al Referente interno, anche in forma riservata.

La Struttura garantisce la **piena tutela del segnalante** da qualsiasi forma di ritorsione, ai sensi del D.Lgs. 24/2023 (recepimento Direttiva UE 2019/1937 – Whistleblowing).

0.8.4 Art. 32 – LE CONSEGUENZE DELLE VIOLAZIONI

Le violazioni del presente Regolamento comportano conseguenze proporzionate alla gravità dell'infrazione:

Gravità	Esempi	Conseguenze
LIEVE	Dimenticanza occasionale di una procedura	Richiamo verbale o scritto; Formazione integrativa obbligatoria Verifica del rispetto delle procedure.

MEDIA	Violazione reiterata. Negligenza nella gestione delle credenziali	Provvedimento disciplinare scritto (biasimo, multa); Sospensione temporanea dell'accesso a determinati sistemi; Formazione aggiuntiva obbligatoria.
GRAVE	Divulgazione di dati sanitari Accesso abusivo ai sistemi Omessa segnalazione di data breach	Provvedimento disciplinare grave (sospensione senza retribuzione); Licenziamento per giusta causa o giustificato motivo; Segnalazione all'autorità giudiziaria in caso di reato; Comunicazione all'Ordine professionale competente

Ferme le conseguenze disciplinari, il personale può essere chiamato a rispondere:

- **civilmente** per i danni causati agli interessati (art. 82 GDPR);
- **penalmente** per i reati previsti dagli artt. 167–172 del D.Lgs. 196/2003.

0.8.5 Art. 35 – AGGIORNAMENTO DEL REGOLAMENTO

Il presente Regolamento è soggetto a revisione **almeno annuale** e ogni volta che intervengano modifiche normative rilevanti, variazioni organizzative significative o incidenti che evidenzino la necessità di aggiornarlo.

Ogni aggiornamento è comunicato a tutto il personale, che è tenuto a **firmarne la presa visione** come condizione per la continuazione dell'attività.

0.9 SEZIONE VIII – DISPOSIZIONI FINALI

0.9.1 Art. 37 – OBBLIGO DI COLLABORAZIONE

Il personale è tenuto a collaborare attivamente con il Titolare, il Referente interno e il DPO. In particolare:

a) segnalare tempestivamente qualsiasi situazione che possa comportare un rischio per i dati personali trattati;
b) partecipare attivamente alle sessioni di formazione;
c) contribuire al miglioramento continuo delle procedure, segnalando al DPO eventuali criticità o suggerimenti.

0.9.2 Art. 38 – PUNTI DI CONTATTO

Per qualsiasi dubbio, chiarimento o segnalazione, il personale può rivolgersi a:

Soggetto	Riferimenti
DPO – Data Protection Officer	Avv. **Maurizio Belloni** dpo@centroteri.com – Tel. +39 06.58230712 *(disponibile per qualsiasi chiarimento, segnalazione o consulenza in materia di protezione dei dati)*
Garante per la Protezione dei Dati Personali	www.garanteprivacy.it Piazza Venezia, 11 – 00187 Roma – Tel. +39 06.696771 *(per l'esercizio dei diritti e per reclami)*

0.10 ALLEGATO A – TABELLA RIEPILOGATIVA DEI COMPORTAMENTI VIETATI

(Elenco esemplificativo e non esaustivo)

