Casa di Cura Privata di Medicina Riabilitativa
Centro Privato di Riabilitazione
Residenza Sanitaria Assistenziale

NOVA SALUS srl
via Roma, 75a - Trasacco (Aq)
tel • 0863.93131 fax • 0863.936363
email • info@novasalus.eu www.novasalus.eu

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Società: **NOVA SALUS S.r.l.** ***Casa di cura di medicina riabilitativa; Centro di Riabilitazione ed RSA***, con sede legale in Trasacco (AQ), via Roma n. 75/A

Data di elaborazione: 5 luglio 2004 **Ultima revisione 13 marzo 2023**

Approvato da: Lucia Di Lorenzo (Titolare del trattamento)

INDICE

1. Premessa

La NOVA SALUS S.r.l., in questo documento per convenzione denominata anche “NS”, ha provveduto (in ossequio a quanto previsto dal punto 19 del “Disciplinare Tecnico in materia di misure minime di sicurezza” allegato al D. Lgs. n. 196/2003, nonché al GDPR) ad aggiornarlo ogni volta che fossero intervenute modifiche sostanziali tali da richiedere una revisione del documento. Il Documento Programmatico sulla Sicurezza contiene idonee informazioni riguardo:

- l’elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati;
- l’analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l’integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia ed accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento dei medesimi o degli strumenti elettronici;
- la previsione di interventi formativi degli incaricati del trattamento per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Il presente documento costituisce l’aggiornamento per l’anno 2023 del DPS aziendale che, pur non necessitando più di redazione/aggiornamento e relativa data certa (ai sensi dell’art. 45 del Decreto semplificazioni n° 5 del 09/02/2012), viene ugualmente revisionato ogni volta che ve ne sia l’opportunità; sia per accertare l’adeguamento normativo (es.: recepimento regolamenti Garante, Nuovo Regolamento Europeo, Disciplina del DSE Dossier Sanitario Elettronico ecc.), sia per accertare il permanere di tutte le condizioni di sicurezza ivi previste. L’adeguamento 2023 in particolare tiene conto delle modifiche introdotte per garantire la sicurezza dei dati, in virtù della crescente informatizzazione dei dati sanitari.

Si riportano di seguito le principali variazioni rispetto alla precedente edizione:

1) gestione server radiologia par. 4.2
2) Aggiornamento piano formativo

Il presente documento (chiamato anche DPSS) definisce le procedure di gestione della Privacy e le misure adottate da NS per la sicurezza dei sistemi informativi e degli archivi documentali elettronici e non.

Il presente DPSS è stato divulgato a tutto il personale della Società e dalla stessa applicato, tramite affissione in bacheca e trasmissione via mail alle figure apicali.

La sicurezza dei sistemi informatici e di telecomunicazione viene definita come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate, processate, dove:

integrità è la proprietà dell'informazione di non essere alterabile;

disponibilità è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati, per le finalità indicate ed il tempo massimo definito;

confidenzialità è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto in base ai presupposti giuridici del trattamento.

Per le informazioni e i sistemi connessi in rete le esigenze di sicurezza includono anche:

autenticità, ossia la certezza da parte del destinatario dell'identità del mittente;

La sicurezza dei sistemi informatici e degli archivi si estrinseca in una politica ed in un piano operativo che fa riferimento agli aspetti di protezione e agli aspetti di emergenza.

Metodologia Applicata

Si è provveduto a censire i trattamenti di dati effettuati in azienda secondo quanto previsto dal GDPR istituendo il registro dei trattamenti come definito, sia per il titolare che per il Responsabile del trattamento.

Le attività effettuate per la scrittura del presente Documento programmatico sono state:

- censire tutte le misure di sicurezza poste a tutela dei singoli trattamenti;
- individuare in modo formalizzato le persone fisiche autorizzate ai diversi trattamenti;
- definire i profili di accesso ai sistemi;
- valutare le misure di sicurezza adottate, verificando la loro corrispondenza con quanto previsto dal Codice Privacy e dal GDPR
- descrivere la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

Sono stati individuati e valutati i seguenti rischi: distruzione e perdita, anche accidentale, dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi rispetto alle finalità della raccolta, tempi di conservazione dei dati.

L'analisi dei rischi ha riguardato i sistemi informatici e telematici; non sono ad oggi attivi sistemi di registrazione telefonica e/o di videosorveglianza.

Il Documento Programmatico della azienda si riferisce ai trattamenti di dati sensibili (in particolare quelli idonei a rilevare lo stato di salute delle persone) svolti direttamente dalla medesima con l'ausilio di strumenti elettronici, con personale e mezzi propri, nell'ambito delle proprie strutture.

Infine, é stato definito un piano di formazione degli incaricati del trattamento.

2. Elenco dei trattamenti – Registro dei trattamenti

Per l'elenco dei trattamenti, i contitolari ed i responsabili esterni, si fa rinvio al registro dei trattamenti, ultima Revisione

3. Distribuzione dei compiti e delle responsabilità

Titolare del trattamento dei dati è la Nova Salus Srl nella persona del suo rappresentante legale.

É stata disposta la distribuzione dei compiti e delle responsabilità previste nell'ambito della struttura aziendale con riguardo alla gestione dei rischi connessi al trattamento di dati personali nonché ai controlli effettuati in materia.

In particolare sono stati presi in considerazione i trattamenti dei dati personali e sensibili svolti con strumenti elettronici.

La NS, nel 2022, con l'avvio della cartella clinica informatizzata ha introdotto il trattamento in forma di Dossier Sanitario Elettronico ed ha provveduto ad una valutazione e revisione dei profili di accesso in virtù del cambio del gestionale informatico per ridurre al minimo l'accesso a informazioni relative a dati sensibili.

3.1. La struttura aziendale

NS ha definito un assetto organizzativo deputato a garantire la gestione della privacy nonché della sicurezza fisica, logica ed organizzativa.

