ASL FROSINONE

REGIONE LAZIO
AZIENDA UNITA' SANITARIA LOCALE

REGIONE LAZIO

ATTO DELIBERATIVO N° 194 DEL 19/02/2020

ORIGINALE ☑ - COPIA ☐ - ALLEGATI N° ✓

Struttura Proponente: **Direzione Generale - U.O.C. Affari Generali, Contratti e Supporto all'Attività Legale** — 185 *(Proposta N°)* — 13.02.2020 *(Data)*

OGGETTO: Regolamento Aziendale Privacy e Protezione dei Dati Personali della ASL di Frosinone ai sensi del Regolamento (UE) 2016/679

L'estensore: Dott. Carlo Baldesi
(Nome e Cognome)

IL DIRETTORE GENERALE
(Dr. Stefano Lorusso)

Parere del Direttore Amministrativo
(Dr.ssa Pierpaola D'Alessandro)
☒ FAVOREVOLE ☐ NON FAVOREVOLE
(con motivazioni allegate al presente atto)
Data 13/02/2020 Firma

Parere del Direttore Sanitario
(Dr.ssa Patrizia Magrini)
☑ FAVOREVOLE ☐ NON FAVOREVOLE
(con motivazioni allegate al presente atto)
Data 14/2/20 Firma

Il Funzionario addetto al controllo di budget, con la sottoscrizione del presente atto, attesta che lo stesso non comporta scostamenti sfavorevoli rispetto al budget economico.

Voce del conto economico su cui si imputa la spesa: NON COMPORTA COSTI
(Descrizione)

Numero Conto Economico

Numero Sub autorizzazione_____

Visto del Funzionario addetto al controllo di budget Dr. Vincenzo Brusca
(Nome e Cognome) *(Firma)*

Data _____

Il Dirigente, con la sottoscrizione del presente atto, a seguito dell'istruttoria, attesta che l'atto é legittimo nella forma e nella sostanza ed é utile per il servizio pubblico.

Responsabile del Procedimento:
Dott. Carlo Baldesi — 13/2/2020 *(Data)* — *(Firma)*

IL DIRIGENTE
Dr.ssa Ornella Falivene — 13/2/2020 *(Data)* — *(Firma)*

IL DIRETTORE U.O.C. AFFARI GENERALI E SUPPORTO ALLE ATTIVITA' LEGALI

VISTA
la determinazione del Direttore affari generali con la quale si è preso atto della nomina del dottor Stefano Lorusso quale Direttore Generale dell'Azienda Sanitaria locale di Frosinone a decorrere dal 01.09.2019

PREMESSO
che in data 25 maggio 2018 è divenuto efficace il Regolamento UE 2016/679 recante disposizioni per la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

che il Decreto Legislativo n.101 del 10 agosto 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell'art.13 della legge di delegazione europea 2016-2017 (legge 25ottobre 2017, n.163) ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n.196/2003;

RITENUTO
necessario di procedere all'aggiornamento del Regolamento Aziendale sulla Privacy della ASL di Frosinone di cui all'atto deliberativo n. 838 del 22 luglio 2015, apportando integrazioni e modificazioni tenuto conto del Regolamento UE e della giurisprudenza del Garante per la protezione dei dati personali;

CHE
nell'opera di aggiornamento si è tenuto conto dei principi di semplificazione ed efficace integrando ed approfondendo i numerosi aspetti che riguardano il trattamento dei dati personali in sanità.

RAVVISATA
pertanto la necessità di procedere all'approvazione dell'aggiornamento del Regolamento Aziendale ai sensi del GDPR 2016/679 che allegato, al presente provvedimento ne costituisce parte integrante e sostanziale;

CONSIDERATO
che la Asl di Frosinone, è qualificabile come Titolare del Trattamento ai sensi dell'art. 4 del Regolamento UE 2016/679 e che nell'adempimento dei propri compiti istituzionali tratta dati personali, anche appartenenti a categorie particolari (dati sensibili) stabilendo finalità e modalità del trattamento.