N.	Comportamento vietato	Norma violata	Possibile conseguenza
1	Comunicare la propria password a colleghi o superiori	Art. 32 GDPR; Codice Art. 14	Disciplinare; responsabilità civile in caso di danno
2	Accedere a cartelle cliniche di pazienti non in carico	Art. 9 GDPR; Art. 167 D.Lgs. 196/2003	Disciplinare grave; responsabilità penale
3	Pubblicare su social media informazioni o immagini che identifichino pazienti	Art. 9 e art. 5 GDPR; segreto professionale	Disciplinare grave; responsabilità penale; denuncia all'Ordine professionale
4	Inviare dati sanitari via WhatsApp o altri canali non sicuri senza autorizzazione	Art. 32 GDPR; Codice Art. 10	Disciplinare; responsabilità civile
5	Lasciare documenti sanitari incustoditi (scrivania, stampante, autovettura)	Art. 32 GDPR; Codice Artt. 11, 21	Disciplinare; responsabilità civile in caso di data breach
6	Non segnalare immediatamente furto/smarrimento di dati	Art. 33 GDPR; Codice Art. 29	Disciplinare grave; sanzione amministrativa
7	Fornire informazioni sanitarie a familiari senza consenso del paziente	Art. 9 GDPR; Art. 622 c.p.	Disciplinare grave; responsabilità penale
8	Utilizzare strumenti informatici aziendali per uso personale	Codice Art. 9; policy aziendale	Disciplinare
9	Disabilitare antivirus o sistemi di protezione del PC	Art. 32 GDPR; Codice Art. 18	Disciplinare grave; responsabilità civile in caso di danno

10	Non consegnare l'informativa privacy ai nuovi pazienti	Art. 13 GDPR	Disciplinare; sanzione amministrativa al Titolare (art. 83 GDPR)
11	Raccogliere dati eccedenti rispetto alle finalità del trattamento	Art. 5, par. 1, lett. c) GDPR	Disciplinare; sanzione amministrativa al Titolare
12	Conservare dati personali oltre i termini previsti	Art. 5, par. 1, lett. e) GDPR	Disciplinare; sanzione amministrativa al Titolare
13	Fotografare documenti clinici con smartphone personale	Art. 9 GDPR; Codice Artt. 10, 22	Disciplinare grave; responsabilità penale
14	Discutere di casi clinici in aree comuni o in presenza di terzi non autorizzati	Art. 9 GDPR; segreto professionale	Disciplinare; responsabilità civile e penale
15	Non partecipare alla formazione obbligatoria senza giustificato motivo	Codice Art. 34; M.O.P.	Disciplinare

0.11 ALLEGATO B – DICHIARAZIONE DI PRESA VISIONE E ACCETTAZIONE

(da compilare in duplice copia: una conservata dalla Struttura, una trattenuta dal sottoscritto)

DICHIARAZIONE DI PRESA VISIONE, COMPRENSIONE E ACCETTAZIONE DEL REGOLAMENTO INTERNO PER LA PROTEZIONE DEI DATI PERSONALI TE.RI. – Terapia Riabilitativa S.r.l.

Il/La sottoscritto/a _____ *(nome e cognome – in stampatello)*

C.F. _____ nato/a a _____ il _____

in qualità di: ☐ Dipendente ☐ Collaboratore ☐ Consulente ☐ Tirocinante

☐ Altro: _____

Mansione/Ruolo: _____

DICHIARA

a) di aver ricevuto copia del Regolamento Interno per la Protezione dei Dati Personali di TE.RI. S.r.l. (v. 1.0 del 04.06.2026);
b) di averne letto e compreso integralmente il contenuto;
c) di accettare incondizionatamente tutte le disposizioni in esso contenute e di impegnarsi a rispettarle nell'esercizio delle proprie attività;
d) di essere consapevole che la violazione del Regolamento comporta le conseguenze disciplinari, civili e penali ivi descritte;
e) di aver ricevuto contestualmente la lettera di incarico al trattamento dei dati personali

SI IMPEGNA A:

a) mantenere la massima riservatezza sulle informazioni relative ai pazienti e agli altri interessati di cui venga a conoscenza nell'esercizio delle proprie attività;
b) adottare tutte le misure di sicurezza previste dal Regolamento e dalle procedure interne;
c) segnalare immediatamente qualsiasi violazione o sospetta violazione dei dati personali al Referente interno Privacy e al DPO;
d) partecipare ai corsi di formazione obbligatori organizzati dalla Struttura;
e) rispettare gli obblighi di riservatezza **anche dopo la cessazione** del rapporto di lavoro o di collaborazione.

Luogo e data Roma, lì _____

Firma del dipendente/collaboratore _____

(per accettazione) *(nome e cognome in stampatello)*

Firma del del Titolare _____

(per ricevuta) Sig.ra Mara Villani