3.1.1. Incaricati del trattamento dei dati

Tutto il personale dipendente che svolge operazioni di trattamento di dati personali è stato preventivamente individuato e ne sono stati designati i responsabili/coordinatori, con specifico incarico, all'uopo delegati che hanno ricevuto istruzioni dal Titolare dei trattamenti. Sono stati rinnovati tutti gli incarichi ai Responsabili del trattamento (o incaricati) per adeguamento al GDPR.

3.1.2. Responsabili del trattamento dei dati personali

Il Responsabile interno del trattamento dei dati personali è il Direttore Amministrativo, Sig.ra Giulia Pendenza

I Responsabili esterni del trattamento dei dati sono: ASL 1 Abruzzo L'Aquila; Istituto Zooprofilattico di Teramo (anche per i dati sensibili); **Dante Labs (anche per i dati sensibili);** Casa di Cura Di Lorenzo S.p.A. (anche per i dati sensibili), DEDALUS s.p.a. (anche per dati sensibili) **fino a dismissione completa del gestionale; DTS Consulting (anche per i dati sensibili); Team System;** Emiliano Baldassarre e **Massimiliano Lupi** (anche per i dati sensibili); Project Innovation s.r.l. (anche per i dati sensibili); Studio Legale Giacobini e Studio Manerin per i dati fiscali, contabili ed anagrafiche dipendenti (dati personali); Avv.ti G. Gigliotti, L. Aureli, T. Marchese per consulenza legale; Cisia Progetti per la gestione, la custodia e la scannerizzazione e trasmissione telematica del contenuto delle Cartelle Cliniche; Fondiaria – SAI SpA, RC (anche per i dati sensibili); Fondazione Salus, per studi clinici e ricerca; Croce Rossa Italiana, AVIS, ESSEBI, S.O.M.

Tali Responsabili hanno ricevuto e firmato per accettazione la lettera di incarico, con le modalità per il corretto svolgimento dell'attività adeguata al GDPR, avendo verificato che siano dotati di Registro dei Trattamenti. ***La ASL1 Abruzzo è stata da noi definita come contitolare, ma non ha sottoscritto la relativa documentazione.***

3.1.3. Gestione della sicurezza logica, organizzativa e fisica

La Sig.ra Giulia Pendenza, in qualità di responsabile della privacy, è anche responsabile per la gestione della sicurezza logica ed organizzativa, nonché incaricata della corretta tenuta delle copie di sicurezza.

In assenza della Sig.ra Giulia Pendenza, è stata designata come sostituto per le funzioni attribuite la Sig.ra Lucilla Volpone, che ha sottoscritto idonea lettera di incarico. E' stata inoltre incaricato della gestione dell'infrastruttura informatica della Società il Sig. Emiliano Baldassarre, con il quale è stato stipulato apposito contratto come definito dal GDPR ed ha sottoscritto la nomina in qualità di amministratore di sistema, unitamente al Sig. Massimiliano Lupi in qualità di Social Media manager. In ultimo è stato incaricato alla definizione dei profili di accesso il DPPS Dott. Maurizio Gentile.

I compiti sono i seguenti:

- garantire la sicurezza, l'integrità e la riservatezza dei dati;

- controllare l'assegnazione dei profili d'accesso al sistema informativo.

Le parole chiave sono custodite dalla medesima che provvede:

- alla custodia delle buste sigillate contenenti le parole chiave;
- all'assegnazione dei profili di utilizzo;
- alla modifica, disattivazione, riattivazione di password per utenti che sono temporaneamente assenti, che hanno cessato il rapporto con la casa di cura o che hanno dimenticato la password;
- alla prima assegnazione delle password agli utilizzatori.

Inoltre, la Sig.ra Giulia Pendenza, con l'ausilio della Sig.ra Lucilla Volpone e del Sig. Emiliano Baldassarre sono responsabili e garanti della sicurezza fisica attuata con i sistemi di allarme e di sicurezza istallati, nonché nominati, unitamente al Dott. Maurizio Gentile **Amministratore di Sistema**. Specificatamente e limitatamente a tale contesto i suoi compiti consistono in:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Il Dott. Gabriele Pizzi Scatena è nominato Data Protection Officer ed ha accettato l'incarico, così come definito nel GDPR.

La Casa di Cura ha inoltre provveduto alla nomina di amministratori di sistemi esterni in relazione ai corrispondenti incarichi affidati in outsourcing.

3.2. Compiti assegnati al responsabile della privacy e agli incaricati. La gestione degli interessati.

3.2.1 La nomina ed il ruolo del Responsabile

Il Responsabile della Privacy della NS ha il compito, in nome e per conto del Titolare, di nominare formalmente eventuali altri Responsabili con specifiche lettere d'incarico che avrà cura di conservare controfirmate per accettazione.

Ciascun Responsabile a sua volta può:

- nominare gli Incaricati del trattamento per le Banche di dati che gli sono state affidate;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice;
- dare le istruzioni adeguate agli Incaricati del trattamento dei dati effettuato con strumenti elettronici e non;
- periodicamente, almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati;
- chiedere la revisione dei profili di accesso se ritiene opportuna un eventuale restrizione.

Il Responsabile dovrà assicurare che si osservino le regole istituite:

- acquisire solo i dati necessari per le finalità dell'azienda;
- provvedere a raccogliere e a registrare dati, agli esclusivi fini dell'inserimento nelle banche dati e/o dell'arricchimento delle stesse, nei limiti e con le modalità e finalità previste nel registro dei trattamenti;
- curare l'esattezza ed il tempestivo aggiornamento dei dati;
- esercitare la dovuta diligenza affinché non vengano conservati dati non necessari o superflui;
- avere cura, secondo le comuni regole della prudenza e della diligenza, di trattare i dati stessi con la massima riservatezza e di impedire, per quanto possibile che estranei non autorizzati prendano conoscenza dei dati;
- restringere i profili di accesso al minimo indispensabile in relazione alle funzioni svolte;
- provvedere alla cancellazione dei dati nel momento in cui non ne sia più prevista la conservazione.

