Tipologia Documento	Documento Aziendale
Campo di applicazione	Fondazione IRCCS San Gerardo dei Tintori
Processo	P22 Miglioramento dell'organizzazione e gestione dei rischi
Attività	A1106 Tutela Privacy
Struttura emittente	AGL
Luogo Archiviazione	QUARC

Storia delle modifiche

Livello revisione	Data Emissione	Descrizione sintetica delle modifiche apportate
1	03.10.2024	NUOVA CODIFICA EX ASST-DA-001
0		Adeguamento passaggio da ASST Monza alla Fondazione IRCCS San Gerardo dei Tintori

Redazione	Verifica conformità SGQ	Iter Approvazione Decreto 979 del 2024	
		I Livello	II Livello
*** Coordinatore del Gruppo di lavoro**	**RQA Barni e DPO**	**Direttore Sanitario A. Andreassi Direttore Amministrativo A. Ferrigno**	**Direttore Generale S. Casazza**

*** Partecipanti al gruppo di lavoro:**

Nome Cognome	Ruolo	Struttura
Mariagrazia Meroni	Collaboratore amm.vo professionale	S.C. Affari Generali e Legali
Davide Pietro Tomè	Direttore f.f.	S.C. Sistemi Informativi Aziendali
Maurizio Pastore	DPO	

1. Premessa

Il presente documento è stato adottato in attuazione del principio di *accountability* ex art 5, comma 2 del Regolamento Generale sulla protezione dei dati (UE) U 2016/679, ed ha lo scopo di fornire regole operative necessarie per una corretta e adeguata gestione dei dati personali dei quali è Titolare la **FONDAZIONE IRCCS SAN GERARDO DEI TINTORI** (di seguito FSGT), con sede in **via Pergolesi, n. 33 - 20900 Monza (MB).**

Preso atto dell'art. 5, comma.2 RE UE 2016/679 e del *Considerando 74*;
Constatato che il principio di "*Accountability*" impone un approccio proattivo; tenuto conto che tale approccio implica di aver fatto e di poter dimostrare tutto quanto è possibile per evitare una gestione dei dati non conforme o tale da arrecare potenziali danni alla tutela dei dati personali, e, quindi, di dover risponderne in futuro;
Ribadito che tali principi si traducono, nella dimostrazione, di aver fatto tutto il possibile per evitarli;
Sottolineato che è richiesto al Titolare del trattamento dei dati, nella fase "*privacy by design*" di dimostrare che l'organizzazione è nella condizione di far fronte ad ogni situazione futura, anche solo possibile, ipotetica, probabile;
Rilevato che nel *Considerando 74*, è richiesto anche di "*dimostrare l'efficacia delle misure*", messe in atto e di rendicontare come si è proceduto, e, con quali metodologie a definire le suddette misure di sicurezza.

Tutto ciò premesso, la FSGT adotta la seguente ***Privacy Policy*** riguardo la gestione del trattamento dei dati sia in forma analogica che digitale, la configurazione delle rete aziendale, la definizione dei livelli di accesso alla documentazione aziendale ed alla rete aziendale, oltre che le norme comportamentali richieste a tutti gli Autorizzati e Designati interni al trattamento dei dati.

2. Scopo e campo di applicazione

Il presente documento a*ziendale* si applica a tutto il personale dipendente, ai collaboratori, liberi professionisti e/o ad ogni altro soggetto che a qualunque titolo, risulti coinvolto nelle attività di trattamento dei dati della FSGT.
Il mancato rispetto o la violazione delle regole ivi contenute, può essere perseguito mediante azioni disciplinari ed eventualmente azioni giudiziarie secondo le leggi vigente. Pertanto, è destinata a tutti gli "**Autorizzati"** e "**Designati",** ossia a coloro che svolgono le operazioni necessarie alla gestione dei trattamenti all'interno dell'organizzazione.
Gli utenti interni all'organizzazione acquistano un ruolo fondamentale rispetto al sistema informativo e alle reti. Il rapporto utente interno - sistema informativo - rete - è di gran lunga più critico, del rapporto utente esterno - sistema informativo - rete. L'utente interno è coinvolto in prima istanza nell'utilizzo esclusivo e privilegiato del sistema informativo, rappresentando pertanto uno dei principali fattori di rischio per la sicurezza delle informazioni e delle reti. In questo contesto si inserisce, come ulteriore elemento che contribuisce alla domanda di sicurezza, l'esigenza di garantire la privacy nel trattamento delle informazioni.