PROPONE

1. di approvare il Regolamento Aziendale Privacy sull'utilizzo dei documenti sanitari, cartelle cliniche, archivi cartacei, strumenti e sistemi informatici contenenti dati personali e sensibili;
2. di trasmettere il presente provvedimento, per quanto di competenza ai tutti i Responsabili/Dirigenti UOC – UOS – UOSD - Unità Funzionali identificati altresì per la carica "Responsabili del Trattamento" con compiti di vigilanza sulla corretta applicazione delle procedure Aziendali Privacy che provvederanno, altresì, alla divulgazione massima ai propri dipendenti;
3. di disporre la pubblicazione del presente provvedimento sul Sito Internet Istituzionale e sul portale Intranet Aziendale alla voce "Ufficio Privacy".

IL DIRETTORE
U.O.C. AFFARI GENERALI E SUPPORTO
ALLE ATTIVITA' LEGALI
Dott.ssa Ornella Falivene

SISTEMA SANITARIO REGIONALE
ASL FROSINONE

REGIONE LAZIO

Regolamento Aziendale Privacy

sull'utilizzo dei documenti sanitari, cartelle cliniche, archivi cartacei, strumenti e sistemi informatici contenenti dati personali e sensibili.

ASL FROSINONE
Via A. Fabi, snc
03100 Frosinone

Tel. 0775.8821
www.asl.fr.it
P. Iva 01886690609

UFFICIO AZIENDALE PRIVACY
c/o Direzione Generale ASL Frosinone
Via A. Fabi, snc – 03100 FROSINONE
Tel. 0775 2072480
e.mail: carlo.baldesi@aslfrosinone.it

Indice

1 Obiettivo del Regolamento 3
2 Definizioni 3
3 Responsabilità e sanzioni 3
4 Principi generali 4
5 Documenti sanitari e cartelle cliniche 6
6 Archivi cartacei 6
6.1 Conservazione degli archivi cartacei 7
6.2 Accesso agli archivi cartacei 7
6.3 Misure di sicurezza per gli archivi cartacei 7
6.4 Invio dei documenti all'archivio storico 8
6.5 Procedura di gestione degli archivi 8
7 Strumenti e Sistemi informatici 8
7.1 Utilizzo dei computer - utilizzo dei social network - servizi di messaggistica 8
7.2 Utilizzo di applicativi aziendali, regionali o nazionali 9
7.3 Utilizzo della mail aziendale 10
7.4 Accesso ad apparecchi elettromedicali 11
7.5 Costruzione password 11
7.6 Videosorveglianza 11
8 Aggiornamenti e Revisioni 122

1 Obiettivo del Regolamento

Obiettivo del Regolamento è quello di definire le norme per le modalità di utilizzo dei documenti sanitari, delle cartelle cliniche, degli archivi cartacei, degli strumenti e sistemi informatici da parte di tutto il personale dipendente o esterno che svolge attività per la ASL Frosinone.
Le modalità di utilizzo sono definite in conformità ai requisiti del Regolamento UE 2016/679 "General Data Protection Regulation" (di seguito "GDPR"), di altre disposizioni nazionali in materia di protezione dei dati personali e delle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" emanate dall'Agenzia per l'Italia Digitale (di seguito "AgID").
Il presente Regolamento è approvato dal Titolare del Trattamento su proposta del Responsabile Aziendale Privacy Dott. Carlo Baldesi -Data Protection Officer ("DPO") della ASL Frosinone -

2 Definizioni

Titolare del Trattamento: il Titolare del Trattamento dei dati in ambito GDPR è la ASL Frosinone nella figura del Direttore Generale.
Data Protection Officer ("DPO"): è la persona nominata dal Titolare del Trattamento per il controllo dell'osservanza delle norme GDPR all'interno della ASL Frosinone.
Documento sanitario: qualsiasi documento cartaceo che contenga informazioni sullo stato di salute e dati personali di un paziente.
Cartella clinica: collezione di documenti sanitari e dati personali di un paziente.
Sistemi informatici: strumenti, servizi e applicazioni utilizzati dal personale della ASL Frosinone per l'espletamento del proprio lavoro.
Archivi cartacei: collezione di documenti sanitari di 2 o più pazienti conservati in ambienti gestiti dalla ASL Frosinone.