3.2.2 La nomina ed i ruoli degli Incaricati

Gli Incaricati al trattamento sono formalmente nominati dal Responsabile con una specifica lettera di incarico controfirmata.

Il Responsabile del trattamento avrà cura di conservare tali lettere controfirmate per accettazione.

In tali lettere sono dettagliati i principi cui l'incaricato deve attenersi per il trattamento dei dati personali, come definito al precedente paragrafo.

L'incaricato si assicurerà sistematicamente che, in caso di allontanamento dal posto di lavoro, i contenitori degli archivi e banche dati (scrivanie, cassetti, armadi, computer, ecc.) siano chiusi a chiave e/o protetti da password e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio. In caso di sostituzione del computer utilizzato, si assicurerà che siano compiute le operazioni di formattazione dell'hard-disk, in maniera tale da rendere irrecuperabili i dati ivi contenuti.

Per garantire la piena funzionalità del trattamento dei dati anche in caso di mancanza di uno degli Incaricati, il Responsabile del trattamento dovrà provvedere ad addestrare e ad assegnare i diritti d'accesso di un determinato trattamento a più Incaricati.

L'elenco degli Incaricati al trattamento, con relative lettere controfirmate dagli interessati per accettazione, è custodito dal Responsabile del Trattamento ed aggiornato periodicamente.

3.2.3 L'acquisizione del consenso degli interessati

Nel caso di trattamento di dati sensibili, viene richiesto il consenso scritto dell'Interessato. Il consenso e l'Informativa sono stati revisionati per adeguarli a tutto quanto previsto nel GDPR e, non appena sarà attivata la cartella clinica informatizzata, saranno adeguati al trattamento tramite DSE. Nei casi previsti di maggior tutela per l'utente, si ritiene opportuno l'oscuramento dei dati in ogni caso, su richiesta del paziente.

Viene richiesto anche il consenso dell'interessato, come stabilito dalla normativa, al momento del ricovero, per determinare se l'interessato vuole o meno che venga comunicata agli eventuali visitatori la sua presenza in struttura. La procedura di acquisizione è dettagliatamente descritta nei documenti del Sistema di Gestione Qualità. Nel medesimo consenso è inoltre acquisita l'autorizzazione e fornire informazioni sullo stato di salute del degente solo ed esclusivamente ai familiari/autorizzati specificamente definiti dall'interessato.

E' compito di ogni Incaricato del trattamento e/o del Responsabile archiviare i documenti comprovanti il consenso dell'Interessato.

3.2.4 La gestione dei diritti dell'interessato

La NS è opportunamente organizzata per poter far fronte alle richieste dell'Interessato, che in particolare ha diritto:

- di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati,
- di ottenere la loro comunicazione in forma intelligibile;
- di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del titolare, e dei responsabili;
- di ottenere l'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- di ottenere l'aggiornamento, la rettifica e l'integrazione dei dati;
- di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- di stabilire se la Casa di Cura può comunicare, o meno, ad eventuali visitatori, la sua presenza in casa di Cura;
- di indicare chi può ricevere informazioni sul suo stato di salute.

Il responsabile del trattamento o il responsabile della privacy sono tenuti a verificare ed a controllare che l'incaricato soddisfi in tempi brevi e correttamente le richieste dell'interessato.

I dati estratti possono essere comunicati al richiedente verbalmente, ma di norma, se tecnicamente possibile e semplice, è opportuno fornirli per iscritto, facendosi controfirmare una copia con data.

In caso di minori (con consenso già prestato dai genitori che devono prestarlo congiuntamente e a tal fine è stato predisposta apposita modulistica), divenuti maggiorenni, il sistema propone ulteriormente ed automaticamente l'acquisizione del Consenso.

4. Analisi dei rischi

L'analisi dei rischi è stata condotta ed aggiornata con riguardo alle circostanze possibili o probabili che potrebbero determinare il verificarsi di vulnerabilità dei sistemi informativi con grave pericolo di distruzione o perdita dei dati, anche laddove accidentalmente procurata, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'analisi delle vulnerabilità del Sistema Informativo di NS ha contribuito alla rilevazione dei rischi che l'azienda stessa si potrebbe trovare a fronteggiare laddove si verificassero talune minacce sulla raccolta e conservazione dei dati, considerando che la Società occupandosi di "Prestazioni Sanitarie" è chiamata a trattare dati ascrivibili, ai fini della privacy, alla categoria dei dati sensibili.

Tutti i rischi esaminati sono stati individuati, classificati e descritti nei seguenti principali raggruppamenti:

1. rischi ambientali e fisici;
2. rischi relativi all'integrità dei dati;
3. rischi relativi alla riservatezza dei dati;
4. rischi relativi ai trattamenti non consentiti o non conformi alle finalità della raccolta;
5. rischi relativi alla continuità e disponibilità dei dati.

4.1. Rischi ambientali e fisici

Nella categoria dei rischi specifici sono stati compresi, classificati ed esaminati, tutti i rischi che, generalmente, non trovano una valida protezione nei sistemi di difesa adottati.

In particolare, sono considerati rischi quelli inerenti all'ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento, quelli inerenti i rischi idrogeologici, elettrici e di accesso fisico a infrastrutture, strumenti elettronici e impianti ausiliari.

Le infrastrutture fisiche ed elettriche sono dislocate nella sede operativa della Società: ed in particolare, nel locale "Accettazione", nei locali adibiti al servizio amministrativo, nelle medicherie dei diversi reparti per tipologia assistenziale, negli studi medici, nello studio di fisioterapia, nel locale adibito ad "Archivio Cartelle", nel locale adibito al server (attualmente dimesso), in Radiologia e nel locale server per le immagini del RIS PACS (dotato di sistemi attivi e passivi antincendio).

