# 1. Premessa

Il presente documento è stato adottato in attuazione del principio di *accountability* ex art 5 co 2 del RE EU 2016/679, ed ha lo scopo di fornire regole operative necessarie per una corretta e adeguata gestione dei dati personali dei quali è Titolare l'**ASST MONZA,** con sede in **via Pergolesi, n. 33 - 20900 Monza (MB).**

Preso atto dell'*Art*. 5, co.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, l'ASST Monza 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 s*i 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 dell'ASST Monza.
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,** 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 SIA, 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 policy privacy vengono qui richiamate alcune definizioni essenziali per qualunque autorizzato 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 (ASST Monza), 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 nel par. 5 e 6.

# 5. Modalità operative

## 5.1 Trattamento dati attraverso strumentazione elettronica

### 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, pertanto:

- vanno custoditi in modo appropriato.
- possono essere utilizzati solo per fini professionali e non anche per scopi personali, tantomeno per scopi illeciti;
- non è consentito prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del proprio Responsabile/Designato e della S.C. Servizio Informativo Aziendale;
- non è consentito rimuovere i contrassegni identificativi, se presenti sulle Apparecchiature Informatiche.
- debbono essere prontamente segnalati alla S.C. Servizio Informativo Aziendale e/o agli Amministratori di Sistema, il danneggiamento o lo smarrimento di tali strumenti. Inoltre, qualora si verifichi un furto o si smarrisca un'Apparecchiatura Informatica di qualsiasi tipo, l'autorizzato o chi ne ha avuto consegna, entro 24 ore dal fatto, dovrà far pervenire alla Direzione l'originale della denuncia all'Autorità di Pubblica Sicurezza;
- è fatto assoluto divieto di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso. Resta inteso che, in caso di violazione, troveranno applicazione la personale responsabilità civile e penale del singolo, nonchè le eventuali sanzioni disciplinari che ASST riterrà di dover comminare;
- è fatto assoluto divieto di trasferire all'esterno dell'Azienda e/o trasmettere files, documenti, immagini, disegni, progetti o qualsiasi altra documentazione riservata e di proprietà dell'ASST, se non per finalità strettamente attinenti lo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile/Designato;
- non è consentita la memorizzazione di documenti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- onde evitare il grave pericolo di introdurre virus informatici, di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal SIA e/o dagli Amministratori di Sistema;
- non è consentito modificare le configurazioni impostate sulle Apparecchiature Informatiche;
- sui PC dotati di scheda audio e/o lettori CD/DVD non è consentito l'ascolto di Files audio o musicali, né la visualizzazione di video e films, se non a fini prettamente lavorativi e/o di ricerca scientifica;

- non è consentito lasciare incustodito e/o accessibile ad altri il proprio PC;
- In caso di allontanamento temporaneo, l'utente deve attivare il salvaschermo con sblocco tramite password. Per agevolare questa attività l'Amministrazione può predisporre un sistema automatico di salvaschermo (blocco computer) con sblocco tramite password dopo un periodo di inattività della postazione.

I dispositivi fissi e mobili (Personal computer, notebook, cellulari, etc.) non utilizzati devono essere restituiti tempestivamente al Servizio Informativo Aziendale.

**UTILIZZO DEL PERSONAL COMPUTER**

Il Personal Computer affidato all'utente/autorizzato ed è uno strumento di lavoro.
Ogni utilizzo non inerente l'attività lavorativa è vietato e può contribuire ad innescare disservizi, costi di manutenzione, minacce alla sicurezza.
Deve essere custodito con cura evitando ogni possibile forma di danneggiamento ed una volta affidato all'utente/autorizzato, permette l'accesso alla rete aziendale (intranet) solo attraverso specifiche credenziali di autenticazione.
Il SIA e gli Amministratore di Sistema, oltre che eventuali utenti/autorizzati interni, possono compiere interventi sul sistema informativo aziendale, diretti a garantire la sicurezza e la salvaguardia del sistema medesimo, nonchè per ragioni di ordine tecnico e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).
Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del SIA per conto dell'Azienda, né viene consentito agli utenti/autorizzati di installare autonomamente programmi provenienti dall'esterno, sussistendo il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.
L'inosservanza della presente disposizione espone ASST a gravi responsabilità civili. Ogni utente/autorizzato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del SIA nel caso in cui siano rilevati virus/criticità.