3 Responsabilità e sanzioni

Il Titolare del Trattamento è responsabile, coadiuvato dal DPO, della definizione delle norme, della sua divulgazione e della verifica dell'applicazione del Regolamento in tutte le strutture dell'ASL Frosinone, attraverso specifici piani di controllo
Ogni Responsabile di Unità Organizzativa della ASL Frosinone è responsabile della corretta e completa applicazione del Regolamento nella sua unità.
Tutto il personale dipendente della ASL Frosinone, compresi i collaboratori esterni, al fine di non esporre sé stessi e l'ASL Frosinone a rischi sanzionatori, sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente e ad osservare e fare osservare le norme contenute nel presente Regolamento.
Il mancato rispetto o la violazione delle norme contenute sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali previsti ex lege.
In particolare:

- per il personale dipendente, il mancato rispetto o la violazione delle regole potranno comportare, l'adozione di provvedimenti disciplinari previsti dal Contratto Collettivo Nazionale di Lavoro (C.C.N.L.), oltre alle azioni civili e penali previste *ex lege*

- per i collaboratori esterni, il mancato rispetto o la violazione delle regole potranno comportare la risoluzione del contratto, oltre alle azioni civili e penali previste *ex lege*

4 Principi generali

Con riferimento alle normative GDPR e AgID, le modalità di utilizzo dei documenti sanitari, delle cartelle cliniche, degli archivi cartacei, degli strumenti e sistemi informatici contenenti dati personali sono definite sulla base dei seguenti principi:

- La protezione dei dati personali detenuti dalla ASL Frosinone è definito obiettivo primario dell'azienda e di tutto il personale che svolge attività per l'azienda e deve garantire il rispetto dei seguenti obiettivi fondamentali:
  - Riservatezza: garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati
  - Integrità: garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico o nell'archivio cartaceo e sia stato modificato esclusivamente in modo legittimo
  - Disponibilità: garanzia di reperibilità di dati aziendali in funzione delle esigenze dei processi e nel rispetto delle norme che ne impongono la conservazione storica
- I dati personali di tipo medico o giudiziario sono considerati <u>sensibili</u> dalle normative GDPR, quindi per la maggior parte dei dati personali gestiti dalla ASL Frosinone si devono assicurare disposizioni di sicurezza aggiuntive per la protezione di questi dati
- L'utilizzo degli strumenti e dei sistemi informatici forniti dalla ASL Frosinone è consentito solo per scopi lavorativi e non personali
- L'accesso ai dati personali sia in modalità informatica che cartacea deve essere permesso al solo personale che ne ha necessità e deve essere limitato e circoscritto ai soli dati necessari all'esecuzione del lavoro assegnato dalla ASL Frosinone
- L'accesso ai dati personali deve poter essere monitorato, deve permettere il riconoscimento di attività non consone alla normativa GDPR e deve permettere l'individuazione del responsabile di tali attività
- Lo scambio, sia in modalità informatica che cartacea, di informazioni contenenti dati personali tra personale interno o esterno alla ASL Frosinone deve essere protetto da adeguate misure di sicurezza per prevenire accessi indesiderati alle informazioni
- Al personale interno ed esterno della ASL Frosinone è richiesto che si attenga alle disposizioni inserite in questo documento e in special modo:

- Procedere ai trattamenti dei dati e alla comunicazione e diffusione dei medesimi in modo lecito, secondo correttezza e nella misura necessaria e sufficiente alle finalità proprie dei compiti assegnati dal proprio responsabile diretto
- Adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, in questo o in altri documenti, da ASL Frosinone
- Segnalare al DPO della ASL Frosinone eventuali circostanze che rendano necessario o opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- prestare la più ampia e completa collaborazione ad ASL Frosinone al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente

Nello svolgimento delle proprie mansioni aziendali i dipendenti interni ed esterni di ASL Frosinone, compiono la propria attività sotto l'assoluto divieto di porre in essere o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle individuate dall'art. 24-bis del D.Lgs. 231/2001), nonché quanto previsto dal Regolamento UE 2016/679 e dal Decreto Legge 101 del 10 agosto 2018.