Le Cartelle Cliniche, su richiesta della Direzione e con cadenza almeno annuale, vengono ritirate dalla Cisia Progetti per essere custodite, archiviate, scannerizzate e messe a disposizione della NS su un server con accessi controllati, tutto come descritto nel DPPS della società.

Il rischio di discontinuità elettrica è attenuato dalla protezione con un gruppo di continuità statico, con la possibilità di sostituire la corrente di rete con un groppo elettrogeno interno.

4.2. Rischi connessi alla protezione di aree e locali

In particolare, sono considerati rischi quelli inerenti accesso fisico a infrastrutture, strumenti elettronici e impianti ausiliari.

I rischi sono stati mitigati dallo spostamento del server RIS PACS (immagini radiologiche) precedentemente ubicato in un locale non sorvegliato, all'interno del locale dedicato agli apparati IT con accessi controllati; il server su cui è installato il gestionale, si trova presso la Casa di Cura Di Lorenzo ed è collegato tramite VPN.

Attualmente il rischio di accesso è mitigato dal fatto che:

- entrambi i locali server (sia presso Nova Salus che presso Di Lorenzo) sono sempre chiusi a chiave e la chiave è custodita esclusivamente dal Responsabile della Privacy o da incaricati del trattamento, all'uopo delegati;
- è stato inoltre istituito un registro degli accessi alla sala server che deve essere compilato da chiunque, ad accezione degli Amministratori di sistema e UL, vi acceda per qualsiasi motivo;
- per quanto concerne il salvataggio dei dati del gestionale DTS questo avviene su una NAS. Inoltre per le immagini radiologiche viene conservata una doppia copia dei dati di back up in luoghi separati.
- Tra la Nova Salus ed il server gestionale ad essa dedicato, presente in Casa Di Cura Di Lorenzo, è stata creata una VPN di tipo L2TP/IPSec. Il protocollo L2TP, acronimo di Layer 2 Tunnel Protocol, è un popolare strumento utilizzato per stabilire connessioni VPN. Di per sé non offre alcuna forma di protezione ed i dati in transito non vengono cifrati. Per questo motivo, L2TP è solitamente utilizzato "in coppia" con il protocollo IPSec che invece integra funzionalità di autenticazione, cifratura e controllo di identità dei pacchetti IP. La chiave di crittografia utilizzata è da 256 bit con server di autenticazione utente di tipo RADIUS.

Vedi anche DPPS Cisia Progetti.

4.3. Rischi relativi all'integrità dei dati

Il concetto di "integrità" riguarda la correttezza, la completezza e la consistenza dei dati sia con riferimento alla protezione dei medesimi, sia alla protezione dai rischi di alterazione o distruzione accidentali o dolose.

Detti rischi sono stati classificati in:

1) rischi connessi a fatti accidentali;
2) rischi derivanti da programmi di cui all'art. 615 quinquies del codice penale;
3) rischi connessi a fatti dolosi.

I rischi di intrusione, che possono provocare danni di integrità oltre che di riservatezza e disponibilità, sono rappresentati dalla possibilità che un soggetto interno (casistica più diffusa) od esterno all'azienda acceda a dati o sistemi, per scopi non leciti, violando la riservatezza, l'integrità o la disponibilità di dati o sistemi.

4.3.1. Integrità dei dati - Rischi connessi a fatti accidentali

Si tratta di rischi di alterazione o distruzione di dati che conseguono all'involontaria sovrascrittura imputabile ad azioni umane errate oppure a guasti delle apparecchiature dedicate alla memorizzazione.

In particolare, vi rientrano le alterazioni o distruzioni di dati dovute a:

- comandi applicativi o operativi errati
- malfunzionamenti hardware;
- deterioramento, nel tempo, dei supporti di memorizzazione e del mezzo fisico che li ospita;
- software pericoloso, in particolare a virus e tool sistemistici generalizzati

Il rischio è mitigato dalle attività di formazione svolte al personale coinvolto e dall'attività di manutenzione hardware e software svolte da ditte specializzate. Nel corrente anno, in virtù del cambio di gestionale, le ore formative dedicate a tale attività sono previste continuativamente fino alla completa attivazione dei sistemi, proprio per mitigare il rischio di errori commessi dagli utilizzatori su un sistema di nuova introduzione.

4.3.2. Integrità dei dati - Rischi da programmi pericolosi

I seguenti rischi sono connaturati alla diffusione di virus e di programmi pericolosi:

- corruzione dei file eseguibili e, a volte, dei dati;
- corruzione di documenti;
- perdita di file;
- perdita di spazio utilizzabile nelle memorie;
- cattivo funzionamento del sistema;
- degrado delle prestazioni del sistema;
- impossibilità di utilizzo del sistema;
- violazioni relative alle ipotesi di cui all'art. 615 quinquies del codice penale;
- danni alla reputazione dell'azienda.

Sulla base dell'analisi delle casistiche nazionali ed internazionali é possibile individuare i seguenti fattori distintivi delle attuali maggiori criticità riscontrate:

- diffusione di virus e worm che sfruttano vulnerabilità note dei programmi e dei sistemi più diffusi per introdursi nel Sistema Informativo;
- posta elettronica ed Internet utilizzato dagli autori di virus per diffondere codici dannosi e pericolosi (virus, cavalli di Troia, worm e backdoor);
- aumento di virus e worm finalizzati ad attacchi DDOS (Distribuited Denial Of Service) contro siti scelti come obiettivo, ovvero lanciati a caso sulla rete.