3. Definizioni

Come stabilito dal Regolamento Europeo n. 2016/679, ai fini della presente privacy policy vengono qui richiamate alcune definizioni essenziali per qualunque autorizzato/designato al trattamento:

a) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «**interessato**»: il soggetto cui i dati personali si riferiscono;

d) «**autorizzato**»: il soggetto che tratta i dati personali in nome e per conto del Titolare del Trattamento secondo le regole e/o istruzioni impartite dal proprio Responsabile e/o Direttore;

e) «**designato**»: il soggetto che in quanto Responsabile e/o Direttore occupa un ruolo apicale di gestione delle Strutture Complesse - Semplici - Dipartimentali o delle Strutture in Staff.

f) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

g) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

h) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

i) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

l) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

m) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

n) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

o) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

p) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

q) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

r) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

s) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

t) «**accountability**»: rinvia al concetto di **"responsabilizzazione"** e pone in carico al Titolare l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche

certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (**principio della "conformità" o *compliance* nell'accezione inglese**). Per il Titolare (FSGT), esiste un vero e proprio obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE.

u) «**privacy by default and by design**»: l'art. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese che rappresenta la necessità di configurare ogni trattamento di dati, prevedendo fin dall'inizio le garanzie indispensabili per soddisfare i requisiti del regolamento stesso e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

v) «**rete**»: ha assunto un significato assai ampio, sostituendosi, all'acronimo ICT (Information and Comunication Tecnology). Le reti sono le strutture di interconnessione (nelle diverse tecnologie wired e wireless), insieme alle diverse macchine (hardware e software), oggetto dell'interconnessione, e, a tutti gli apparati a supporto della interconnessione stessa. Per estensione, anche ***gli utenti*** vengono a buon diritto a far parte della rete.

w) «**internet**»: si configura come una rete che attraverso milioni di nodi di scambio (router) interconnette centinaia di milioni di calcolatori, comprendendo fra questi non solo i server, ma anche i dispositivi di elaborazione in possesso degli utenti (workstation, personal computer, palmari, cellulari con avanzate capacità di elaborazione e comunicazione dati).

z) «**data protection officer (DPO)**»: un professionista che nei termini di cui agli artt. 37, 38 e 39 del Regolamento UE, viene nominato dal Titolare del Trattamento. La nomina del DPO è obbligatoria in tutte le organizzazioni, pubbliche che trattano dati particolari su larga scala. Chi svolge la funzione di DPO, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, trovarsi anche solo potenzialmente in conflitto di interessi, essendo in tal caso vietata la nomina.

4. Responsabilità e gestione del rischio

Qualsiasi organizzazione affida gran parte dei propri processi istituzionali, ai sistemi informativi e quindi alle informazioni trattate. Quando un evento dannoso, sia esso di origine naturale o dolosa, colpisce i sistemi che gestiscono le informazioni di cui l'organizzazione ha bisogno (comprese le reti), quasi sempre questo si traduce in una brusca interruzione dei processi aziendali che può compromettere la continuità dell'attività e operatività. Oggi, più di ieri, essere sicuri vuol dire fronteggiare qualsiasi evento, dalle catastrofi naturali (allagamenti, incendi, terremoti) all'attacco informatico, garantendo l'***integrità*** e la ***continuità*** dei più intimi e vitali processi dell'organizzazione.
Le responsabilità e la gestione del rischio sono descritte nei paragrafi. 5 e 6.

5. Modalità operative

5.1 I SISTEMI INFORMATIVI AZIENDALI - NORME GENERALI

Tutte le apparecchiature informatiche, i Personal Computer, fissi o mobili, smartphone, i relativi programmi e/o le applicazioni, affidate agli utenti/autorizzati sono strumenti di lavoro.

Regole generali sul utilizzo per tutte le apparecchiature informatiche:

- le apparecchiature in dotazione dell'utente devono essere custodite con cura evitando ogni possibile forma di danneggiamento e possono essere utilizzati solo per fini professionali e non per scopi personali, tantomeno per scopi illeciti;
- è vietato prestare o cedere a terzi qualsiasi apparecchiatura senza la preventiva autorizzazione del proprio responsabile e dalla S.C. Sistemi Informativi Aziendali;
- è vietato rimuovere i contrassegni identificativi dall'apparecchiatura;
- devono essere prontamente segnalati tramite il servizio Fleet alla S.C. Sistemi Informativi Aziendali il danneggiamento o il malfunzionamento dell'apparecchiatura.
- In caso di furto o smarrimento di apparecchiatura informatica l'autorizzato o chi ne ha avuta consegna dovrà procedere tempestivamente a sporgere denuncia alle competenti Autorità di Polizia del territorio, presentare in originale la stessa al proprio Responsabile e darne comunicazione al DPO Aziendale ed alla S.C . Sistemi Informativi Aziendali;

- è vietato modificare le configurazioni impostate sulle apparecchiature;
- è vietata la memorizzazione sui dispositivi aziendali di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- qualsiasi apparecchiatura se non utilizzata deve essere restituita tempestivamente alla S.C. Sistemi Informativi Aziendali.

