CASA DI CURA
MADONNA DEL RIMEDIO

REGOLAMENTO AZIENDALE PER IL TRATTAMENTO DEI DATI PERSONALI

Versione 1.0 del 01/11/2018
Protocollo 34/2018

1 PREMESSA

La Casa di Cura Madonna del Rimedio ha intrapreso un percorso di progressiva riorganizzazione ed informatizzazione di tutti i processi aziendali e di loro adeguamento alla normativa in materia di protezione dei dati personali.

Questo processo ha importanti ricadute sulle attività quotidiane di tutti coloro che prestano la propria opera in Casa di Cura Madonna del Rimedio (di seguito "Azienda") e notevoli implicazioni sugli aspetti dei gestione dei dati aziendali e sulla loro sicurezza. Si rende quindi necessario attivare una serie di norme, restrizioni e controlli volti a garantire la sicurezza dei processi aziendali e definire le responsabilità degli utilizzatori delle risorse nel rispetto della normativa sulla privacy.

L'adozione di queste politiche viene fatta nell'intento di:

- garantire la riservatezza delle informazioni ed il corretto trattamento dei dati personali;
- garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- provvedere ad un servizio continuativo nell'interesse dell'Azienda;
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche;
- garantire la massima sicurezza nello scambio di dati ed informazioni tra l'Azienda e le altre istituzioni.

E' infatti compito dell'Azienda:

- adottare tutti i dispositivi di sicurezza necessari a difendere i propri sistemi informatici;
- implementare meccanismi di controllo e monitoraggio per evitare intrusioni o abusi;
- responsabilizzare e formare gli operatori circa i rischi penali, civili, amministrativi connessi all'uso indebito dei mezzi informatici;
- evitare che i propri operatori, utilizzando gli strumenti informatici dell'Azienda, compiano abusi legati all'utilizzo improprio delle risorse della Rete Internet e della Rete Intranet interna e dei dati ivi contenuti.

Premesso che qualsiasi comportamento posto in essere dell'ambito di un rapporto di lavoro, tra i quali l'utilizzo delle risorse informatiche aziendali, deve sempre ispirarsi al principio della diligenza e correttezza, l'Azienda ha adottato il presente regolamento per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza del trattamento dei dati.

Il Regolamento Aziendale di seguito riportato viene incontro, quindi, alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte degli operatori aziendali e contiene informazioni utili per comprendere cosa può fare ogni operatore per contribuire a garantire la sicurezza dei sistemi informativi di tutta l'Azienda.

2 OBIETTIVI DEL DOCUMENTO

Il presente documento ha l'obiettivo fornire agli operatori idonee misure di sicurezza e linee di comportamento atte a garantire il corretto trattamento dei dati personali dei quali l'Azienda è Titolare ed il corretto e non rischioso utilizzo degli strumenti informatici, delle applicazioni, della rete interna, della posta elettronica aziendale e della navigazione Internet.

L'inosservanza delle norme sulla privacy può comportare responsabilità di natura civile e penale per l'operatore e per l'Azienda, per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

3 RIFERIMENTI NORMATIVI E DEFINIZIONI

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE» (di seguito GDPR), ha imposto la previsione ed il rispetto di requisiti, adempimenti formali e misure di sicurezza volti a garantire la tutela dei diritti dell'interessato.

Tale Regolamento, definitivamente vincolante a partire dal 25 maggio 2016, uniforma la normativa in tutti gli Stati Membri dell'Unione Europea e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3.1 PRINCIPALI DEFINIZIONI DEL GDPR

Le principali definizioni previste dall'articolo 4 del GDPR sono le seguenti:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere 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.

Particolari categorie di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del GDPR).

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.

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.

Dati relativi alla salute (o Dati sanitari): 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.

Dati personali relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).

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.

Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

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;

Pseudoanonimizzazione: 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;

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;

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

DPO – Data Protection Officer: persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratti dati personali per conto del titolare del trattamento.

Persone autorizzate al trattamento: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile. Tali operazioni possono essere effettuate solo da incaricati che operino sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

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.

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.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Violazione dei dati personali - Data breach: Violazione di sicurezza che comporti 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.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro.

3.2 PRINCIPI GENERALI DEL GDPR

Ai sensi dell'articolo 5 del GDPR i principi generali ai quali deve ispirarsi il trattamento i dati personali sono i seguenti:

Liceità, correttezza e trasparenza: i dati devo essere trattati in modo lecito e secondo correttezza**;**

Limitazione della finalità: i dati devono essere raccolti e registrati unicamente per finalità istituzionali, esplicite e legittime, e successivamente trattati in modo tale che il trattamento non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;

Minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati

Esattezza: i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati

Limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato;

Integrità e riservatezza: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;

3.3 SISTEMA DI GESTIONE PRIVACY

L'Azienda predispone le misure tecniche ed organizzative adeguate a garantire di essere in grado di dimostrare che il trattamento dei dati personali è effettuato in conformità alla normativa vigente, tenuto conto della natura dei dati trattati, dell'ambito di applicazione, del contesto operativo, delle finalità del trattamento e del possibile rischio di lesione dei diritti e delle libertà degli interessati.

Tali misure sono riesaminate e aggiornate periodicamente e compongono il "Sistema di Gestione Privacy Aziendale", che include:

a) Il Data Protection Officer (DPO);
b) Il Registro delle attività di trattamento dei dati;
c) Il sistema di attribuzione delle responsabilità del trattamento dei dati personali;
d) La documentazione relativa alle valutazioni preliminari di impatto;
e) Le regolamentazioni, le policy, le procedure e le disposizioni operative adottate per i singoli trattamenti di dati personali;
f) L'analisi dei rischi e i documenti di valutazione;
g) Il sistema di audit e verifica periodica del corretto trattamento dei dati personali;
h) Il sistema di formazione continua delle Persone Autorizzate, dei Responsabili e degli Amministratori di Sistema;

i) Il rapporto del Titolare del Trattamento dei dati con gli Interessati.