È fatto divieto, in particolare, di:

- Alterare documenti informatici e cartacei, pubblici o privati, aventi efficacia probatoria
- Accedere abusivamente al sistema informatico o telematico di ASL Frosinone e ai suoi archivi cartacei, al fine di alterare e/o cancellare dati e/o informazioni
- Detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti diversi da Asl Frosinone, pubblici o privati, al fine di acquisire informazioni riservate
- Detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate
- Svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate
- Svolgere attività di modifica e/o cancellazione di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità

5 Documenti sanitari e cartelle cliniche

La gestione dei documenti sanitari e delle cartelle cliniche da parte del personale della ASL Frosinone deve garantire che:

- Ogni documento sanitario sia conservato integro e a disposizione del personale sanitario per il tempo necessario al suo utilizzo e poi riposto in una cartella clinica.
- Ogni cartella clinica sia conservata nella sua interezza e a disposizione del personale per il tempo necessario al suo utilizzo e poi riposto in un archivio cartaceo.
- L'accesso ai documenti sanitari e alle cartelle cliniche sia riservato al personale della ASL Frosinone o a persone debitamente autorizzate al solo scopo di tutelare la salute del paziente.
- Il paziente, o persona da lui debitamente autorizzata, possa accedere ai propri documenti sanitari durante o successivamente la propria degenza.

Di conseguenza nella gestione dei documenti sanitari e delle cartelle cliniche, il personale dell'ASL di Frosinone si deve attenere alle seguenti norme di comportamento:

- È fatto divieto di lasciare incustoditi note-disposizioni Aziendali, documenti sanitari e cartelle cliniche in ambienti accessibili da soggetti non appartenenti al personale della ASL Frosinone.
- Non consentire a soggetti non appartenenti al personale della ASL Frosinone di accedere ai luoghi di lavoro dove vengono custoditi i dati sensibili e personali (anche di dipendenti), documenti sanitari e le cartelle cliniche; nel caso questo non sia possibile per l'espletamento dei servizi offerti dall'ASL Frosinone ai pazienti, è fatto obbligo di impedire la consultazione a tali soggetti posizionando i documenti sanitari e le cartelle cliniche in cassetti o armadi chiusi a chiave.
- Non consentire agli accompagnatori dei pazienti, se non dallo stesso debitamente autorizzati, di accedere ai documenti sanitari e alle cartelle cliniche.
- Non consentire ai Volontari delle Associazioni operanti all'interno delle strutture della ASL Frosinone di accedere ai documenti sanitari e alle cartelle cliniche, limitando la loro presenza alle aree loro destinate e per le sole finalità definite nel protocollo d'intesa.

Ogni comportamento che violi le norme esposte, deve essere immediatamente segnalato al Responsabile della Unità Organizzativa che eroga il servizio in cui vi è stata la violazione.

6 Archivi cartacei

La ASL Frosinone gestisce un elevato numero di archivi cartacei, alcuni centralizzati in Direzione Sanitaria (in particolare le cartelle cliniche dei reparti ospedalieri e dei Pronto Soccorsi), ma in larga misura gestiti dalle singole Unità Organizzative. Nella maggior parte dei casi i dati personali gestiti dalla ASL Frosinone sono

identificati come sensibili e necessitano di una gestione accurata per la prevenzione di accessi indesiderati a tali dati.
Presso la Direzione Sanitaria e le Unità Organizzative sono conservate le informazioni più recenti mentre quelle storiche sono archiviate presso un'apposita società di gestione degli archivi storici.