Regole specifiche sull'utilizzo dei personal computer aziendali fissi o mobili:

- il Personal Computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento e possono essere utilizzati solo per fini professionali e non per scopi personali o per scopi illeciti;
- l'utilizzo del personal computer e la navigazione sulla rete aziendale è consentita solo attraverso credenziali di autenticazione personale;
- il personale della S.C. Sistemi Informativi Aziendali e gli Amministratori di Sistema possono accedere ai pc, in modalità fisica o da remoto, per compiere interventi diretti a garantire la sicurezza e la salvaguardia del sistema, nonché per ragioni di ordine tecnico e/o manutentivi (ad es. aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware etc.), previo avviso e/o consenso da parte dell'utente;
- è vietato l'uso di programmi diversi da quelli ufficialmente installati dal personale della S.C. Sistemi Informativi Aziendali o dagli Amministratori del Sistema;
- è vietato agli utenti installare autonomamente programmi provenienti dall'esterno e non espressamente autorizzati. L'inosservanza della presente disposizione espone la FSGT e l'utente a conseguenze civili e penali;
- l'utente deve prestare la massima attenzione nell'utilizzo di supporti di origine esterna, avvertendo immediatamente attraverso il servizio Fleet il personale della S.C. Sistemi Informativi Aziendali nel caso in cui siano rilevati virus o criticità;
- in caso di allontanamento temporaneo dalla propria postazione, l'utente deve attivare il blocca schermo tramite password. Per agevolare questa attività l'Amministrazione può predisporre un sistema automatico di salvaschermo con sblocco tramite password dopo un periodo di inattività predefinito in tutte le postazioni;
- il Personal Computer deve essere spento ogni giorno, prima di lasciare la postazione di lavoro, salvo non sia utilizzato nel corso delle 24 ore;
- i dati archiviati sul disco locale del personal computer non sono soggetti alle policies di backup aziendali, pertanto si raccomanda di utilizzare le cartelle di rete per salvare i documenti di lavoro;
- non sarà garantito, in caso di cancellazione da parte dell'utente o guasto della postazione, il recupero dei file non presenti nelle cartelle di rete messe a disposizione dell'utente;
- risulta opportuno che con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia delle cartelle di rete, ed alla cancellazione dei file obsoleti o inutili (nel rispetto del "*Titolario e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario*" vigente). Particolare attenzione deve essere prestata alla duplicazione dei dati.

Regole specifiche sulla gestione ed assegnazione delle credenziali informatiche:

- tutti gli utenti autorizzati ad avere accesso alle risorse informatiche devono possedere credenziali nominali per autenticarsi alle postazioni, alla rete ed alle applicazioni aziendali;
- le credenziali di autenticazione per l'accesso al PC e quelle necessarie all'utilizzo delle applicazioni utili all'espletamento delle attività amministrative e/o cliniche, vengono assegnate dalla S.C. Sistemi Informativi Aziendali all'utente previa richiesta del Responsabile o del Coordinatore di struttura di appartenenza;
- le credenziali di autenticazione sono da considerarsi strettamente personali e consistono in un nome utente univoco e una password di primo accesso, che ogni soggetto sarà obbligatoriamente tenuto a personalizzare;
- la password di dominio ha validità di 60 (sessanta) giorni, dopodiché dovrà essere sostituita per garantirne la sicurezza e riservatezza;
- le password devono caratterizzarsi per complessità e lunghezza come stabilito dalla normativa vigente e dalle prassi in uso presso le P.A. Si rinvia alle indicazioni stabilite dal Garante per la protezione dei dati Personali ("Suggerimenti per creare e gestire password a prova di privacy.");
- le password non devono essere comunicate ad altri, né devono essere esposte sul PC mediante etichette e/o adesivi riportanti nome utente e/o password;

- è vietato l'utilizzo di nome utente e password di altri utenti per l'accesso alle risorse informatiche, aree protette ed applicativi in nome e/o per conto di altri, nemmeno se fornite volontariamente o di cui si è a conoscenza;
- è vietato all'utente cedere, una volta autenticato con le proprie credenziali, l'uso della propria postazione o dei Software ad altro utente;
- è vietato lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione.

. **Regole specifiche sull'utilizzo e conservazione dei dati e dei supporti removibili:**

- tutti i supporti rimovibili (CD e DVD riscrivibili, dispositivi di storage USB, ecc.), contenenti dati personali o lavorativi, nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o ancora successivamente alla cancellazione, recuperato;
- l'utente è responsabile della custodia dei supporti e dei dati aziendali memorizzati in essi;
- è vietato introdurre e/o conservare in FSGT a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico (CD e DVD riscrivibili, dispositivi di storage USB, anche in forma cartacea) contenente dati di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso. In caso di violazione, troveranno applicazione la personale responsabilità civile e penale del singolo, nonché le eventuali sanzioni disciplinari che FSGT riterrà di dover comminare;
- è vietato trasferire all'esterno della FSGT attraverso supporti removibili file, documenti, immagini, disegni, progetti, audio, video, o qualsiasi altra documentazione riservata e di proprietà della FSGT, se non per finalità strettamente attinenti lo svolgimento delle proprie mansioni.