3.4 PROTEZIONE DEI DATI PERSONALI PER IMPOSTAZIONE PREDEFINITA

L'Azienda, al fine tutelare i diritti degli Interessati, nello stabilire le modalità e gli strumenti del trattamento dei dati personali, valuta preventivamente i possibili rischi aventi probabilità e gravità diverse sui diritti e libertà degli Interessati tenendo conto dello stato dell'arte dello sviluppo tecnologico, dei costi di attuazione, della natura dei dati trattati, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Inoltre, mette in atto misure tecniche e organizzative adeguate, già in fase preprogettuale e precontrattuale, per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento tenendo conto, in particolare:

- della quantità dei dati personali raccolti;
- della portata del trattamento;
- del periodo di conservazione dei dati;
- dell'accessibilità ai dati;
- dei soggetti a cui è consentito il trattamento.

Tali misure garantiscono, inoltre, che, per impostazione predefinita, i dati personali siano accessibili solo alle persone autorizzate e limitatamente a quanto necessario per il periodo di trattamento.

4 CAMPO DI APPLICAZIONE

Sulla base dell'ampia definizione di "trattamento dati" data dal GDPR, tutte le persone fisiche, che prestano la propria opera in Azienda, trattano dati personali e dati sanitari. Spesso questo avviene mediante l'uso di strumenti informatici.

Ciò posto, le presenti Istruzioni si applicano a:

- tutte le persone fisiche, lavoratori dipendenti o collaboratori dell'Azienda, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, ecc., di seguito "Perone Autorizzate") che si trovino ad operare sui dati aziendali e più specificatamente sui dati personali dei quali l'Azienda è titolare;
- tutte le attività o comportamenti posti in essere nell'ambito del rapporto di lavoro, con particolare riferimento a quelli che determinano il trattamento di un dato personale e a quelli connessi all'utilizzo delle applicazioni aziendali, della rete interna aziendale, della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'accesso dell'infrastruttura aziendale.

5 LINEE GUIDA GENERALI

Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, ogni Persona Autorizzata deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie dall'Azienda per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

1. Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e soggetti al segreto d'ufficio;

2. Le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
3. Non devono essere eseguite operazioni di trattamento per fini non previsti dai compiti assegnati;
4. Devono essere svolte le sole operazioni di trattamento necessarie al raggiungimento dei fini per i quali i dati sono stati raccolti;
5. Deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed alla eventuale distruzione.

5.1 AUTORIZZAZIONE AL TRATTAMENTO DATI

1. Come previsto dall'articolo 30 del GDPR, l'Azienda tiene costantemente aggiornato il registro delle attività di trattamento dei dati personali (c.d. Registro dei Trattamenti) quale strumento indispensabile per tenere traccia delle operazioni effettuate dall'Azienda sui dati personali degli interessati ed essere in grado di valutare gli obblighi normativi applicabili, nonché di attuare un modello di governo della privacy adeguato al proprio contesto organizzativo.
2. Il registro riporta per ogni singolo trattamento le informazioni atte a identificarlo e a specificalo nelle sue caratteristiche salienti (finalità del trattamento, categoria di interessati, categorie di dati trattati, ecc). Per ogni trattamento, inoltre, vengono individuati i ruoli aziendali autorizzati ai singoli trattamenti nell'ambito delle strutture o funzioni organizzative responsabili del servizio o processo per cui vengono raccolti i dati personali.
3. L'Azienda pubblica periodicamente nella propria intranet aziendale il "Manuale dei Trattamenti per Ruolo" che riporta per ogni ruolo aziendale i trattamenti dei dati personali autorizzati e le ulteriori specifiche di trattamento per il singolo ruolo.
4. L'attribuzione di uno specifico ruolo nell'ambito dei processi aziendali (mediante ordine di servizio o turni di servizio) equivale alla nomina, per il periodo di svolgimento del ruolo, quale "Persona Autorizzata" ai trattamenti relativi.

5.2 ACCESSO AI DATI

1. I dati personali cui è consentito accedere sono quelli la cui conoscenza è strettamente necessaria per adempiere ai compiti affidati e indispensabili per l'esecuzione delle prestazioni aziendali.
2. Le Persone Autorizzate possono effettuare esclusivamente i trattamenti di dati personali definiti per lo specifico ruolo nel "Manuale dei Trattamenti per Ruolo", con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea, degli strumenti informatici, e delle banche dati aziendali che contengono i predetti dati personali nei limiti di quanto previsto per la specifico trattamento dallo specifico ruolo.
3. Di norma tutti gli archivi cartacei e digitali e le relative applicazioni che ne danno accesso sono configurati in modo da limitare al massimo i dati accessibili alla singola Persona Autorizzata. Nel caso, per questioni organizzative o tecniche, ciò non fosse completamente possibile, la Persona Autorizzata non deve mai comunque accedere a dati personali non strettamente necessari allo svolgimento della propria attività.

5.3 RISERVATEZZA DELLE INFORMAZIONI

1. Occorre prestare molta attenzione alla riservatezza delle informazioni scambiate e alla custodia dei dati al fine di garantirne l'integrità, la disponibilità e la riservatezza.
2. Nessuna informazione riservata aziendale, in particolare quelle contenenti dati personali, può essere condivisa con personale non autorizzato, interno o esterno. Il trattamento dei dati da parte delle Persone Autorizzate al trattamento è vincolato al rispetto del segreto d'ufficio.
3. Il vincolo di riservatezza è valido anche una volta terminato il trattamento dei dati personali e una volta terminato il rapporto di lavoro.