In sintesi, i virus ed i programmi pericolosi si diffondono principalmente attraverso:

- Internet, mediante la posta elettronica;
- Internet, attraverso la semplice connessione a siti infetti o attraverso il prelievo di file corrotti;
- supporti removibili, ed in particolare CD Rom infetti provenienti da terzi o importati dai dipendenti senza l'autorizzazione dell'azienda;

Per mitigare i rischi connessi alla diffusione di virus o di programmi pericolosi la NS utilizza sistemi antivirus costantemente aggiornati in tempo reale su firewall dedicato cui accedono i PC dotati di connessione al web; inoltre tutti i PC connessi alla rete aziendale sono dotati di antivirus aggiornato periodicamente.

4.3.3. Integrità dei dati - Rischi connessi a fatti dolosi

Sono comprese tutte le alterazioni dell'integrità dei dati conseguenti ad azioni dolose perpetrate allo scopo di:

- modificare i dati;
- inserire nuovi dati;
- distruggere i dati.

4.4. Rischi di Riservatezza dei dati, e Rischi di trattamenti non consentiti o non conformi alle finalità della raccolta

Tale rischio è stato esaminato in relazione alla possibilità che si realizzino rilasci di informazioni non autorizzati e/o accessi non autorizzati ai dati.

Per quanto attiene la "riservatezza" si è fatto in modo di garantire la dovuta protezione delle informazioni contro ipotetiche divulgazioni non autorizzate, consentendo l'utilizzo ed il trattamento solamente ai soggetti incaricati dei trattamenti.

Sono stati valutati i rischi di accessi fraudolenti dall'interno, dovuti a:

- un "profilo" di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di "privilegi" di accesso eccessivi.
- "inferenza", ossia alla cattura di informazioni che, se correlate, consentono di giungere alla conoscenza indiretta di dati.
- utilizzo dei privilegi di "amministratori di sistema" per l'accesso ad archivi.
- "personificazione" di un soggetto autorizzato all'accesso ai sistemi.
- "manomissione" delle autorizzazioni da parte del personale addetto al controllo ed all'amministrazione dei profili di accesso.

Tali rischi sono eliminati dalla non condivisione delle stazioni di lavoro se non con specifica autorizzazione dell'amministratore dei sistemi che opera sotto la supervisione del legale rappresentante della società, grazie all'attribuzione di password per l'accesso alle postazioni contenenti dati riservati ed inoltre grazie ai profili di accesso per singolo utente che non consentono

l'accesso ad aree riservate del sistema. Il profilo di accesso, definito per ciascun operatore, in relazione ai ruoli e alle responsabilità, nonché ai bisogni del profilo professionale ricoperto, viene associato al soggetto al momento della prima assegnazione di password e ne è stata recentemente effettuata un'attenta revisione in occasione dell'istallazione del nuovo gestionale DTS.

4.5. Rischi di Continuità e Non Disponibilità dei dati

Il concetto di "disponibilità" dei dati é riferito alla necessità di assicurare che l'accesso ai dati sia sempre disponibile, evitando la perdita o la riduzione dei sistemi, dei dati e dei servizi.

I rischi di non disponibilità sono stati esaminati in relazione ad eventi di natura accidentale o intenzionale.

4.5.1. Non Disponibilità - Rischi di carattere accidentale

In questo gruppo di rischi è compresa l'eventualità che le informazioni non siano disponibili a causa di eventi non volontari e/o non previsti, dovuti a:

- anomalie in programmi
- errori commessi dal personale
- malfunzionamento dell'hardware
- dimensionamento non sufficiente delle risorse tecnologiche
- non continuità del servizio

I rischi di carattere accidentale sono mitigati da interventi tempestivi della ditta responsabile della manutenzione degli strumenti informatici.

Le immagini radiologiche vengono rese immediatamente disponibili su CD separati ed in ogni caso rimangono nella memoria (prima dell'apparecchio radiologico e poi del server) qualora vi siano guasti che non consentono l'archiviazione su CD dovuta a malfunzionamenti del masterizzatore. In caso di necessità di visualizzazione immediata delle immagini, le stesse vengono masterizzate su CD o visualizzate su altro video.

4.5.2. Non Disponibilità – Rischi di carattere intenzionale

In questa tipologia di rischi sono incluse le fattispecie in cui le informazioni non sono disponibili a causa di azioni umane volontarie, compiute con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte di soggetti autorizzati.

Tali minacce sono messe in relazione a danneggiamento o manomissione di sistemi per infedeltà del personale addetto alla gestione delle informazioni.

I rischi intrinseci sono mitigati da controlli organizzativi e la supervisione del responsabile al trattamento dei dati, nonché dalle procedure di gestione dei documenti previste dal sistema di gestione qualità.

4.6. Data Breach

In ogni caso, qualora si dovesse verificare, per qualsiasi ragione, una violazione dei dati, il Data Protection Officer Dott. Gabriele Pizzi Scatena, in collaborazione con il Titolare del Trattamento, Dott.ssa Lucia Di Lorenzo, provvede entro 48 ore lavorative alla Comunicazione al garante, come previsto nel relativo regolamento, con la modulistica prescritta dal Garante ed informa altresì l'interessato cui si riferisce l'eventuale violazione.

5. Misure organizzative per garantire la protezione dei dati

Sono state emanate e tenute aggiornate specifiche policy sulla segretezza delle password per tutto il personale.

Il personale è stato sensibilizzato sulle problematiche di rischio inerenti le credenziali di autenticazione ed i sistemi di posta elettronica.

L'attività formativa sul tema viene rinnovata con cadenza preferibilmente biennale.

6. Misure da adottare per garantire la protezione delle aree, dei locali e degli impianti

6.1. Protezione delle aree e dei locali

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

Gli uffici sono protetti da una porta chiusa a chiave.

Il personale verifica le persone in entrata.

I dati personali contenuti nei documenti cartacei sono custoditi in un apposito archivio sotto il controllo del personale addetto alla segreteria ed autorizzato ad accedervi.

Nei reparti il personale infermieristico verifica le persone in entrata e custodisce i documenti cartacei presso le medicherie.

In particolare le sale server (in struttura e decentrata) sono dotate di impianto rileva fumi. La porta risulta chiusa a chiave e gli accessi (e le attività) sono controllati mediante specifico registro.