Il Personal Computer deve essere spento ogni giorno, prima di lasciare la postazione di lavoro, salvo non sia utilizzato nel corso delle 24 ore. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito utilizzo. Sui dispositivi deve essere attivata la modalità automatica di screen-saver a tempo, con obbligo di reintrodurre la password per l'accesso. Per agevolare questa attività l'Amministrazione può predisporre un sistema automatico di salvaschermo (blocco computer) con sblocco tramite password dopo un periodo di inattività della postazione.

**GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE**

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 dal SIA all'utente/autorizzato in relazione al ruolo professionale ricoperto, previa richiesta del Responsabile di struttura di appartenenza.

Le credenziali di autenticazione consistono in un codice di identificazione dell'autorizzato (user-id), e password di primo accesso, che ogni soggetto sarà automaticamente tenuto a modificare. Ogni 60 giorni l'utente/autorizzato deve modificare la propria password. Per agevolare questa operazione l'Amministrazione può predisporre un sistema automatico di scadenza delle password.

Le password devono caratterizzarsi per complessità e lunghezza di caratteri alfanumerici anche in combinazione fra loro come stabilito dalla normativa vigente e dalle prassi in uso presso le P.A., e, non deve mai contenere riferimenti agevolmente riconducibili all'autorizzato. 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 user e/o password.

Non è in alcun modo consentito l'utilizzo di user-id e password di altri "utenti aziendali", neanche per l'accesso ad aree protette o applicativi in nome e per conto di altri.

Risulta opportuno che con regolare periodicità (almeno ogni tre mesi), ciascun utente/autorizzato provveda alla pulizia degli archivi, ed alla cancellazione dei file obsoleti o inutili (nel rispetto del Massimario di scarto ultima versione approvata). Particolare attenzione deve essere prestata alla duplicazione dei dati.

**UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI**

Tutti i supporti rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o particolari, nonchè 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. In ogni caso, i supporti rimovibili contenenti dati particolari, devono essere dagli utenti/autorizzati adeguatamente custoditi in armadi chiusi. L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

**UTILIZZO DI DISPOSITIVI MOBILI (PC PORTATILI, CELLULARI E TABLET)**

L'utente/autorizzato è responsabile di tutti i dispostivi aziendali che gli vengono assegnati o che utilizza e deve custodirli con diligenza sia durante gli spostamenti, sia nel luogo di lavoro.

Ai dispositivi di qualunque natura si applicano le regole di utilizzo previste dalle presenti norme, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna. Quando utilizzati in mobilità all'esterno dell'Azienda, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessarie per evitare danni o sottrazioni.

Al fine di garantire i necessari aggiornamenti di sicurezza, è necessario che l'utilizzare colleghi il pc portatile alla rete aziendale almeno una volta ogni 30 giorni.

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. Si dovrà tempestivamente darne comunicazione al DPO Aziendale ed al SIA.

**ACCESSO A INTERNET E USO DI RETE AZIENDALE**

La navigazione in internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione.
L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e per il conseguimento dei fini istituzionali della ASST.
I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà dell'Azienda.
La banda Internet ed il sistema di posta elettronica sono operanti con continuità, 24 h al giorno per 365 giorni all'anno.
Per l'accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione (ID utente) e una parola chiave segreta (password).
È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. La parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le regole sopra definite.
Superato il sistema di autenticazione l'utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.
Tutti gli utenti cui è assegnata una postazione di lavoro possono utilizzare internet, compatibilmente con le bande a disposizione.
Al fine di garantire la sicurezza dei Sistemi Informativi Aziendali, l'Ente può adottare soluzioni informatiche per il blocco della navigazione Internet in siti ritenuti non consoni all'attività dell'Amministrazione e/o comunque ritenuti pericolosi.

L'utente non deve:

- cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a intranet e ai servizi di posta elettronica;
- lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- utilizzare credenziali (ID utente e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza.

L'utente deve altresì conservare la password nella massima riservatezza e con la massima diligenza.

I medesimi principi qui richiamati, si applicano anche all'utilizzo degli accessi assegnati agli utenti anche da Enti Terzi quali la carta SISS – lo SPID o altri.