6.1 Conservazione degli archivi cartacei

La conservazione degli archivi cartacei riguardanti i pazienti che hanno avuto accesso ai servizi della ASL Frosinone o del personale dipendente della stessa azienda, deve essere organizzata tenendo presenti i seguenti obiettivi:

- Conservazione e reperimento delle informazioni necessarie alle attività della ASL Frosinone
- Rispetto dei termini di legge per la conservazione delle informazioni
- Protezione degli archivi da accessi indesiderati di persone non addette alle attività della ASL Frosinone, in particolare per i dati personali sensibili

6.2 Accesso agli archivi cartacei

L'accesso agli archivi cartacei contenenti dati personali deve soddisfare le seguenti norme:

- L'accesso all'archivio cartaceo di una Unità Organizzativa è consentito solo al personale della stessa unità ed è responsabilità della Unità Organizzativa che le persone che vi accedono ne abbiano titolarità.
- Nel caso di prelievo di uno o più documenti da parte del personale dell'Unità Organizzativa per svolgere la propria attività, la conservazione e protezione di questi documenti è di responsabilità del prelevante che li deve restituire alla fine dell'attività lavorativa per cui li aveva prelevati.
- Nel caso di prelievo di uno o più documenti da parte di personale esterno all'Unità Organizzativa che li conserva il prelevante è responsabile della corretta conservazione e protezione dei documenti fino alla loro restituzione.
- I documenti prelevati non possono rimanere incustoditi (ad esempio su scrivanie o tavoli non presidiati) e devono essere riposti in armadi o cassetti o stanze chiuse a chiave oppure restituiti all'archivio da cui si erano prelevati.

6.3 Misure di sicurezza per gli archivi cartacei

Le misure di sicurezza degli archivi cartacei contenenti dati personali devono assicurare l'accesso ai documenti conservati al solo personale che ne ha necessità per svolgere la propria attività, quindi le misure di sicurezza adottate dalla Direzione Sanitaria e da ogni singola Unità Organizzativa che gestisce uno o più archivi cartacei, devono soddisfare le seguenti norme:

- I documenti devono essere conservati in appositi armadi e cassettiere chiuse a chiave o in stanze chiuse a chiave
- Le chiavi, in particolare per gli archivi che conservano dati personali sensibili, devono essere di sicurezza e deve essere gestito un registro delle copie e dei possessori di tali copie
- Gli armadi e le stanze a protezione di archivi cartacei contenenti dati personali, possono rimanere aperte solo in presenza di personale dell'Unità Organizzativa che gestisce l'archivio e che ne

garantisca la protezione; non è permesso lasciare incustoditi armadi o stanze aperte, anche per breve tempo

- Le chiavi di armadi e stanze a protezione di archivi cartacei contenenti dati personali, non possono essere lasciate incustodite (ad esempio appese al muro o lasciate su una scrivania o tavolo) ma devono essere sempre custodite da personale dell'Unità Organizzativa o riposte in armadi o cassetti chiusi a chiave

6.4 Invio dei documenti all'archivio storico

L'invio dei documenti di un archivio cartaceo all'archivio storico gestito da un fornitore esterno è sotto la responsabilità dell'Unità Organizzativa proprietaria dell'archivio cartaceo e deve soddisfare le seguenti norme:

- L'invio deve garantire la sicurezza dei dati personali
- I documenti devono essere catalogati in modo da essere reperibili per i tempi di conservazione previsti
- I tempi di conservazione di ciascuna tipologia di documenti devono essere indicati al fornitore, terminati i quali il fornitore deve procedere alla distruzione dei documenti

6.5 Procedura di gestione degli archivi

Per una corretta gestione degli archivi cartacei ciascun Responsabile di Unità Organizzativa deve vigilare sulla corretta gestione degli archivi ed informare il personale dell'unità circa:

- Tipologia dei dati personali gestiti.
- Localizzazione dell'archivio (stanza, armadio, cassettiera) e modalità di sicurezza da adottare per impedire l'accesso indesiderato ai documenti, la loro alterazione o il loro smarrimento.
- Gestione delle chiavi e modalità di assegnazione delle stesse ed indicazione delle persone assegnatarie.
- Modalità di accesso ai documenti dell'archivio e di riconsegna degli stessi; nel caso di consegna a personale esterno all'Unità Organizzativa, si devono indicare le modalità di utilizzo, di consegna e restituzione dei documenti.