Regole specifiche sull'utilizzo di Dispositivi mobili quali pc portatili cellulari e Tablet

- l'utente è responsabile di tutti i dispositivi aziendali che gli vengono assegnati o che utilizza e deve custodirli con diligenza sia durante gli spostamenti, sia nel luogo di lavoro;
- il dispositivi utilizzati all'esterno della FSGT, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessarie per evitare danni o sottrazioni;
- i dispositivi possono essere utilizzati solo per fini professionali e non per scopi personali o per scopi illeciti;
- i dispositivi devono essere configurati con accesso tramite credenziali aziendali o in caso di Smartphone e Tablet devono essere protetti da pin, password o altro sistema di riconoscimento di accesso;
- al fine di garantire i necessari aggiornamenti di sicurezza, occorre che l'utente colleghi il pc portatile alla rete aziendale ed esegua l'accesso almeno una volta ogni 30 giorni, in caso di dispositivi Smartphone e Tablet devono essere attivati gli aggiornamenti automatici di sicurezza del dispositivo;
- in caso di dismissione dei dispositivi non più necessari l'utente deve provvedere alla rimozione di eventuali file e documenti di qualunque forma memorizzati nel dispositivo prima della riconsegna;
- in caso di furto o smarrimento l'interessato dovrà procedere a sporgere denuncia alle competenti Autorità di Polizia del territorio e presentare in originale la stessa al proprio Responsabile entro 24 h. Si dovrà tempestivamente darne comunicazione al DPO Aziendale ed alla S.C Sistemi Informativi Aziendali.

Norme generali sull'utilizzo della rete aziendale, della posta elettronica ed Internet

Tutti gli utenti a cui a cui sono state assegnate le credenziali aziendali possono accedere internet e tutti gli utenti dipendenti o gli utenti con un contratto di collaborazione con la FSGT possono disporre (previa richiesta del loro Responsabile / Coordinatore) di un indirizzo di posta elettronica aziendale.
La FSGT fornisce, la Casella di Posta Elettronica nominale ed univocamente assegnata. L'eventuale utilizzo condiviso di caselle di posta elettronica istituzionali e/o di struttura, sarà gestita in modo da consentire l'identificazione univoca dell'autore dell'attività di consultazione e gestione della casella di posta medesima.
Per l'accesso ai pc, quindi anche per l'accesso alla rete aziendale, altresì da dispositivi mobili quali tablet e smartphone tramite Wi-Fi, l'utente deve utilizzare le proprie credenziali aziendali.
Le Password di accesso alla rete (ed ai programmi) sono strettamente personali non cedibili e vanno gestite secondo le regole sopra definite ed è assolutamente proibito accedere alla rete (e ai programmi) con credenziali altrui.

Internet ed il sistema di posta elettronica sono strumenti di comunicazione, informazione e trasmissione. L'uso di entrambi nelle loro numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e per il conseguimento dei fini istituzionali della FSGT.
I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà della FSGT.
Al fine di garantire la sicurezza dei Sistemi Informativi Aziendali, la FSGT può adottare soluzioni informatiche per il blocco della navigazione Internet in siti ritenuti non consoni all'attività dell'Amministrazione e/o pericolosi.
I medesimi principi qui richiamati, si applicano anche all'utilizzo degli accessi assegnati per altri Servizi di Enti Terzi quali la carta SISS, l'identità SPID, il servizio di posta elettronica certificata PEC, la registrazione su siti istituzionali Regionali/Nazionali o di aziende di servizi esterne, ecc..

In caso di utilizzo improprio delle credenziali **la responsabilità ricade sul titolare** delle stesse.

La Posta Elettronica è uno strumento di lavoro messo a disposizione per svolgere le attività legate alle mansioni assegnate, pertanto l'indirizzo è personale ma non privato. Ognuno è direttamente responsabile, disciplinarmente e giuridicamente, del contenuto della propria Casella di Posta e dei messaggi inviati.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali devono essere inviate mediante gli strumenti quali PEC e/o protocollate sul sistema protocollo aziendale.

Regole generali comportamentali:

- l'accesso alla posta elettronica è personale e si accede tramite nome utente e password;
- l'accesso alla mail personale non può essere condiviso o ceduto, non può essere attivato l'inoltro automatico ad un altro indirizzo mail;
- è vietato utilizzare la Posta Elettronica per motivi non attinenti allo svolgimento delle mansioni assegnate;
- è vietato inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- è vietato l'utilizzo della Posta Elettronica di altri utenti per l'invio di comunicazioni a proprio nome o in nome di questi;
- è obbligatorio porre la massima attenzione nell'aprire i file allegati ("*attachments*") alle mail ricevute prima del loro utilizzo: non eseguire download di file eseguibili o aprire documenti sospetti;
- si esorta l'utente a non rispondere mai alle mail che richiedono l'inserimento di credenziali aziendali, codici o dati privati, in caso di richiesta sospetta contattare il servizio di Assistenza Fleet;
- si esorta l'utente, in caso di assenza programmata, ad attivare la risposta automatica "di fuori sede" con l'indicazione dei soggetti terzi autorizzati a cui indirizzare la corrispondenza di competenza;
- è vietato l'utilizzo della casella di posta elettronica aziendale per l'iscrizione a social network o a altri servizi per uso personale, se non previa autorizzazione della Direzione.