Le chiavi sono in possesso dell'Amministratore di Sistema.

6.2. Protezione degli impianti

I principali impianti (gruppo elettrogeno, impianto antincendio, ecc.) sono protetti tramite controllo degli accessi ai relativi locali d'uso ed esecuzione delle operazioni di manutenzione ordinaria.

7. Misure di sicurezza per garantire l'integrità e disponibilità dei dati *(segue regola 19.4).*

Le tecniche ed i sistemi di sicurezza adottati dalla NS per la protezione dei dati personali e sensibili fanno riferimento sia al trattamento informatico che non.

Le misure di sicurezza adottate risultano idonee alla protezione dei dati e soddisfano le misure minime richieste dal Codice della Privacy e l'esigenza di un adeguato livello di protezione dei dati.

7.1. Misure di sicurezza per la prevenzione dei rischi di carattere accidentale

Al fine di garantire il ripristino dei dati è previsto il salvataggio dei dati con frequenza giornaliera.

É in vigore una procedura per l'effettuazione dei back up al fine di realizzare gli obiettivi temporali di ripristino.

Sono di seguito identificati gli interventi a carico di NS :

- E' previsto il back up periodico (almeno semestrale) per i dati attualmente archiviati localmente al fine di garantire il ripristino completo dell'operatività di una postazione di lavoro eventualmente danneggiata, su hard disk esterno, conservato presso l'Ufficio della Direzione Generale. Il contenuto dei PC in locale sarà progressivamente (in corso di censimento e predisposizione dell'attività) automaticamente salvato sul server con cadenza definita e in base al censimento effettuato e registrato

- I dati sui server sono salvati settimanalmente con unità di back up automatico.
- I dischi che contengono i back up sono custoditi in luoghi separati dal server.
- Nel processo di sensibilizzazione e formazione del personale, viene costantemente dedicata particolare attenzione, anche tramite note informative, sulla necessità di attuare comportamenti conformi alle corrette procedure di gestione delle informazioni trattate in modalità elettronica, al fine di garantirne l'integrità e la disponibilità nel tempo.
- Per minimizzare eventuali problemi dovuti a guasti hardware si provvede ad una costante manutenzione degli apparecchi e alla copertura dei rischi con garanzia del produttore/fornitore. E' inoltre in vigore un contratto di manutenzione con Project Innovation per garantire immediato intervento in caso di malfunzionamento della VPN di collegamento al server esterno.
- Tutti i PC con sistema operativo obsoleto e non in grado di supportare i sistemi operativi più recenti, in grado di garantire la sicurezza, sono stati sostituiti e sugli stessi sono istallati sistemi operativi ed antivirus recenti, ferma restando la barriera costituita dal firewall centralizzato.

7.2. Aggiornamenti periodici dei programmi per elaboratore volti a prevenire le vulnerabilità degli strumenti elettronici (patching software)

Gli aggiornamenti periodici alle versioni di software sui singoli PC consentono di eliminare delle vulnerabilità intrinseche di questi software al momento del loro rilascio da parte del fornitore.

Questi aggiornamenti vengono chiamati patch (effettuati durante la normale operatività) oppure Hot fix (in caso di grave vulnerabilità da rimuovere con urgenza nel corso di attacchi).

Le macchine hanno installato sistemi operativi Windows.

Gli aggiornamenti di configurazione dei software sulle singole postazioni di lavoro e sui server vengono effettuati in modo tempestivo anche con l'utilizzo di autoupdate di Microsoft; tali interventi sono affidati ad Emiliano Badassarre. I singoli utilizzatori di PC sono comunque istruiti sulla necessità di procedere agli aggiornamenti.

7.3. Sicurezza delle trasmissioni dei dati

L'accesso ad Internet avviene transitando dal firewall, in modo tale da avere garanzie sui filtri di sicurezza impostati.

7.4. Misure di sicurezza contro il rischio di intrusione

I rischi di intrusione sono rappresentati dalla possibilità che un soggetto interno (casistica più diffusa) od esterno all'azienda acceda a dati o sistemi, per scopi non leciti, violando la riservatezza, l'integrità o la disponibilità di dati o sistemi.

Detta condotta può essere realizzata anche attraverso l'uso di programmi malevoli.

Le contromisure contro i rischi esterni di intrusione sono prevalentemente architetturali (firewall, configurazioni non standard, eliminazione di porte logiche inutili) o legati alla dotazione di software antivirus.

I sistemi antintrusione consistono in:

- i firewalls sono configurati secondo i criteri di tutte le connessione inbound negate e tutte le interconnessioni outbound abilitate.

Una contromisura efficace è rappresentata dalla registrazione dei log delle attività dei sistemi in tutti i punti critici del sistema.

Gli antivirus sono le contromisure consigliate contro i programmi malevoli. Essi consentono inoltre di individuare i programmi potenzialmente dannosi già presenti nei singoli sistemi.

È fatto divieto di utilizzare software non ufficialmente rilasciato.

Nel caso in cui si verifichi una contaminazione da virus è prevista una procedura di intervento immediato di isolamento del PC al fine di minimizzare la diffusione del virus e l'impatto sull'azienda; successivamente, si analizzano le cause del problema per eliminarle e ripristinare il normale funzionamento del PC

È periodicamente effettuato il monitoraggio della efficacia della diffusione degli ultimi aggiornamenti distribuiti sull'intero parco macchine.

7.5. Misure di autenticazione informatica ed autorizzazione per l'accesso ai dati

Di seguito vengono descritti i criteri e le procedure adottati per garantire la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica.

7.5.1. Misure per il controllo dell'accesso Sistema di autenticazione

Per la connessione alla rete interna è prevista una procedura di autenticazione mediante il codice identificativo dell'utente e la relativa password.