7 Strumenti e Sistemi informatici

La ASL Frosinone fornisce al proprio personale interno ed esterno l'accesso a strumenti e sistemi informatici quali computer, mail e applicativi della ASL, regionali e nazionali. L'utilizzo di tali strumenti e sistemi deve garantire i principi generali indicati di seguito.

7.1 Utilizzo dei computer

L'utilizzo dei computer aziendali deve soddisfare le seguenti norme:

- L'utilizzo dei computer è consentito solo per scopi lavorativi e non personali e devono essere rispettate le seguenti indicazioni:
    - Le configurazioni hardware delle risorse assegnate in uso non possono essere modificate autonomamente
    - Non possono essere installati software sul computer senza l'assenso del Dipartimento ICT e senza il possesso della regolare licenza d'uso
    - È tassativamente vietato l'impiego di programmi a scopo di intrusione ed intercettazione di dati (ad esempio sniffer, keylogger, "malicious" software in genere)
- La userid e la password di accesso al dominio ASL Frosinone è strettamente personale e non può essere ceduta ad altri, anche colleghi o superiori
- La password utilizzata deve essere mantenuta riservata e quindi non può essere memorizzata su supporti non protetti (ad esempio sui post-it); se si ritiene necessario memorizzare la password, questa deve essere conservata in ambiente sicuro protetto da una chiave a sola disposizione della persona che l'ha memorizzata
- Eventuali file contenenti dati personali devono essere conservati in cartelle accessibili solo tramite password di dominio (ad es. nella cartella "Documenti")
- Eventuali file contenenti dati personali sensibili devono essere conservati in cartelle accessibili solo tramite password di dominio (ad es. nella cartella "Documenti") e protetti da ulteriore password propria del particolare programma con cui il file è stato creato o di un programma di compressione
- Quando il computer in cui è stata inserita la propria password di dominio viene lasciato incustodito, anche per breve tempo, è necessario attivare lo screen saver o lo spegnimento per impedire accessi indesiderati
- È vietato copiare su dispositivi esterni personali, dati la cui titolarità è della ASL Frosinone

Utilizzo dei Social network e messaggistica;

L'utilizzo dei social network e messaggistica (Whatsapp, Telegram...) da parte dei dipendenti (o collaboratori) della ASL Frosinone deve sottostare alle seguenti linee comportamentali:

- Salvo il diritto di esprimere valutazioni e diffondere informazioni a tutela dei diritti sindacali, ben rappresentando questo tipo di opinione, il dipendente si deve astenere da dichiarazioni pubbliche offensive nei confronti dell'amministrazione, e deve osservare il segreto di ufficio e la normativa ai sensi della privacy;
- Nel caso in cui si riportano fatti e circostanze, è necessario: riportare dati obiettivi e di dominio pubblico; evitare di pubblicare notizie o fatti di dubbia veridicità e di fonte ignota; evitare la pubblicazione di foto di locali aziendali e ambienti di lavoro e, in particolare, di dati che potrebbero essere interessati a vincoli di riservatezza e confidenzialità (per esempio: email, circolari, ecc);

- Si deve evitare la diffusione, in qualsiasi forma e attraverso qualunque media e social media, di informazioni riservate e informazioni identificative personali di cui ne sia venuti a conoscenza con il proprio lavoro o di informazioni confidenziali provenienti dall'attività clinica e assistenziale;
- Si deve rispettare il diritto alla privacy dei pazienti, utenti dei servizi e colleghi evitando di postare foto, immagini o descrizioni che non siano preventivamente autorizzate per iscritto dagli stessi pazienti, utenti dei servizi e colleghi.;