Regole Specifiche sull'utilizzo della VPN:

Una VPN (Virtual Private Network) è una tecnologia che crea una connessione sicura e crittografata tra un dispositivo e un server remoto.
L'abilitazione alla VPN mette l'Ente in una situazione di potenziale rischio intrusione (la maggior parte delle intrusioni di sistemi malevoli avviene attraverso le VPN); pertanto saranno abilitate solo per chi ha "reale" necessità di operare da remoto sui sistemi aziendali in quanto previsto dalle mansioni e/o eventuali incarichi ricevuti (Es: Reperibilità, Smart Working, etc…).
Pertanto:

- l'accesso alla VPN deve essere richiesto dal Responsabile/Coordinatore tramite apposito modulo e viene autorizzato dal Responsabile della S.C. Sistemi Informativi Aziendali;
- l'accesso alla VPN attraverso le credenziali rilasciate dalla S.C. Sistemi Informativi Aziendali è nominale ad uso esclusivo e non cedibile;
- la possibilità di accesso scade quando il ruolo del richiedente cambia o cessano le motivazioni per le quali è stata concessa;
- l'autorizzazione all'uso della VPN ha scadenza di 12 mesi dopodiché viene sospesa automaticamente e il dipendente deve essere riautorizzato all'uso;
- l'utente deve utilizzare la VPN solo per accedere alle risorse aziendali autorizzate e non tentare di accedere a risorse non autorizzate;
- l'uso della VPN è riservato esclusivamente per uso lavorativo;

- l'utente che utilizza la VPN deve assicurarsi che i dispositivi utilizzati per accedere alla VPN siano protetti con antivirus aggiornati e firewall attivi;
- l'utente deve disconnettersi dalla VPN quando ha terminato le sue attività lavorative;
- l'utente deve segnalare immediatamente alla S.C. Sistemi Informativi Aziendali qualsiasi incidente di sicurezza, come il furto di credenziali, il furto o lo smarrimento del dispositivo dove è stata installata la VPN;

L'uso della VPN è monitorato per garantire la sicurezza della rete aziendale. Le attività sospette saranno segnalate e indagate.
In ogni caso, la S.C. Sistemi Informativi Aziendali può procedere con la disattivazione immediata di un accesso VPN per la quale vengono rilevate attività sospette o traffico malevolo.
La violazione delle regole comportamentali per il corretto uso della VPN e delle tecnologie informatiche può comportare sanzioni disciplinari.

Regole specifiche utilizzo PEC aziendale:

La PEC (Posta Elettronica Certificata) è un sistema di e-mail con valore legale. Una mail trasmessa da una casella di PEC e ricevuta da una casella PEC ha il medesimo valore legale della tradizionale raccomandata postale con ricevuta di ritorno.
Perché tutto questo avvenga è necessario che anche il mittente abbia un indirizzo PEC. Il termine "certificata" si riferisce al fatto che al mittente viene rilasciata una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e di eventuali allegati ed al mittente la ricevuta di avvenuta consegna. La PEC attesta, quindi, che il messaggio è stato spedito, consegnato e che non è stato modificato.
La richiesta di PEC aziendali deve essere inviata alla S.C. SIA tramite il Servizio di assistenza Fleet ed è sottoposta all'autorizzazione della Direzione Generale.

Firma da porre in calce ai messaggi e-mail FSGT

I messaggi di posta elettronica, inviati tramite il sistema di posta elettronica aziendale, devono contenere la firma come da istruzioni aziendali al fine di rendere univoca la comunicazione dei soggetti. Viene introdotto un *"template"* di firma univoco aziendale personalizzabile con nome cognome, struttura di appartenenza, dati di contatto, logo aziendale, ecc.

Sicurezza informatica

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte alla sicurezza informatica, monitorizzano il corretto utilizzo delle risorse informatiche dell'Ente secondo le normative vigenti anche in virtù dell'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta delle Autorità Competenti.

Protezione Antivirus

Il sistema informativo aziendale è protetto da software antivirus aggiornato costantemente. Ogni utente deve comunque tenere comportamenti adeguati al fine di ridurre il rischio di attacco ai sistemi dell'Ente da parte di virus o qualsiasi altro software malevolo.
Nel caso l'antivirus rilevi la presenza d software malevoli, l'utente dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al Servizio Fleet.

SOCIAL MEDIA

Si ritiene vietato l'utilizzo dei social media, quali a titolo esemplificativo Facebook™, Twitter™, Linkedin™, dei blog e dei forum durante l'orario di lavoro, ove il loro utilizzo non sia motivatamente connesso all'attività lavorativa.