5.4 LA POSTAZIONE DI LAVORO

1. Il Personal Computer (PC) aziendale affidato direttamente alla Persona Autorizzata o assegnato al servizio nel quale la Persona Autorizzata opera è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dei dati aziendali.
2. La Persona Autorizzata non può modificare le caratteristiche di sistema operativo e software impostate sul proprio PC, né può installare o utilizzare programmi non autorizzati dall'Azienda.
3. La Persona Autorizzata non può smontare o spostare il PC né collegare o scollegare le relative periferiche (stampati, scanner, mouse, tastiere, ecc). La postazione di lavoro composta da PC e periferiche connesse può essere gestita solo dal personale a ciò preposto.
4. La Persona Autorizzata non deve salvare sul PC file personali quali, a titolo di esempio, fotografie, file musicali, file video, file di attività extra lavorative.
5. La Persona Autorizzata non può collegare al PC o utilizzare supporti removibili di origine sconosciuta (hard disk esterni, penne usb etc.). Ad esempio, non può assolutamente collegare al PC una chiavetta USB trovata per caso.
6. La Persona Autorizzata non può utilizzare risorse informatiche personali (PC, notebook, tablet, smartphone, ecc.) per accedere alla rete o ai dati aziendali a meno che non sia stato esplicitamente autorizzato. In tal caso anche per gli apparati personali la Persona Autorizzata deve attenersi alle stesse disposizioni previste per gli apparati aziendali.
7. Il PC non deve mai essere lasciato incustodito con le applicazioni lasciate accessibili; nel caso di spostamenti anche brevi deve sempre essere attivato il blocco "screen saver" con password. Al termine dell'utilizzo delle applicazioni occorre sempre eseguire il logout (disconnessione) dalle stesse.
8. Allo stesso modo non devono essere lasciati incustoditi dispositivi portatili, ancorché bloccati, (notebook, tablet o smartphone) che contengano dati aziendali o mediante i quali sia possibile accedere ai dati o alla rete aziendale.
9. Il sistema operativo e gli applicativi installati sul PC o utilizzati via web registrano l'attività fatta dalla Persona Autorizzata nello svolgimento del proprio lavoro attribuendogliene la paternità. Quindi tutte le attività svolte sul PC ed i dati caricati sugli applicativi con determinate credenziali sono considerati "firmati elettronicamente" dal titolare delle credenziali stesse. Lasciare un PC non bloccato con le applicazioni accessibili equivale a lasciare sulla scrivania un foglio bianco con in calce la propria firma autografa sul quale chiunque può scrivere e farvi dichiarare ciò che vuole.
10. Il PC deve essere spento al termine del suo utilizzo, in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.

5.5 LE CREDENZIALI DI ACCESSO

1. L'Azienda provvede da consegnare alla Persona Autorizzata le credenziali di accesso per alle diverse applicazioni e servizi aziendali ai quali è abilitato. In Azienda è attivo un "dominio aziendale" denominato "MDR" e l'utente di dominio dà accesso al PC. Ove possibile, vengono utilizzate tecniche di "accesso integrato" così da utilizzare l'utente di dominio anche per l'accesso ad altre applicazioni o servizi aziendali.
2. Le credenziali di accesso (utente e password) sono strettamente personali, vanno custodite con diligenza e non devono mai essere comunicate ad altri. La password deve essere sempre cambiata al primo utilizzo e successivamente secondo le scadenze definite dal sistema di autenticazione nel rispetto di quanto previsto dalla normativa sulla privacy.
3. La password deve essere composta rispettando i requisiti minimi di complessità imposti dal sistema di autenticazione. I caratteri che la compongono non devono contenere informazioni facilmente riconducili alla Persona Autorizzata titolare quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.
4. La Persona Autorizzata deve sempre prestare la massima attenzione al momento della digitazione della password in presenza di altri soggetti. Occorre sempre accertarsi che nessuno dei presenti possa memorizzare la sequenza di tasti o riprendere con un smartphone o altro strumento l'operazione. E' buona norma avere le stesse accortezze e precauzioni di quanto di digita il PIN del bancomat. Allo stesso modo, è opportuno che il soggetto terzo che dovesse assistere alla digitazione della password da parte di un'altra Persona Autorizzata diriga, durante questa fase, lo sguardo da un'altra parte.
5. La password non deve essere mai trascritta su supporti cartacei (es. fogli, post-it) o informatici (file txt, xls, doc), né deve essere lasciata memorizzata sul proprio PC.
6. La Persona Autorizzata non deve utilizzare credenziali di altre Persone Autorizzate nemmeno se fornite volontariamente dal titolare delle stesse; Nel caso in cui venga in qualsiasi modo a conoscenza delle credenziali di altri operatori, la Persona Autorizzata deve darne immediata comunicazione al Servizio IT che a sua volta imporrà il cambio password al titolare delle stesse.
7. Nel caso di smarrimento delle credenziali di accesso la Persona Autorizzata deve prontamente darne comunicazione all'Azienda che provvederà a cambiarle ed a comunicargliele nuovamente. Nel caso la Persona Autorizzata abbia anche solo il sospetto che le proprie credenziali siano conosciute da terzi deve immediatamente provvedere al cambio della password.

5.6 LA RETE AZIENDALE

1. Per l'accesso alla rete aziendale ciascuna Persona Autorizzata verrà specificamente autorizzata dall'Azienda.
2. Le cartelle della Persona Autorizzata o le cartelle di gruppo presenti nei server aziendali sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e Backup. Si ricorda che tutti i dischi o altre unità di memorizzazione locali dei singoli PC non sono soggette a Backup. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico della singola Persona Autorizzata.
3. L'Azienda può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza dei dati sia sui singoli PC sia sulle unità di rete.

4. Con regolare periodicità (almeno ogni tre mesi), ciascuna Persona Autorizzata provvede alla pulizia dei propri archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5.7 PROTEZIONE ANTIVIRUS

1. Il Sistema Informatico Aziendale è protetto da software antivirus aggiornato quotidianamente. Ogni Persona Autorizzata deve comunque tenere comportamenti tali da ridurre il rischio di attacco mediante virus o mediante ogni altro software malevolo.
2. Occorre sempre essere consapevoli che la posta elettronica e la navigazione Internet sono veicoli per l'introduzione sul proprio PC (e quindi in Azienda) di virus e altri elementi potenzialmente dannosi. Questi strumenti vanno quindi sempre utilizzati con un adeguato livello di attenzione e nel rigoroso rispetto delle direttive impartite.
3. Nel caso per lo svolgimento delle attività lavorativa si rendesse necessario l'utilizzo di supporti removibili (chiavette USB, Hard Disk esterni, CD, DVD), ogni Persona Autorizzata deve prestare la massima attenzione accertandosi preventivamente della provenienza del supporto stesso, effettuando sempre scansione antivirus prima di accedere al suo contenuto e avvertendo immediatamente il Servizio IT nel caso in cui siano rilevati virus.
4. Nel caso l'antivirus rilevi la presenza di un virus, segnalandolo con apposito messaggio, o si verifichi un malfunzionamento del PC, che possa far sospettare la presenza di un virus, la Persona Autorizzata deve:
    a. sospendere ogni operazione sul PC evitando di lavorare con il sistema infetto;
    b. informare immediatamente in Servizio IT;
    c. chiudere tutte le applicazioni senza spegnere il PC.