Sono state fornite a tutti i dipendenti le indicazioni per l'elaborazione delle password: devono avere almeno 8 caratteri alfanumerici contenenti almeno una maiuscola, una minuscola ed un carattere speciale, ma essere facilmente memorizzabili per l'utente.

È prevista una password per l'accesso ai dati con scadenza automatica ogni 90 giorni

Le password di accesso con i relativi profili sono archiviate nel sistema, ma non visibili; l'elenco degli utenti con password assegnata è costantemente aggiornato dal sistema e riproducibile su carta. Il Titolare del trattamento, con qualifica di Superuser, dotato di apposita password, può riabilitare e disabilitare gli utenti (in caso di allontanamento per un determinato periodo o definitivo) anche parzialmente, ma non può visionare le password.

7.5.2. Autonoma sostituzione della parola chiave

È prevista l'autonoma sostituzione della parola chiave ogni novanta giorni o qualora l'utente lo considerasse necessario.

Tramite interventi di formazione/sensibilizzazione è stato comunicato ai dipendenti che la parola chiave può essere utilizzata anche per proteggere singoli file elettronici o cartelle contenenti dati riservati ma il personale non è comunque autorizzato a detenere dati personali e riservati sui PC della NS.

7.5.3. Soggetti preposti alla custodia delle credenziali di autenticazione

È stata formalizzata una procedura che indica le modalità per assicurare la disponibilità di dati o strumenti elettronici accessibili tramite password in caso di prolungata assenza o impedimento da parte dell'utente incaricato.

E' stata redatta e distribuita agli interessati una nuova Istruzione per la gestione delle firme digitali.

7.5.4. Istruzioni non accessibilità strumento elettronico

Le macchine per le quali se ne rilevi la necessità, sono dotate di blocco con password in caso di temporanea assenza dell'utente.

7.6. Misure per la gestione delle autorizzazioni

7.6.1. Autorizzazione all'accesso agli strumenti

Tutti gli strumenti dai quali si può accedere ai dati sono censiti e codificati.

È operativo un sistema informativo ed informatico nel quale le autorizzazioni non si riferiscono mai a tali strumenti bensì ai singoli operatori.

È attivo un sistema di log che consente di risalire ai dati relativi al sistema e all'operatore che hanno eseguito una specifica operazione.

7.6.2. Autorizzazioni agli incaricati del trattamento

Con riguardo alle autorizzazioni è prevista l'adozione di una politica aziendale che persegua la logica del "minimo privilegio", le autorizzazioni saranno legate al reale bisogno di accesso ai dati (*need to know e need to do*) da parte del personale della NS nell'espletamento delle mansioni lavorative assegnategli, tramite un sistema di profili.

È prevista la formalizzazione di un sistema di profili al fine di associare all'utente i diritti relativi al trattamento dei dati autorizzato.

Tutte le autorizzazioni verranno sottoposte a verifica periodica (almeno annuale) in relazione alla permanenza delle necessità di accesso.

7.6.3. Misure per il controllo dell'accesso ai dati in locale su PC

L'accesso ai dati di carattere personale all'interno delle risorse del singolo personal computer è regolato da password per i quali l'amministrazione ne ha ravvisato le necessità.

Le persone autorizzate al trattamento dei dati personali vengono identificate a priori con lettera di incarico controfirmata per accettazione ed il loro accesso è regolato dalla stesura di particolari profili di autorizzazione distinti per tipologia di trattamento effettuato.

7.7. Misure atte a garantire la disponibilità di dati e sistemi *(già regola 19.5)*

7.7.1. Postazioni di lavoro – Hardware di rete

Il rischio di non disponibilità dei singoli PC degli utenti è presidiato mediante un contratto di manutenzione che prevede l'assistenza in loco e la sostituzione tempestiva dei PC eventualmente non riparabili.

Il ripristino dei dati delle singoli stazioni di lavoro per i dati considerati rilevanti per l'azienda sono ripristinati dal back up appena sostituito il PC.

7.7.2 Ripristino in tempi certi

Il ripristino di tutti i sistemi è garantito in quarantotto ore lavorative.

In caso di pronto intervento da parte di Fornitori esterni, viene richiesta, rilasciata ed archiviata una attestazione degli interventi tecnici effettuati sui sistemi di sicurezza e relativamente al ripristino dei dati.

7.7.3 Registro eventi anomali

La registrazione degli eventi anomali viene effettuata attraverso il Sistema di Gestione Qualità con l'apertura di una Non Conformità, annotando anche le caratteristiche del virus o altro evento anomalo, la sua origine, gli effetti provocati e la risoluzione del problema. Nel caso di violazioni di particolare gravità si apre una segnalazione ai sensi del D.L.vo 231/2001 e si attiva la segnalazione del Data Breach come previsto al par. 4.6.

7.7.4 Continuità elettrica

Tutta la sala server è posta sotto continuità elettrica grazie ad UPS .E' inoltre possibile la fornitura di energia elettrica in autonomia tramite gruppo elettrogeno.

7.8. Ulteriori misure per la riservatezza disponibilità e integrità dei dati *(segue regola 19.5)*

7.8.1. Policy e regolamenti

È organicamente integrato nelle procedure operative del sistema gestione qualità il regolamento relativo alle misure per la protezione dei dati personali, tramite costante aggiornamento con revisioni delle relative PO. In particolare tale regolamento è inserito nella PO "Cartella clinica" e nelle procedure di "Gestione manutenzioni" e della "Contabilità Clienti".

È stato altresì adottato un Regolamento relativo all'utilizzo degli strumenti informatici, tramite l'emanazione della Procedura Operativa (PO) "Gestione Informatica e Privacy" integrato nel SGQ. Nella citata PO è inserito anche un inventario dei client, delle stampanti, delle condivisioni, della possibilità di accesso alla rete.

Ulteriore strumento di controllo è l'audit interno annuale che viene effettuato, in base alla check-list allegata per verificare il rispetto di tutte le prescrizioni normative.