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

**USO DELLA POSTA ELETTRONICA - PEC**

La ASST fornisce, limitatamente agli "utenti aziendali" / "autorizzati" che ne hanno necessità, una 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 la identificazione univoca dell'autore dell'attività di consultazione e gestione della casella di posta medesima. Tale circostanza impone una maggiore responsabilizzazione a cura delle figure diverse che rientrano nel gruppo professionale e che accedono ala stessa Casella. Anche la Posta Elettronica è uno strumento di lavoro messo a disposizione per svolgere le attività legate alle mansioni assegnate, pertanto l'indirizzo attribuito agli "utenti aziendali" è personale ma non privato. Ognuno è direttamente responsabile, disciplinarmente e giuridicamente, del contenuto della propria Casella di Posta e dei messaggi inviati.

La casella di posta deve essere mantenuta in ordine, cancellando periodicamente i messaggi in SPAM e svuotando il cestino.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile di Area o dalla Direzione di competenza.

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, da inviarsi mediante gli strumenti quali PEC o posta tradizionale e devono essere autorizzate e firmate dalla Direzione Generale e/o dai Direttori di Struttura e/o Responsabili, a seconda del loro contenuto e dei destinatari delle stesse.

È obbligatorio porre la massima attenzione nell'aprire i file *attachments* di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente.

In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio web-mail entro quindici giorni - verrà attivata a cura dell'Azienda.

Sarà comunque consentito al superiore gerarchico dell'utente o all'incaricato della custodia della copia delle credenziali, individuato dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

L'accesso alla posta elettronica è personale e vi si passa tramite nome utente e password di identificazione.

L'accesso non può essere condiviso o ceduto.

Si ritiene inoltre utile segnalare che:

- non è consentito utilizzare la Posta Elettronica, interna ed esterna, per motivi non attinenti allo svolgimento delle mansioni assegnate;

- non è consentito inviare o memorizzare messaggi, interni ed esterni, di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- non è consentito l'utilizzo della Posta Elettronica di altri "utenti aziendali" per l'invio di comunicazioni a proprio nome o in nome di questi.
- in caso di assenza programmata il lavoratore, dovrà attivare la risposta automatica di fuori sede con l' indicazione dei soggetti terzi autorizzati cui indirizzare la corrispondenza di competenza.
- non è consentito creare, consultare, utilizzare caselle di Posta Elettronica private.

**SISTEMI DI RISPOSTA AUTOMATICA E DISCLAIMER IN CALCE ALLE EMAIL**

Sistemi di risposta automatica

Per prevenire l'apertura della posta elettronica dei dipendenti e per rispettare il principio di necessità e non eccedenza del trattamento di dati personali, l'Azienda Ospedaliera mette a disposizione di ciascun lavoratore apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze (ad es. per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura.

Il dipendente è tenuto ad avvalersi di tali modalità in caso di assenze prolungate.

In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non abbia provveduto ad attivare la procedura descritta (anche avvalendosi di servizi web mail), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, semprechè sia necessario e mediante personale appositamente incaricato (ad es., l'Amministratore di Sistema), può disporre lecitamente l'attivazione di un analogo accorgimento, avvertendo gli interessati.

Ciascun lavoratore, a tal fine, è tenuto a nominare un fiduciario che, nel caso di assenza improvvisa o prolungata, sussistendo improrogabili necessità legate all'attività lavorativa, possa essere individuato quale destinatario dei messaggi di posta elettronica del lavoratore assente.

Disclaimer da porre in calce ai messaggi email dell'ASST

I messaggi di posta elettronica inviati tramite il sistema di posta elettronica aziendale devono contenere un avvertimento ai destinatari, nel quale viene dichiarata l'eventuale natura non personale dei messaggi stessi, precisando che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente, con le modalità di cui al presente Regolamento aziendale.

L'utente potrà adottare il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute da persone appartenenti all'organizzazione lavorativa del mittente secondo le modalità previste dal regolamento aziendale adottato in materia. Se per un disguido avete ricevuto questa mail senza essere i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo del mittente*".

Al fine di rendere univoca la comunicazione dei soggetti autorizzati viene introdotto un t*emplate* di firma univoco aziendale personalizzabile con nome cognome – ruolo – struttura di appartenenza – logo aziendale.