Laddove per fini aziendali ne viene ammesso l'utilizzo, questo dovrà ispirarsi alle seguenti regole comportamentali:

- garantire la segretezza delle informazioni aziendali riservate (ad esempio informazioni economico-finanziarie, piani aziendali, e relative a pazienti, clienti, fornitori e partners);

- rispettare i diritti di proprietà industriale e d'autore (di terzi e dell'organizzazione) quando si procede alla pubblicazione dei contenuti;
- non è consentito comunicare o diffondere dati personali (dati anagrafici, immagini, video, suoni e voci) di colleghi e collaboratori aziendali senza il loro preventivo ed espresso consenso, e, comunque, non è possibile postare immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo ed espresso consenso di ogni soggetto coinvolto;
- astenersi dal realizzare attività civilmente o penalmente rilevanti (ad esempio diffamazione, discriminazioni, ecc.) nei confronti di terzi, dell'organizzazione, di colleghi, di pazienti, clienti e di fornitori;
- queste regole vanno rispettate anche in caso di utilizzo di un dispositivo e partecipazione social media a titolo personale.

Controlli

Nel rispetto del divieto di controllo a distanza del lavoratore e dello Statuto dei Lavoratori nel quale tale divieto è contenuto, la FSGT effettua controlli sull'uso degli strumenti elettronici da parte degli utenti tramite consultazione dei file di log solo in relazione:

- ad esigenze di sicurezza e finalità di tutela del proprio patrimonio (ad es. nel caso in cui l'integrità del sistema sia minata da un problema di sicurezza e sia necessaria la consultazione dei file di log per individuare e eliminare l'anomalia);
- all'indispensabilità dei dati di log rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di rispondere ad una specifica richiesta dell'Autorità Giudiziaria o dell'Autorità di Pubblica Sicurezza.

GRADUAZIONE DEI CONTROLLI

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, la FSGT effettua per le finalità di tutela di cui all'articolo precedente, con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- controllo preliminare su dati aggregati (riferiti all'intera struttura lavorativa o a una sua area e rilevazione della tipologia di utilizzo, e-mail, file audio, accesso a risorse estranee alle mansioni);
- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti aziendali con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti il settore in cui è stata rilevata l'anomalia;
- solo in caso di successivo permanere dell'anomalia la FSGT si riserva la facoltà di procedere ad effettuare controlli circoscritti su singole postazioni di lavoro.

Sono in ogni caso vietati controlli prolungati, costanti o indiscriminati.

5.2 Trattamento dati attraverso supporti cartacei

ACCESSO AI DATI

E' consentito l'accesso agli archivi cartacei nei limiti in cui ciò sia indispensabile per prelevare, consultare e riporre documenti necessari allo svolgimento delle attività.
Le porte dei locali ove sono riposti i documenti e/o archivi (armadio/cassettiera), devono essere custoditi, non possono risultare incustoditi e se possibile è opportuna la conservazione in armadi chiusi a chiave (o con altra chiusura).
Ogni utente/autorizzato dovrà preoccuparsi di avvisare tempestivamente il proprio Responsabile/Designato di riferimento nel caso in cui dovesse ravvisare accessi agli archivi di soggetti non autorizzati (interni/esterni) o qualunque altro tipo di anomalia. La tempestività nella segnalazione degli incidenti costituisce elemento di riduzione del rischio di perdita e/o compromissione definitiva delle banche dati analogiche.

CONSERVAZIONE DEI DATI

Ogni utente/autorizzato ha l'obbligo di attenersi alle modalità organizzative di conservazione dei dati adottate dal proprio Responsabile/Designato. Deve sempre preferirsi la conservazione in locali o armadi muniti di apposita chiusura, soprattutto quando i documenti contengano dati personali (comuni – particolari – giudiziari). Ogni postazione di lavoro non deve essere lasciata incustodita e nel caso in cui ci si allontani o si cessi la propria attività lavorativa, i documenti cartacei contenenti dati personali vanno riposti e tenuta pulita la postazione di lavoro stessa (*desk clean*).

CANCELLAZIONE DATI O DOCUMENTI

I documenti contenenti dati personali che devono essere eliminati vanno distrutti fisicamente, senza che possano recuperarsi informazioni riferite a dati personali (comuni – particolari – giudiziari).
È vietato cestinare copie permettendo a terzi il recupero delle informazioni o la consultazione delle stesse.
La modalità di distruzione migliore, se disponibile, è mediante il distruggi documenti, oppure attraverso il taglio manuale (a mezzo forbici, taglierini o altri strumenti).

STAMPANTE SCANNAER FOTOCOPIATRICI

Ogni utente è autorizzato all'utilizzo delle stampanti, scanner e fotocopiatrici aziendali.