Il questionario di Customer Satisfaction è aggiornato con la relativa informativa.

La Casa di Cura ha implementato un proprio ***Modello di Organizzazione, Gestione e Controllo per la responsabilità amministrativa, conforme ai requisiti individuati nel D.Lgs. 231/2001*** e pertanto, ha effettuato:

- Nomina dell'Organismo di Vigilanza e Controllo (OdV) ed emanato relativo regolamento di funzionamento dell'Organismo stesso
- Elaborato e distribuito a tutti il Modello Organizzativo (Parte Gen. + parti Spec.) e il "Codice Etico";
- Mappato tutte le attività a rischio reato e definito i processi sensibili da analizzare (Analisi del rischio), per i quali ha emanato/revisionato le apposite procedure;
- Definito Mansionari, Deleghe e Procure;
- Definito e condiviso un Sistema Disciplinare e Sanzionatorio – Sistema Premiante;
- Formazione del personale;
- Analizzato e monitorato attraverso audit interni condotti dall'ODV le attività identificate e definito i flussi informativi verso l'OdV.

7.8.2. Riutilizzo controllato dei supporti e loro dismissione

I PC dismessi vengono catalogati e distrutti, con apposita registrazione controfirmata dall'esecutore, oppure conservati in apposito magazzino chiuso a chiave, previa cancellazione dei dati.

Prima della distruzione viene effettuato un back up sull'hard disk esterno dedicato ai back up in locale.

Tutti i PC sono comunque dimessi/rottamati secondo le prescrizioni di legge.

8. Piano di formazione *(già regola 19.6)*

Il piano di formazione è finalizzato a rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Per tutto il personale incaricato del trattamento è stata effettuata nel periodo 2015-2016 un'attività formativa con i seguenti contenuti essenziali:

- informazioni sul D. Lgs. n. 196/03 e sul relativo disciplinare tecnico;
- novità in tema di privacy
- rischi possibili e probabili cui sono sottoposti i dati;
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi;

- misure di sicurezza fisiche;
- misure di sicurezza organizzative;
- misure di sicurezza logiche;
- comportamenti e modalità di lavoro per prevenire i rischi, con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure anti-hacker), contenitori di sicurezza (ad es.: schedari, archivi, etc.), sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di backup, con particolare riguardo alle recenti novità introdotte dal Garante: amministratore di sistema, uso corretto del web (internet/email), dismissione/rottamazione dei pc, ecc.;
- attività in capo all'Ufficio del Garante.

Nel 2018 è stata effettuata la formazione specifica sull'entrata in vigore del GDPR e le novità dallo stesso introdotte.

Nel 2020 è stato effettuato, da tutti gli incaricati un corso FAD di aggiornamento sulla privacy. Chi non ha risposto all'invito di effettuare il corso è stato sollecitato e sanzionato in caso di mancata conclusione dell'evento formativo.

Nell'anno 2022 è stata effettuata specifica formazione sull'utilizzo dei sistemi informatici e nuovi eventi formativi sono in programma anche per l'anno 2023 in virtù della progressiva informatizzazione della struttura.

Nel piano formativo del biennio 2022-2023 è stato previsto l'aggiornamento del corso privacy.

Infine, la formazione in materia è sempre prevista al momento dell'assunzione nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati personali.

9. Trattamenti affidati all'esterno

Nella seguente tabella sono riportati i trattamenti affidati all'esterno:

Descrizione sintetica dell'attività esterna	***Trattamenti di dati interessati***	***Soggetto esterno***	***Descrizione criteri/impegni***
Sistema gestionale utenti	Pazienti	DTS Consulting/Dedalus (fino a dismissione solo per consultazione)	Nomina responsabile/amm. di sistema
Gestione Paghe e contributi	Personale	Studio Manerin	Nomina responsabile/amm. di sistema
Archiviazione Cartelle cliniche	Pazienti	Cisia Progetti	Nomina responsabile/amm. di sistema
Gestione contabilità	Personale	Studio Giacobini Team System	Nomina responsabile esterno/amm. di sistema
Analisi di laboratorio in service, servizi sanitari	Pazienti	Casa di Cura *Di Lorenzo*	Nomina responsabile
Esecuzione test molecolari Covid 19	Pazienti	Istituto Zooprofilattico Teramo/Dante Labs	Nomina/contratto

Gestione sinistri RC sanitaria	Pazienti	Unipol SAI	Nomina/contratto

10. Cifratura dei dati o separazione dei dati identificativi *(già regola 19.8)*

Questa struttura sanitaria protegge tutti i dati personali sensibili idonei a rivelare lo stato di salute o la vita sessuale dei clienti utilizzando le modalità previste dal produttore del software soddisfacenti la normativa ed indicate nella tabella seguente:

Trattamento del dato	Protezione scelta	Data di effettività	Tecnica adottata	Informazioni utili
DB clienti-sistema Dedalus DTS Consulting	Separazione tra dati identificativi e dati sensibili	2000 2022	Gli archivi non sono criptati con tecniche di cifratura, ma sono illeggibili senza i corrispondenti tracciati di transcodifica (ODBC) in possesso solo di utenti autorizzati.	Il fornitore ha rilasciato dichiarazione formale sulla modalità della protezione scelta, che ne attesti la conformità alle disposizioni del disciplinare tecnico-allegato B al Dlgs 196/2003

11. Allegati

Sono parte integrante del presente DPS i seguenti documenti:

1. PO-UL-INF (Gestione informatica e privacy)
2. IO-FIR (Gestione firme digitali)
3. Modulistica
4. Check-list di verifica adempimenti privacy: ultimo aggiornamento
5. Verbale di controllo annuale: assegnazione profili di accesso; vigenza password; controllo IPA
6. Registro dei trattamenti del Titolare
7. Registro dei trattamenti del Responsabile

Trasacco, ***13/03/2023***

Il Titolare del Trattamento