**CONTROLLI SULL'ACCESSO E L'UTILIZZO DEI SERVIZI INTERNET E DI POSTA ELETTRONICA TRAMITE LE RISORSE INFORMATICHE DA PARTE DEGLI UTENTI**

Registrazione delle attività sull'uso dei servizi

Le attività sull'uso dei servizi Internet e di Posta Elettronica dell'utente vengono registrate elettronicamente sotto forma di file di log.

L'attività di registrazione viene effettuata a cura dell'Amministratore del Sistema, che garantisce anche la custodia dei file di log, in base alle normative vigenti.

**MEMORIZZAZIONE FILES DI LOG DELLA NAVIGAZIONE AD INTERNET**

Al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento internet, memorizzano un giornale (file di log) contenente le informazioni relative sia ai siti che agli strumenti informatici visitati. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente.

L'accesso a questi dati è consentito all'Amministratore del Sistema o, su autorizzazione di quest'ultimo, al personale del Sistema Informativo Aziendale.

I sistemi softtware sono programmati e configurati in modo da cancellare periodicamente i dati relativi agli accessi ad Internet ed al traffico telematico ai sensi di legge.

L'eventuale prolungamento dei tempi di conservazione è eccezionale e può aver luogo solo rispetto ad esigenze tecniche e di sicurezza del tutto particolari, in relazione all'indispensabilità del dato per l'esercizio o la difesa di un diritto in sede giudiziaria, oppure in ragione dell'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta della Polizia Giudiziaria o dell''Autorità Giudiziaria.

**USO DELLA POSTA ELETTRONICA CERTIFICATA**

La PEC (Posta Elettronica Certificata) è un sistema di una 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.

Perchè 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.

L'email inviata da un dominio non certificato, ovvero non PEC (p.e. da un normale programma di posta elettronica) ad un indirizzo di PEC non assume, invece, valore formale e legale, e pertanto non crea vincoli di alcun genere per l'ente.
L'ASST ha attivato le caselle di Posta Elettronica Certificata per diverse strutture aziendali.

**PROTEZIONE ANTIVIRUS**

Il sistema informativo aziendale è protetto da software antivirus aggiornato quotidianamente. Ogni utente/autorizzato deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema medesimo aziendale da parte di virus o ogni altro software aggressivo.

Nel caso l'antivirus ne rilevi la presenza, l'utente/autorizzato dovrà immediatamente sospendere ogni elaborazione in corso e segnalare prontamente l'accaduto al SIA e agli Amministratori di Sistema.

**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 ove 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.

### 5.1.1 Controlli

Nel rispetto del divieto di controllo a distanza del lavoratore e dello Statuto dei Lavoratori nel quale tale divieto è contenuto, l'ASST 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, l'Azienda 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 l'Azienda Ospedaliera 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 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/FOTOCOPIATRICI**

Ogni utente/autorizzato all'utilizzo delle stampanti / fotocopiatrici aziendali:

-non deve utilizzare carta riciclata recante, sul retro del foglio, dati personali;
-non deve lasciare incustodita la documentazione durante lo svolgimento delle operazioni di fotocopiatura;
-deve rendere illeggibile il contenuto della fotocopia malriuscita, prima di cestinarla;
-deve ritirare tempestivamente gli originali e le copie fatte al termine della procedura.

## 5.3 Trattamento dati attraverso la comunicazione

**CONFIDENZIALITÀ DEI DATI PERSONALI TRATTATI**

Anche nel rispetto delle vigenti norme sul segreto professionale, gli autorizzati 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 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 l'ASST, 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 P.S. 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 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 |

**b) <u>Trattamenti svolti manualmente / attraverso documentazione cartacea:</u>**

| 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<br><br>(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.
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 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 della Privacy 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. <u>Pubblicità della Privacy Policy</u>

La presente istruzione aziendale verrà diffusa attraverso la rete interna e pubblicata sul sito web aziendale nella Sezione Amministrazione trasparente - Altri contenuti - Privacy.

## 8. <u>Documenti di riferimento o Bibliografia o Sitografia</u>

D. L.gs. n. 196/2003 e s.m.i.
Regolamento Europeo n. 2016/679
Provvedimenti del Garante per la protezione dei dati personali
Sito: www.garanteprivacy.it
Codice etico e di comportamento dell'ASST di Monza