Regole generali comportamentali:
- è vietato utilizzare carta riciclata recante, sul retro del foglio, dati personali;
- è vietato lasciare incustodita la documentazione durante lo svolgimento delle operazioni di fotocopiatura, scansione dei documenti;
- l'utente deve ritirare tempestivamente gli originali e le copie fatte al termine della procedura;
- l'utente deve rendere illeggibile il contenuto della fotocopia mal riuscita prima di cestinarla.

5.3 Trattamento dati attraverso la comunicazione

CONFIDENZIALITÀ DEI DATI PERSONALI TRATTATI

Anche nel rispetto delle vigenti norme sul segreto professionale, gli Autorizzati e i Designati sono tenuti a mantenere l'assoluta segretezza sulle informazioni inerenti, in particolare, i dati personali, di cui vengono a conoscenza nel corso delle operazioni di trattamento, evitando qualsiasi loro diffusione. Le aree di passaggio o quelle nelle quali i contenuti delle conversazioni possono essere intercettate anche da persone terze e/o da personale non autorizzato, vanno evitate, ed in ogni caso va mantenuta la debita distanza di sicurezza a tutela dei contenuti delle informazioni. Nelle aree di attesa va rispettato l'ordine di precedenza e di chiamata evitando l'individuazione nominativa (utilizzo di codici numerici).

RILASCIO DI INFORMAZIONI SULLO STATO DI SALUTE DEI PAZIENTI

Non è possibile fornire informazioni inerenti lo stato di salute del paziente senza il consenso per iscritto dell'interessato e possono essere comunicate a quest'ultimo esclusivamente per il tramite di un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente.

RILASCIO DI INFORMAZIONI SULLA PRESENZA DELL'INTERESSATO PRESSO LA STRUTTURA

E' possibile comunicare la presenza di un paziente in un reparto a terzi legittimati (familiari, conoscenti, ecc.). L'interessato, se cosciente e capace, deve essere preventivamente informato e posto in condizione di fornire indicazioni circa le persone che possono venire a conoscenza del ricovero e del reparto di degenza. E' necessario rispettare l'eventuale volontà dell'interessato che la sua presenza presso la struttura non sia comunicata neanche a terzi legittimati.

Non è mai giustificata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, indipendentemente dalla menzione o meno della patologia o dell'intervento da erogare.

ULTERIORI PRESCRIZIONI

Gli Autorizzati ed i Designati sono tenuti a non parlare di questioni riservate in aree pubbliche (ad es.: sala caffè, mensa, mezzi di trasporto pubblico, newsgroup su Internet, ecc.) in modo tale che terzi possano avere accesso alla conversazione e a non mostrare, anche accidentalmente, documenti contenenti informazioni riservate.

UTILIZZO DI STRUMENTI QUALI TELEFONO, SCANNER

Nel caso di richieste di dati personali tramite telefono è necessario:

- verificare quanto dichiarato dall'interessato al momento dell'accesso; se la persona è ricoverata presso la FSGT, è possibile fornire tale informazione solo col consenso del paziente, espresso sull'apposito modulo;
- dare informazioni telefoniche riguardanti lo stato di salute dei pazienti, solo in casi di necessità ed urgenza (aggravamento delle condizioni di salute del paziente, ricovero da Pronto Soccorso del paziente non accompagnato, ecc.). In questo caso è necessario accertare l'identità dell'interlocutore e verificare che questi sia autorizzato ad acquisire tali informazioni;
- verificare l'identità del richiedente (ad esempio formulando una serie di quesiti a mezzo di intervista guidata oppure attribuendo all'interessato un codice identificativo che quest'ultimo gli comunicherà previamente ad ogni comunicazione impersonale);
- chiedere il numero di telefono dal quale è effettuata la chiamata.

Nel caso in cui gli autorizzati o i designati procedano ad acquisire in formato digitale della documentazione cartacea tramite scanner, devono verificare che il contenuto del documento oggetto di scansione sia correttamente conservato.

6. Violazione dei dati (DATA BREACH)

Per violazione dati (c.d. DATA BREACH) s'intendono tutte quelle attività che possono comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque degli interessati (utenti-pazienti-dipendenti-collaboratori-terzi-ecc.).

- **Distruzione**: consiste nell'indisponibilità definitiva dei dati personali con impossibilità di ripristino degli stessi determinata da un'eliminazione logica (es. cancellazione dei dati) o fisica (es. rottura supporti di memorizzazione) non autorizzata;
- **Perdita**: consiste nella sottrazione, smarrimento, furto di dispositivi contenenti dati personali o di documenti cartacei;
- **Modifica**: consiste in una variazione non autorizzata o dolosa dei dati personali gestiti;
- **Rivelazione**: consiste in una distribuzione non autorizzata o dolosa dei dati personali verso terze parti non legittimate a venirne a conoscenza;
- **Accesso**: consiste nell'accesso improprio o non autorizzato ai dati personali, sia che si tratti di accessi a sistemi informatici sia in caso di ingresso in locali dove siano presenti archivi cartacei.