5.8 UTILIZZO DEI PC PORTATILI, TABLET E SMARTPHONE AZIENDALI

1. La Persona Autorizzata è responsabile degli strumenti di elaborazione e comunicazione portatili assegnatigli dall'Azienda (notebook, tablet e smartphone) e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro o altrove.
2. La Persona Autorizzata deve essere consapevole che uno strumento portatile che contiene dati aziendali o che viene utilizzato per accedervi presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa e pertanto deve attenersi, oltre che alle disposizioni previste per le postazioni fisse, alle specifiche precauzioni previste per gli apparecchi aziendali portatili. Gli strumenti informatici personali autorizzati sono assimilati agli strumenti aziendali.
3. Al pari degli altri strumenti aziendali, anche gli strumenti portatili devono essere utilizzati solo per attività pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto previa autorizzazione dell'Azienda.
4. La Persona Autorizzata deve operare sempre nella massima riservatezza e protezione quando si utilizzano strumenti portatili aziendali in pubblico avendo cura di evitare che osservatori indiscreti possano carpire i dati visualizzati o le credenziali di accesso digitate.
5. La Persona Autorizzata deve prestare, altresì, la massima attenzione alla rete utilizzata per connettere ad internet gli strumenti portatili aziendali. Se disponibile una connessione dati cellulare

del proprio smartphone o chiavetta dati (c.d. UMTS) deve essere sempre utilizzata questa privilegiandola rispetto alle reti WiFi. Se la connessione UMTS non fosse disponibile devono essere evitate sempre le reti WiFi pubbliche aperte e senza password di protezione. Possono essere utilizzare reti WiFi protette personali o messe a disposizione da clienti o fornitori avendo cura di utilizzare solo connessioni criptate (HTTPS) per accedere ai dati aziendali.

6. Lo strumento portatile non deve essere mai lasciato incustodito in caso di utilizzo in ambito esterno all'Azienda e deve essere conservato in un luogo sicuro alla fine della giornata lavorativa;
7. Lo smartphone o il tablet aziendale non deve mai essere collegato a PC non aziendali anche solo per finalità di ricarica della batteria. Questa semplice attività può consentire al PC l'accesso immediato a tutti i dati presenti nello smartphone o nel tablet.
8. La Persona Autorizzata deve avvertire tempestivamente il Servizio IT in caso di furto o smarrimento dello strumento portatile aziendale e da questo riceverà le opportune indicazioni.

5.9 RIPRESE VIDEO E FOTOGRAFICHE IN AZIENDA

1. E' sempre proibito fare fotografie o filmati all'interno del perimetro dell'Azienda. Non devono mai essere fotografati o filmati pazienti, parenti, colleghi, documenti, locali, strutture e attrezzature aziendali.
2. Le Persone Autorizzate non devono mai, nemmeno per esigenze lavorative, fotografare o riprendere documenti contenenti dati aziendali, dati personali, o peggio dati sanitari. E' assolutamente proibita la pratica di utilizzare sistemi di instant messaging (Whatsapp, Messenger, Telegram, ecc.) per scambiarsi immagini che contengano dati sanitari con altre Persone Autorizzate o con terzi.
3. Ogni Persona Autorizzata deve dissuadere le altre Persone Autorizzate, i pazienti, i parenti o il personale esterno in genere dal fare fotografie e filmati all'interno delle strutture aziendali e soprattutto dal condividerli sui social network (Facebook, Instagram, Twitter, ecc) o da scambiarseli via sistemi di instant messaging (Whatsapp, Messenger, Telegram, ecc.).

5.10 UTILIZZO E CONSERVAZIONE DI SUPPORTI REMOVIBILI

1. Tutti i supporti rimovibili (pennine USB, hard disk portatili, CD, DVD, floppy disk), contenenti dati personali nonché informazioni aziendali in genere, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto o, successivamente alla cancellazione, recuperato.
2. Al fine di assicurare la distruzione e l'inutilizzabilità dei supporti rimovibili contenenti dati personali, ciascuna Persona Autorizzata dovrà contattare il personale del Servizio IT e seguire le istruzioni da questo impartite.
3. In ogni caso, i supporti rimovibili contenenti dati personali devono essere dalle Persone Autorizzate adeguatamente custoditi in armadi chiusi.
4. I supporti rimovibili di incerta provenienza non devono mai in nessun caso essere connessi ai PC aziendali (fissi o mobili) o comunque alla rete aziendale.
5. La Persona Autorizzata è responsabile della custodia dei supporti removibili a lui assegnati e dei dati aziendali in essi contenuti;

5.11 UTILIZZO DI TELEFONI, FAX, STAMPANTI E FOTOCOPIATRICI

1. Il telefono aziendale affidato alla Persona Autorizzata è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, e non sono quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità e urgenza.
2. Fax, stampanti e fotocopiatrici aziendali devono essere utilizzati esclusivamente per finalità lavorative ed attenendosi a specifiche disposizioni in merito alla produzione, utilizzo e distribuzione dei documenti aziendali.
3. Nel caso venga stampato un documento contenente dati personali occorre prestare la massima attenzione alla stampante alla quale viene inviata la stampa. Occorre sempre prediligere stampanti presenti nello stesso locale nel quale si trova il PC dal quale si lancia la stampa o, in mancanza, stampanti posizionate in locali ai quali possano accedere solo Persone Autorizzate a visualizzare i dati stampati.
4. Le stampe contenenti dati personali devono essere immediatamente prelevate dalla stampante per essere opportunamente archiviate.
5. In ogni caso occorre ridurre al minimo la produzione di copie cartacee ed utilizzarle solo se strettamente necessarie e se previsto dalle diverse procedure aziendali.
6. La Persona Autorizzata non può smontare, spostare o modificare la configurazione di telefoni, fax, stampanti e fotocopiatrici. Tutte queste attrezzature possono essere gestite solo dal personale a ciò preposto.