7.2 Utilizzo di applicativi aziendali, regionali o nazionali

L'utilizzo di applicativi aziendali, regionali o nazionali deve soddisfare le seguenti norme:

- L'utilizzo degli applicativi è consentito solo per scopi lavorativi e non personali
- La userid e la password di accesso agli applicativi è strettamente personale e non può essere ceduta ad altri, anche colleghi o superiori
- La password utilizzata deve essere mantenuta riservata e quindi non può essere memorizzata su supporti non protetti (ad esempio sui post-it); se si ritiene necessario memorizzare la password, questa deve essere conservata in ambiente sicuro protetto da una chiave a sola disposizione della persona che l'ha memorizzata
- Quando il computer su cui è stato effettuato l'accesso all'applicativo viene lasciato incustodito, anche per breve tempo, è necessario effettuare la chiusura dell'applicativo per impedire accessi indesiderati
- Lo scarico di dati personali dagli applicativi e la sua memorizzazione su computer o l'invio tramite mail deve essere protetto
- Non è permesso copiare su dispositivi esterni personali dati la cui titolarità è dell'ente proprietario dell'applicativo (ASL Frosinone, Regione Lazio, Stato Italiano)
- La stampa di dati personali dagli applicativi deve essere effettuata su stampanti in locali protetti, deve essere recuperata al più presto e deve essere conservata in appositi archivi cartacei protetti o distrutta dopo il suo utilizzo

7.3 Utilizzo della mail aziendale

L'utilizzo della mail aziendale deve soddisfare le seguenti norme:

- L'utilizzo della mail aziendale è consentito solo per scopi lavorativi.
- La userid e la password di accesso alla mail aziendale è strettamente personale e non può essere ceduta ad altri, anche colleghi o superiori.
- La password utilizzata deve essere mantenuta riservata e quindi non può essere memorizzata su supporti non protetti (ad esempio sui post-it); se si ritiene necessario memorizzare la password, questa deve essere conservata in ambiente sicuro protetto da una chiave a sola disposizione della persona che l'ha memorizzata

7.4 Accesso ad apparecchi elettromedicali

La ASL Frosinone per erogare i propri servizi ai cittadini utilizza un gran numero di apparecchi elettromedicali che possono memorizzare dati personali dei pazienti insieme a dati di tipo medico.
L'accesso a tali apparecchi, nel caso sia prevista una password di acceso, può avvenire tramite password propria dell'apparecchio o tramite password assegnata a ciascun operatore dell'apparecchio. Inoltre gli apparecchi possono prevedere una funzionalità di cambio operatore o di richiesta di reintroduzione password. Nel caso tali funzionalità non siano presenti, queste si possono simulare spegnendo e riaccendendo gli apparecchi, però solo per gli apparecchi in cui tale processo non pregiudichi la corretta funzionalità degli stessi.
Le misure di sicurezza per la gestione degli apparecchi contenenti dati personali associati a dati medici, dipendono dalla tipologia di password presente:

- Apparecchio senza password: l'apparecchio non può essere lasciato incustodito in ambienti accessibili da persone che non sono gli utilizzatori dello stesso; quindi quando non utilizzato, l'apparecchio deve essere riposto in una stanza accessibile solo agli utilizzatori dello stesso
- Apparecchio con unica password: quando l'apparecchio viene lasciato incustodito deve essere attivata la funzionalità di reintroduzione della password o, se questa non è presente, l'apparecchio deve essere spento; nel caso di apparecchio che non è possibile spegnere per non compromettere la funzionalità dello stesso, l'apparecchio deve essere riposto in una stanza accessibile solo agli utilizzatori dello stesso
- Apparecchio con password per ogni operatore: quando l'apparecchio viene lasciato incustodito o è terminata l'attività di uno specifico operatore, deve essere attivata la funzionalità di reintroduzione della password o, se questa non è presente, l'apparecchio deve essere spento; nel caso di apparecchio che non è possibile spegnere per non compromettere la funzionalità dello stesso, l'apparecchio deve essere riposto in una stanza accessibile solo agli utilizzatori dello stesso

Le password di accesso agli apparecchi non possono essere fornite a persone che non sono utilizzatori dello specifico apparecchio. Inoltre non è permesso copiare su dispositivi esterni personali, dati dall'apparecchio la cui titolarità è dell'ASL Frosinone.