Per riuscire a chiarire meglio il significato di violazione dati, di seguito vengono riportati alcuni possibili esempi distinguendo tra trattamenti attraverso l'ausilio di strumenti elettronici o documentazione cartacea, tenendo sempre a mente che una violazione può essere dovuta sia a un comportamento involontario/accidentale sia a un comportamento doloso.

a) Trattamenti svolti con l'ausilio di strumenti elettronici:

POSSIBILE VIOLAZIONE	ESEMPIO PRATICO
▪ **Erronea esecuzione di comandi o procedure dovuta a distrazione**	Erronea formattazione di dispositivi di memorizzazione, divulgazione accidentale di credenziali di accesso a colleghi o soggetti non autorizzati.

▪ **Rottura di componenti hardware**	Distruzione di supporti di memorizzazione a causa di eventi naturali, caduta accidentale del supporto, ecc..
▪ **Fornitura dati a persone fisica diversa dall'interessato**	Invio comunicazioni via e-mail a soggetti diversi dal reale destinatario contenenti dati personali dell'organizzazione.
▪ **Guasti alla rete aziendale**	Caduta delle comunicazioni durante il trasferimento dati e conseguente perdita degli stessi durante la trasmissione.
▪ **Compromissione o rivelazione abusiva di credenziali di autenticazione**	Scambio delle credenziali tra gli operatori o conoscibilità delle stesse da parte dei colleghi.
▪ **Utilizzo di software malevolo ai fini di una truffa informatica o un furto di dati**	Atteggiamento doloso di un soggetto esterno o, addirittura, di un operatore che impiegando un software/programma mira a sottrarre dati personali o a chiedere un riscatto per il rilascio degli stessi.

Trattamenti svolti manualmente / attraverso documentazione cartacea:

POSSIBILE VIOLAZIONE	ESEMPIO PRATICO
▪ **Distruzione accidentale o dolosa di documenti**	Dovuti ad eventi quali incendi, allagamenti dei locali dove sono presenti gli archivi cartacei o causati volontariamente dal personale.
▪ **Smarrimento di documenti**	Perdita di documenti contenenti dati personali a causa di una non corretta e adeguata conservazione degli stessi.
▪ **Accesso non autorizzato da parte del personale interno o soggetti esterni a locali in cui sia presente documentazione contenenti dati personali**	Mancata chiusura a chiave di locali archivi o di controllo dell'accesso agli stessi. (in tali casi non si verificherà una violazione se si ha ragionevole certezza che non vi sia stata lettura o copia dei documenti).
▪ **Furto della documentazione contenente dati personali degli interessati**	Sottrazione materiale di documentazione dell'organizzazione in cui siano presenti dati personali afferenti agli utenti o al personale interno.

Ogni Autorizzato al trattamento dei dati, qualora rilevi un incidente nella gestione dei dati personali o dovesse anche solo averne il sentore, deve riferire il prima possibile al proprio Responsabile/Designato tutte le informazioni riguardanti gli eventi o le vulnerabilità connesse alla sicurezza dei dati e delle informazioni. Si rimanda, a questo proposito, alla procedura operativa "GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI (*Data Breach*) (A1106_P22_P02) ed al MODULO SEGNAZIONE DATA BREACH (A1106_P22_P02_M01).
Le modalità di segnalazione possono variare in base alle circostanze ma devono avere, per quanto possibile, le caratteristiche di rapidità, disponibilità, accessibilità e rintracciabilità.

Ogni Autorizzato/Designato al trattamento dei dati deve astenersi dal tentare di verificare e/o risolvere la vulnerabilità sospetta individuata, ciò in ragione del fatto che il tentativo potrebbe essere interpretato come un potenziale uso non consentito o improprio del sistema ovvero potrebbe aggravare la situazione o provocare ulteriori danni, con la conseguente esposizione a responsabilità ed azioni legali.

Tutte le attività successive alla segnalazione, quindi, saranno delegate a chi ne sia stato espressamente autorizzato, a partire dall'adozione delle immediate contromisure, per passare alla successiva valutazione dell'accaduto, individuazione di nuove misure di sicurezza per finire all'eventuale notifica al Garante per la protezione dei dati personali o comunicazione agli interessati.
Al termine della gestione dell'evento, saranno comunicate le eventuali nuove misure di sicurezza da adottare o nuove istruzioni operative da seguire a tutto il personale.

7. Pubblicità della Privacy Policy

Il presente documento aziendale verrà diffuso attraverso la rete interna e pubblicata sul sito web aziendale nella Sezione Amministrazione trasparente - Altri contenuti - Privacy.

8. Documenti di riferimento o Bibliografia o Sitografia

D. L.gs. n. 196/2003 e s.m.i.
Regolamento Generale sulla protezione dei dati (UE) 2016/679
Provvedimenti del Garante per la protezione dei dati personali
Sito: www.garanteprivacy.it