5.12 UTILIZZO DELLA POSTA ELETTRONICA

1. Le caselle di posta elettronica assegnate alla Persona Autorizzata sono uno strumento di lavoro e le persone assegnatarie sono responsabili del corretto utilizzo delle stesse. Le caselle possono essere personali (nome.cognome@azienda.it) ad esclusivo utilizzo del singola Persona Autorizzata o di servizio/ufficio (amministrazione@azienda.it) utilizzate da più Persone Autorizzate dall'ambito del servizio/ufficio.
2. Le caselle di posta elettronica devono essere utilizzate solo per motivi strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, la Persona Autorizzata non potrà utilizzare la posta elettronica per:
    a. l'invio o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) o file in genere non legati all'attività lavorativa;
    b. l'invio o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
    c. la partecipazione a catene telematiche (o di Sant'Antonio);
    d. iscriversi a newsletter, forum, blog, o servizi on line in genere non strettamente legati all'attività lavorativa.
3. Il contenuto di una casella di posta aziendale è considerato sempre "informazione aziendale riservata" se non anche, a seconda dei messaggi ivi presenti, archivio contenente dati personali.
4. L'accesso alla mail aziendale può avvenire di norma solo utilizzando gli strumenti aziendali. Può essere concesso l'accesso alla casella di posta anche via web mail e/o via client SMTP. In questo

caso la Persona Autorizzata deve porre la massima attenzione all'utilizzo di questo servizio sia direttamente via web browser sia mediante configurazione della connessione alla casella di posta su un proprio PC portatile, tablet o smartphone. Devono essere strettamente osservate le disposizioni in merito alla gestione delle credenziali accesso, avendo la consapevolezza che l'impiego di queste ultime all'esterno dei locali aziendali rende il loro l'utilizzo ancora più critico.

5. La Persona Autorizzata che utilizza la mail aziendale mediante strumenti non aziendali può accedervi solo con strumenti dei quali la Persona Autorizzata abbia l'utilizzo esclusivo e che siano sotto il suo diretto e costante controllo. Non è ammesso l'accesso alla mail aziendale mediante strumenti posizionati in locali pubblici, di clienti o fornitori, di parenti o amici.
6. La Persona Autorizzata deve prestare la massima attenzione alla digitazione in pubblico delle credenziali di accesso alla casella di posta aziendale ed alla consultazione dei messaggi ivi contenuti, avendo cura che nessuno possa carpire volontariamente od involontariamente dette informazioni. A titolo di esempio è sufficiente che qualche malintenzionato riprenda con lo smartphone la testiera mentre si digita la password o fotografi il monitor mentre si visualizza una mail per rubare informazioni aziendali o dati personali.
7. L'accesso alla posta elettronica aziendale dall'esterno dell'azienda deve essere fatto sempre mediante connessioni sicure e criptate. Se disponibile una connessione UMTS deve sempre essere utilizzata questa. In caso di indisponibilità, non possono mai essere utilizzare reti wireless non protette da password. E' possibile utilizzare la propria rete wireless casalinga o quella messa a disposizione da clienti o fornitori a patto che si utilizzino connessioni criptate (HTTPS).
8. L'accesso via web alla mail aziendale crea sempre nello strumento utilizzato delle copie degli allegati scaricati se non anche dei messaggi letti. La configurazione dell'accesso alla mail mediante il client di posta del proprio PC, tablet o smartphone crea sugli stessi una copia integrale del contenuto dalla casella di posta. La Persona Autorizzata deve pertanto porre la massima attenzione alla custodia degli strumenti personali utilizzati per accedere alla mail aziendale. In caso di smarrimento, furto o accesso abusivo un terzo potrebbe entrare in possesso di documenti riservati aziendali o dati personali. Dalla lettura sistematica dei messaggi di una casella di posta aziendale, infatti, un estraneo potrebbe entrare in possesso di atti, dati di stretta pertinenza aziendale la cui conoscenza potrebbe causare gravi danni all'Azienda.
9. Nell'utilizzo della posta elettronica ciascuna Persona Autorizzata deve tenere in debito conto che i soggetti esterni di regola attribuiscono carattere istituzionale alla corrispondenza ricevuta da una casella di posta aziendale. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi.
10. La Persona Autorizzata nella formulazione dei messaggi deve sempre far uso di un linguaggio appropriato, corretto e rispettoso che tuteli la dignità delle persone, l'immagine e la reputazione dell'Azienda.
11. Non devono essere predisposti messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.
12. Occorre prestare sempre la massima attenzione alle informazioni inviate via email. Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare.
13. In caso di errore nella spedizione di un messaggio occorre contattare il destinatario cui è stata trasmessa per errore la comunicazione chiedendone l'eliminazione del messaggio compresi gli allegati.

14. Occorre limitare al minimo l'invio mediante posta elettronica di dati personali. In questi casi occorre avere l'assoluta certezza che l'indirizzo mail utilizzato sia corretto.
15. Deve essere prestata la massima attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque estraneo dal proprio contesto lavorativo. In tali casi le Persone Autorizzate non devono mai in nessun caso:
    a. aprire i file allegati al messaggio;
    b. eseguire il download di file linkati nel messaggio o accedere a siti FTP riportati nel messaggio;
    c. rispondere al messaggio in quanto tale atto assicura al mittente l'esistenza del destinatario;

    Il messaggio deve essere immediatamente cancellato e il cestino svuotato.
16. La casella di posta deve essere mantenuta in ordine, conservando le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni o indicazioni operative provenienti da soggetti esterni, e cancellando documenti inutili e soprattutto allegati ingombranti. Il cestino della casella deve essere svuotato regolarmente.
17. 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 dell'Azienda. In tal caso, la funzionalità deve essere attivata dalla Persona Autorizzata titolare della casella di posta. In alternativa ciascuna Persona Autorizzata può indicare, mediante disposizione scritta, un collega delegato all'accesso al proprio account di posta elettronica aziendale durante le assenze, anche non programmate.
18. In caso di assenza non programmata (ad es. per malattia) la procedura di risposta automatica, qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni, verrà attivata a cura del Servizio IT.
19. Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato dell'Azienda potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella politica aziendale.

5.13 NAVIGAZIONE INTERNET

1. Il PC assegnato alla singola Persona Autorizzata o al Servizio nel quale la Persona Autorizzata opera ed abilitato alla navigazione Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.
2. In questo senso, a titolo puramente esemplificativo, la Persona Autorizzata non potrà utilizzare internet per:
    a. l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione;

b. l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Azienda e comunque nel rispetto delle normali procedure di acquisto aziendali;

c. ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;

d. la partecipazione a forum o blog non professionali, l'utilizzo di chat line o social network, anche utilizzando pseudonimi, se non espressamente autorizzati dall'Azienda;

3. Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda adotta di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti.