7.5 Costruzione password

Per la costruzione di password personali gestite dagli utenti, si devono utilizzare le seguenti indicazioni:

- La password deve avere minimo 8 caratteri e contenere almeno tre di questi elementi: una lettera minuscola, una lettera maiuscola, una cifra e un carattere speciale ($, £, %, ecc.)
- La password non deve contenere vocaboli compresi nei dizionari di lingua italiana, frasi comuni, né essere in alcun modo collegata alla vita privata; non deve essere usato il nome o il cognome proprio o di parenti, la targa dell'auto, la data di nascita, la città di residenza, il proprio account (user-id)
- Ogni nuova password deve essere diversa dalle ultime utilizzate in passato

7.6 Videosorveglianza

L'Azienda effettua attività di videosorveglianza esclusivamente per lo svolgimento delle proprie funzioni istituzionali ovvero:

1. per garantire la sicurezza del patrimonio aziendale e delle persone che, a vario titolo, frequentano gli ambienti delle strutture aziendali o che accedono agli stessi;
2. per il perseguimento di finalità di cura delle persone che si avvalgono delle prestazioni erogate dall'Azienda (c.d. videocontrollo per monitoraggio pazienti).

Il Titolare del Trattamento dei dati raccolti con i sistemi di videosorveglianza è l'Azienda Unità Sanitaria Locale di Frosinone, nella persona del suo rappresentante legale pro-tempore.
Il Responsabile-Incaricato del trattamento dei dati raccolti con i sistemi di videosorveglianza è il Security Manager Tonino Perruzza.

8 Aggiornamenti e Revisioni

Il presente Regolamento è soggetto ad aggiornamento e/o revisione con frequenza annuale.
Il DPO, in quanto figura deputata anche all'aggiornamento della documentazione interna in materia di privacy, verifica costantemente la complessiva idoneità delle norme predisposte al fine di assicurare il conseguimento degli obiettivi posti dalla disciplina vigente in materia, tenendo conto, in particolare, delle modifiche eventualmente intervenute nella normativa di riferimento, negli assetti organizzativi del Titolare nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.
Tutto il personale della ALS Frosinone può, inoltre, proporre, se ritenuto necessario, integrazioni o specificazioni al presente documento. Le proposte verranno esaminate dal Titolare del trattamento, con la consulenza del DPO.

Il Responsabile Aziendale Privacy
DPO Dott. Carlo Baldesi

IL DIRETTORE GENERALE

- Vista la relazione-proposta che precede;
- Visti i pareri del Direttore Amministrativo e del Direttore Sanitario;
- Visto il Parere del Funzionario addetto al controllo di budget;
- Visto il parere del Dirigente e/o Responsabile del Procedimento attestante che l'atto è legittimo nella forma e nella sostanza ed è utile per il servizio pubblico;

D E L I B E R A

di approvare la proposta così come formulata rendendola disposto.

IL DIRETTORE GENERALE
Dott. Stefano Corusso

IL DIRETTORE U.O.C. AFFARI GENERALI, CONTRATTI E SUPPORTO ALL'ATTIVITA' LEGALE

ATTESTA CHE

La deliberazione è pubblicata all'Albo Pretorio nell'elenco N° 194 del 19/02/2020

- È stata trasmessa al Collegio Sindacale il 19/02/20 prot. n° 28
- È pubblicata all'albo Pretorio dal 19/02/2020 al 05/03/2020
- È esecutiva dalla data di adozione.

IL DIRETTORE
Dott.ssa Ornella Falivene