5.14 TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

1. Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.
2. Quando i dati personali devono essere comunicati telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che lo stesso sia legittimato ad ottenere quanto domandato.
3. Nel caso di comunicazioni telefoniche a terzi di dati personali, l'elenco delle identità e dei relativi dei numeri telefonici autorizzati a riceverle deve essere desunto dai dati comunicati dall'interessato. Nel caso di chiamate in ingresso, se il numero del chiamate non fosse rilevabile dal display del telefono, la Persona Autorizzata deve richiederlo all'interlocutore e annotarselo assieme alla sua identità provvedendo quindi a richiamarlo verificandone ulteriormente l'identità.
4. L'invio o la ricezione via Fax di dati personali deve essere limitata allo stretto necessario. Nel caso di invio occorre essere assolutamente certi del numero di telefono al quale il fax viene inviato, dell'identità della persona fisica che poi entrerà in possesso delle informazioni ed infine del fatto del il soggetto destinatario sia autorizzato a conoscerle. Occorre sempre avere la ragionevole certezza che il fax al quale si inviano i documenti contenenti dati personali sia presidiato e che i documenti entrino in possesso solo ed esclusivamente della persona con la quale si intende interloquire.
5. Quando il dato personale deve essere inviato a mezzo posta elettronica occorre prestare la massima attenzione affinché l'indirizzo di posta elettronica del destinatario sia corretto e gli eventuali file allegati siano quelli che realmente si intende inviare.
6. Le Persone Autorizzate che provvedono alla duplicazione di documenti contenenti dati personali con stampanti, fotocopiatrici o altre apparecchiature, in caso di copia erronea, non correttamente leggibile o comunque non più necessaria sono tenuti a distruggere il documento esclusivamente mediante apposita macchina "distruggi documenti". Si ricorda che anche la distruzione di un documento cartaceo è considerato un "trattamento di dati" ed in quanto tale deve essere fatta secondo la normativa, ossia con un distruggi documenti del "livello di sicurezza" corretto sulla base al tipo di dati contenuti ed idoneo a garantire la non leggibilità o ricostruibilità del documento originario.

5.15 ARCHIVI CARTACEI

1. Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima

perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o anche ad interni non autorizzati al trattamento.

2. In caso di trattamento di dati personali tutta la documentazione cartacea deve essere conservata in armadi o cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.
3. L'accesso a tutti i locali aziendali contenenti archivi cartacei deve essere consentito solo a personale preventivamente autorizzato dall'Azienda.

6 LINEE GUIDA PER LA GESTIONE DEI DATI SANITARI

Buona parte dei dati personali trattati in Azienda sono Dati Sanitari, ossia dati personali che rivelano informazioni relative allo stato di salute di una persona.

Vista la criticità del trattamento di questa tipologia di dati, l'Azienda ritiene opportuno prevedere delle specifiche e più stringenti norme. In questo contesto per Paziente si intente la persona fisica cui si riferiscono i dati sanitari.

6.1 RACCOLTA DEI DATI SANITARI

1. La raccolta dei dati personali e sanitari ed i loro inserimento negli archivi aziendali è consentito solo dopo aver fornito al paziente l'informativa sul trattamento dei propri dati ed aver successivamente raccolto il suo consenso scritto al trattamento. Sono fatte salve le situazioni di emergenza sanitaria nelle quali il paziente non sia cosciente o comunque non sia in grado di prestare il proprio consenso. In questi casi l'informativa dovrà essere resa ed il consenso raccolto non appena la situazione sanitaria del paziento lo dovesse consentire.
2. Le uniche finalità per le quali l'Azienda raccoglie i dati sanitari sono quelle di assistenza, diagnosi e cura. La Persona Autorizzata non può in nessun caso utilizzare i dati raccolti per finalità diverse.
3. La Persona Autorizzata addetta alla prenotazione/accettazione dei pazienti e alla raccolta dei loro dati sanitari deve garantire la tutela della riservatezza di questi ultimi:
   a) assicurandosi che i soggetti terzi presenti nel locale (sala d'attesa o studio medico) rispettino le distanze di cortesia;
   b) utilizzando un tono di voce udibile esclusivamente dall'interessato.
4. La Persona Autorizzata deve inoltre prestare particolare attenzione all'inserimento dei dati personali e sanitari nei programmi che gestiscono i processi sanitari, verificando scrupolosamente la correttezza dei dati raccolti.
5. Nel caso in cui venga richiesta la prenotazione di una prestazione sanitaria per telefono, l'addetto è tenuto ad accertarsi dell'identità del soggetto chiamante prima di procedere alla prenotazione. In ogni caso è assolutamente vietato rivelare dati personali di pazienti presenti sul sistema a soggetti terzi che ne facciano richiesta, neppure per finalità di prenotazione.

6.2 RISERVATEZZA DEI DATI SANITARI

1. La Persona Autorizzata è tenuta ad adottare tutte le misure di sicurezza concretamente necessarie a garantire la costante tutela della riservatezza dei dati sanitari dei pazienti.
2. Tutti le Persone Autorizzate che trattano i dati sanitari devono:
   a. condividere i dati sanitari solo con le altre Persone Autorizzate direttamene coinvolte nel processo di assistenza, diagnosi e cura e condividere solo i dati strettamente necessari allo svolgimento delle attività di ciascuno in base al ruolo ricoperto in Azienda;

b. evitare di dare o chiedere ad altre Persone Autorizzate informazioni sulle condizioni cliniche dei pazienti per mere esigenze informative personali;

c. evitare di confrontarsi con le altre Persone Autorizzate sulle condizioni cliniche dei pazienti nei corridoi o in luoghi nei quali possano essere presenti persone interne non autorizzate o soggetti terzi;

d. nel caso in cui il paziente condivida la camera con altri soggetti, effettuare i colloqui col paziente o con i suoi familiari se possibile in un luogo riservato e comunque nel modo più riservato possibile nelle specifiche condizioni logistiche;

e. assicurarsi che pazienti o visitatori non entrino nelle sale riservate al personale dove possano essere custoditi dati personali e sanitari;

f. assicurarsi che le persone interne estranee al reparto o servizio non entrino nelle sale riservate al personale dove possano essere custoditi dati personali e sanitari;

g. dialogare con i pazienti allo sportello con voce moderata ed in modo riservato evitando che le altre persone in attesa possano sentire quando detto;

h. effettuare le chiamate dei pazienti esclusivamente per numero di attesa, senza fare alcun riferimento al nome o cognome del paziente o alla tipologia di prestazione sanitaria che debba effettuare;

i. assicurarsi di chiudere la porta dell'ambulatorio prima di iniziare la visita o la raccolta delle informazioni sanitarie del paziente.

3. Le Persone Autorizzate che per qualsiasi motivo dovessero trovarsi in luoghi della struttura nei quali siano presenti dati sanitari cartacei o siano visualizzati su PC dati sanitari ai quali non sono autorizzati devono sempre mettersi nelle condizione di non accedervi nemmeno per caso; non devono mai indugiare con lo sguardo su dati che fossero visibili su documenti cartacei o sullo schermo di un PC.

6.3 ACCESSO AI DATI SANITARI

1. A Ciascuna Persona Autorizzata è consentito accedere esclusivamente ai dati personali e sanitari dei pazienti in favore dei quali debba rendere la propria prestazione per finalità di assistenza, diagnosi e cura. È tassativamente vietato trattare i dati dei pazienti per finalità diverse da quelle sopra indicate.

2. Accedendo ai dati sanitari, la Persona Autorizzata deve sempre prestare attenzione a che le altre persone presenti non possano visualizzare dati ai quali non sono autorizzati. Questo vale sia per i soggetti esterni (pazienti, visitatori, fornitori, ecc) sia per le altre persone interne non autorizzate per funzione svolta o perché estranei al reparto o servizio. Occorre sempre porsi la domanda se la persona che visualizza i dati assieme a noi abbia titolo o meno per accedere ai dati.

3. Gli schermi dei monitor dei PC fissi usati per accedere a dati sanitari devono essere sempre posizionati in modo da non essere visibili dall'esterno del locale che li ospita; i PC portatili utilizzati nei corridoi dei reparti per registrare i dati sanitari non devono mai essere lasciati incustoditi con i dati sanitari visibili.

4. Particolare attenzione deve essere prestata alla custodia e all'archiviazione delle cartelle cliniche cartacee, dei referti clinici cartacei dei pazienti o di tutti i documenti stampati per la gestione dei processi sanitari (liste di pazienti, di esami, ecc.), assicurandosi di non depositarli, neppure temporaneamente, in luoghi in cui rimangano incustoditi e nei quali possano accedervi soggetti terzi non autorizzati.

6.4 COMUNICAZIONE DI DATI SANITARI E TRASMISSIONE DI DOCUMENTI

1. Nessun dato personale e sanitario può essere comunicato o trasmesso a terzi se non per finalità istituzionali e solo nei casi espressamente previsti da specifiche procedure interne.
2. Le Persone Autorizzate possono comunicare i dati sanitari solo al paziente interessato o un soggetto che lo assista e che sia munito dei necessari poteri di rappresentanza (genitori, amministratori di sostegno, tutori) e previo accertamento della sua identità. Nel caso il paziente lo abbia espressamene richiesto, i dati possono essere comunicati anche agli altri soggetti nominativamente indicati dal paziente (o da chi lo rappresenta) per lo specifico episodio di cura.
3. In ogni caso le informazioni contenenti dati sanitari comunicate a terzi autorizzati devono essere quelle strettamente indispensabili per la gestione dell'episodio di cura del paziente e non per mere esigenze informative dell'interlocutore.
4. Anche la sola conferma della presenza di un paziente in cura presso la Casa di Cura è considerato un dato sanitario e non deve essere mai comunicato a terzi se non seguendo le regole dei paragrafi precedenti.
5. Le comunicazioni telefoniche di dati sanitari devono essere sempre ridotte ai casi strettamente indispensabili al processo di assistenza, diagnosi e cura e possono avvenire solo dopo essersi accertati sia dell'identità dell'interlocutore sia dell'esistenza di una specifica autorizzazione sullo specifico episodio di cura. Devono essere, ove possibile, privilegiate le comunicazioni di persona.
6. L'Azienda si pone come obiettivo la totale eliminazione della trasmissione o ricezione dei dati sanitari a mezzo fax. Per raggiungerlo ogni Persona Autorizzata deve sempre dissuadere l'interlocutore dall'utilizzo del fax quale mezzo di trasmissione di dati sanitari invitandolo sempre a fornire in alternativa un indirizzo di posta elettronica. I dati sanitari possono essere inviati via fax solo se l'interlocutore non dovesse realmente disporre di altri strumenti di comunicazione. Nel caso di invio occorre essere assolutamente certi del numero di telefono al quale il fax viene inviato, dell'identità della persona fisica che poi entrerà in possesso delle informazioni e, infine, del fatto che il soggetto destinatario sia autorizzato a conoscerle. Occorre sempre avere la ragionevole certezza che il fax al quale si inviano i documenti contenenti dati sanitari sia presidiato e che i documenti entrino in possesso solo ed esclusivamente della persona con la quale si intende interloquire. Nel caso di ricezione occorre chiedere all'interlocutore di essere avvertiti prima dell'invio dei documenti in modo da poter presidiare il fax e ritirare il documento non appena stampato.
7. Quando il dato sanitario deve essere inviato a mezzo posta elettronica occorre prestare la massima attenzione affinché l'indirizzo del destinatario sia corretto e gli eventuali file allegati siano quelli che realmente si intende inviare.
8. Nel fosse necessario inviare via posta elettronica di schermate di applicativi software o di report a scopo di richiesta di assistenza, i dati presenti nell'immagine devono essere per quanto possibile preventivamente anonimizzati cancellando sempre il nome e la data di nascita del paziente ed identificando i dati oggetto di assistenza mediante codice (numero impegnativa, numero di cartella clinica, ecc.)
9. I documenti contenenti dati sanitari (analisi di laboratorio, referti, documenti contenuti nella cartella clinica e foglio per le dimissioni SDO) possono essere consegnati a mano solo una volta accertata l'identità del soggetto richiedente, che deve coincidere col paziente interessato o un soggetto che lo assista e che sia munito dei necessari poteri di rappresentanza (genitori, amministratori di sostegno, tutori) o di apposita delega accompagnata da copia fotostatica del documento d'identità del delegante e del delegato.

6.5 ARCHIVI CARTACEI E RIPRODUZIONE DI COPIE CARTACEE

1. E' necessario prestare particolare attenzione all'archiviazione delle cartelle cliniche e di tutti i documenti contenenti dati sanitari. Durante il ricovero dei pazienti, le cartelle e gli altri documenti non devono mai restare incustoditi, neppure all'interno delle sale di medici e infermieri se queste sono accessibili a terzi. Il personale sanitario deve aver cura di riporli tempestivamente negli appositi carrelli o negli armadi presenti all'interno delle sale di medici e infermieri e di chiudere a chiave i predetti archivi ogniqualvolta vi sia il rischio che il carrello o la sala possano non essere continuativamente presidiati.
2. Anche la sola movimentazione di documenti contenenti dati personali o sanitari è considerata un trattamento dati e tutti gli operatori che la effettuano devono essere specificamente autorizzati.
3. La movimentazione delle cartelle cliniche complete, dal reparto verso l'Ufficio Ricoveri e da questo verso l'archivio temporaneo, deve avvenire sempre in fascicoli o faldoni chiusi dai quali non sia desumibile esteriormente alcun dato personale o sanitario. Nei vari tragitti le cartelle non devono mai restare incustodite.
4. L'accesso all'archivio delle cartelle cliniche deve avvenire sempre garantendo la sicurezza fisica dei locali che le contengono. Gli archivi non devono mai restare incustoditi ed accessibili a terzi nemmeno per brevissimi periodi. La movimentazione delle cartelle dall'archivio temporaneo verso l'ufficio ricoveri per necessità di accesso ad episodi di ricovero chiusi deve avvenire seguendo le regole del paragrafo precedente.
5. La duplicazione delle cartelle cliniche deve avvenire in locali e con processi idonei a garantire la riservatezza dei dati sanitari. Per il periodo che la cartella sta fuori dall'archivio deve essere depositata in cassetti, armadi o locali chiusi a chiave che garantiscano che nessun terzo possa accedervi. Solo la Persona Autorizzata che esegue materialmente la copia dei documenti deve accedere fisicamente alla cartella.
6. Il trasporto dei referti ambulatoriali interni che devono essere archiviati in cartella clinica deve avvenire sempre in busta chiusa o utilizzando un contenitore che garantisca che i dati sanitari ivi presenti non siano accessibili a soggetti terzi o comunque non autorizzati, compreso l'operatore che li trasporta.
7. I referti ambulatoriali esterni non immediatamente consegnati ai pazienti devono essere fatti pervenite al servizio preposto alla consegna in busta chiusa. Quest'ultimo provvederà quindi a consegnarli a mano solo una volta accertata l'identità del soggetto richiedente, che deve coincidere con paziente interessato o un soggetto che lo assista e che sia munito dei necessari poteri di rappresentanza (genitori, amministratori di sostegno, tutori) o di apposita delega accompagnata da copia fotostatica del documento d'identità del delegante e del delegato.
8. Le Persone Autorizzate che provvedono alla duplicazione di documenti contenenti dati sanitari con stampanti, fotocopiatrici o altre apparecchiature, in caso di copia erronea, non correttamente leggibile o comunque non più necessaria sono tenuti a distruggere il documento esclusivamente mediante apposita macchina "distruggi documenti" che garantisca la non leggibilità o ricostruibilità del documento originario.

6.6 CAMPIONI BIOLOGICI UMANI

1. I campioni biologici umani sono a tutti gli effetti "dati particolari" e le regole di gestione sono le stesse previste per il trattamento dei dati sanitari.
2. Dal prelievo sino alla consegna al laboratorio analisi, sia interno che esterno, i campioni biologici non devono mai restare incustoditi, neppure all'interno delle sale di medici e infermieri se queste sono accessibili a terzi. Il trasporto verso il laboratorio interno o esterno deve avvenire in un

contenitore che garantisca che i campioni ivi presenti non siano accessibili a soggetti terzi o comunque non autorizzati.

3. Durante il processo di analisi in laboratorio i campioni biologici non devono mai stare incustoditi ed accessibili a terzi nemmeno per brevissimi periodi.
4. I campioni biologici non più necessari devono essere distrutti al termine delle analisi in modo tale che non possano essere più analizzati e ricondotti al paziente dal quale sono stati prelevati.

7 ACCESSO AI DATI DELLA PERSONA AUOTRIZZATA

1. L'Amministratore di Sistema dell'Azienda può accedere ai dati trattati dalla Persona Autorizzata tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici, manutentivi o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento, sostituzione, implementazione di programmi, manutenzione hardware).
2. Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale del Servizio IT incaricato accederà ai dati su richiesta della Persona Autorizzata o comunque previo avviso al medesimo.
3. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato del Servizio IT avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.
4. Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).
5. L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata della Persona Autorizzata o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica della Persona Autorizzata per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione alla Persona Autorizzata.
6. L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.
7. L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome della Persona Autorizzata, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.
8. Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente i dati personali della Persona Autorizzata relativi agli accessi internet e al traffico telematico.
9. L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dalla Persona Autorizzata all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.

10. Sarà cura della Persona Autorizzata la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
11. In ogni caso, l'Azienda garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:
    a. lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
    b. riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
    c. lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

8 CONTROLLI DA PARTE DELLA TITOLARITA'

1. Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali delle Persona Autorizzata e del presente Regolamento.
2. In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.
3. In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.
4. In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.
5. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

9 DATA BREACH

Nel caso in cui la Persona Autorizzata al trattamento venga a conoscenza di una violazione dei dati personali (c.d. Data Breach) deve provvedere ad informare senza ritardo il Servizio IT affinché possa notificare la violazione all'autorità di controllo competente, secondo quanto previsto dall'articolo 33 del GDPR.

10 RESPONSABILITÀ E SANZIONI

1. La Persona Autorizzata, al fine di non esporre sé stesso e l'Azienda a responsabilità nei confronti di terzi ed a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.
2. Le Persone Autorizzate sono responsabili del corretto utilizzo degli strumenti informatici, dei servizi Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio ed alla reputazione aziendale.
3. Tutte le Persone Autorizzate sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

a. per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;

b. per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.

11 AGGIORNAMENTI E PUBBLICAZIONE

Il presente regolamento verrà costantemente aggiornato per tener conto del modifiche normative e dell'evoluzione dei processi aziendali.

Dopo ogni modifica verrà pubblicato e reso disponibile nella intranet aziendale accessibile da ogni PC aziendale all'indirizzo internet http://intranet.mdr.lan.

Per Il Titolare del trattamento
Casa di Cura Madonna del Rimedio S.p.A.
Il delegato Dr. Luigi Pinto

Firmato digitalmente da
LUIGI PINTO
CN = PINTO LUIGI