ATTO DI NOMINA
A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI
(ai sensi dell'art. 29 del D.Lgs. 30 giugno 2003, n. 196 e dell'art. 28 del Regolamento UE 2016/679)

TRA

L'**ASL ROMA 2**, quale Titolare del Trattamento, in persona del Legale Rappresentante *pro-tempore*, Direttore Generale, Dott.ssa Flori Degrassi (di seguito, per brevità "**Titolare**");

E

_____, quale *Responsabile Esterno del Trattamento* (di seguito, per brevità, "**Responsabile**"),

Di seguito, congiuntamente, le "**Parti**".

PREMESSO CHE
(Le premesse formano parte integrante e sostanziale del presente Atto)

- Tra la ASL Roma 2 e _____ è in atto una Convenzione/Contratto attinente a _____
- Con deliberazione n 784/Cs/2016 il Direttore Amministrativo, Dott.ssa Silvia Cavalli è stata delegata dal Legale Rappresentante *pro-tempore* Asl Roma 2 alla sottoscrizione degli Atti di nomina a Responsabile esterno ai sensi e per gli effetti 29 del D.Lgs. 30 giugno 2003, n. 196 e dell'art. 28 del Regolamento UE 2016/679);
- per l'esecuzione delle attività svolte a favore dell'ASL Roma 2, il Responsabile tratterà dati personali di cui l'ASL Roma 2 è Titolare;
- l'ASL Roma 2, in persona del legale rappresentante *p.t.*, Titolare del trattamento dei dati personali ai sensi degli artt. 4 e 28 del D. Lgs. 196/2003 e s.m.i. e degli artt. 4 e 24 del Regolamento UE 2016/679, ha pertanto individuato, _____, quale Responsabile Esterno del Trattamento sulla base delle evidenze documentali ovvero delle dichiarazioni dallo stesso fornite al Titolare e della successiva verifica da parte del Titolare medesimo, per quanto ragionevolmente possibile, della loro rispondenza al vero, circa le caratteristiche di esperienza, capacità e affidabilità che vengono richieste dalla norma per chi esercita tale funzione affinché il trattamento rispetti i requisiti della normativa e garantisca la tutela degli interessati.

SI CONCORDA E SI STIPULA QUANTO SEGUE:

Art. 1
Definizioni

Ai fini del presente Atto di nomina valgono le seguenti definizioni:

- Per **"Legge Applicabile"** o **"Normativa Privacy",** si intende 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 (di seguito, per brevità, "***GDPR***") a far data dal 25.05.2018, il D.Lgs. 196/2003 e s.m.i. e i suoi allegati (di seguito, per brevità, anche "**Codice della Privacy**"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, anche emanata ai sensi dell'art. 13 della Legge

n. 163 del 25 ottobre 2017, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali (di seguito, per brevità, "**Garante**");

- per **"Dati Personali"**: si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 comma 1 lett. b) del Codice della Privacy e dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi di cui alla Convenzione/Contratto stipulata/o con l'Azienda;
- per "**Interessato**": si intende la persona fisica cui si riferiscono i Dati Personali;
- per **"Servizi"**: si intendono i Servizi resi dal Responsabile oggetto della Convenzione/Contratto nonché il relativo trattamento dei dati personali, così come meglio descritto nel presente Atto di nomina e nei suoi allegati;
- per "**Titolare**": si intende, ai sensi dell'art. 4 comma 1 lett. f) del Codice della Privacy, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza e, ai sensi dell'art. 4, par. 7 del GDPR, 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;
- per **"Responsabile del Trattamento"**: si intende, ai sensi dell'art. 4 comma 1 lett. g) del Codice della Privacy, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali e, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- per **"Ulteriore Responsabile"**: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte dei Servizi e che quindi tratta dati personali;
- per **"Misure di Sicurezza"**: si intendono le misure di sicurezza di cui alla Normativa privacy;
- per "**Trattamento**": si intende, ai sensi dell'art. 4 comma 1 lett. a) del Codice della Privacy, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati e, ai sensi dell'art. 4, par. 2 del GDPR, 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.

Art. 2
Nomina e oggetto

In attuazione degli art. 29 del Codice della Privacy e dell'art. 28 del GDPR, l'ASL Roma 2, in qualità di Titolare del trattamento, nomina il soggetto indicato in premessa, quale Responsabile per il Trattamento dei Dati Personali reso necessario per l'espletamento dei Servizi.

Il Responsabile tratterà i Dati Personali di cui verrà in possesso/a conoscenza nello svolgimento dei Servizi oggetto della Convenzione/Contratto solo in base a quanto ivi stabilito e a quanto previsto nel presente Atto e nel suo Allegato che ne forma parte inscindibile.

Art. 3
Durata e finalità

Il presente Atto produce i suoi effetti a partire dalla data di sottoscrizione delle Parti e rimarrà in vigore fino alla cessazione delle attività svolte dal Responsabile a favore del Titolare, indipendentemente dalla causa di detta cessazione. Inoltre, fermo il diritto del Titolare di revocare, in qualsiasi momento e senza bisogno di motivazione, l'affidamento del Trattamento al Responsabile e/o la sua stessa nomina, il Trattamento, fatto salvo ogni eventuale obbligo di legge, avrà una durata non superiore a quella necessaria al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Art. 4
Modalità e istruzioni

Le modalità e le istruzioni per il Trattamento dei Dati Personali impartite dal Titolare al Responsabile sono specificatamente indicate e declinate nella Convenzione/Contratto, nella presente nomina e nel suo ***Allegato 1*** "*Compiti ed istruzioni per i Responsabili del trattamento dei dati personali*".

Art. *5*
Obblighi e doveri del Responsabile del trattamento

Il Responsabile, al momento della sottoscrizione del presente Atto, dichiara e garantisce di avere una struttura ed una organizzazione adeguata per l'esecuzione dei Servizi e si impegna ad adeguarla ovvero a mantenerla adeguata alla delicatezza della nomina, garantendo il pieno rispetto (per sé e per i propri dipendenti e collaboratori interni ed esterni) delle istruzioni sul trattamento dei dati personali specificatamente indicate e declinate nella Convenzione/Contratto e nel documento di cui al sopra citato ***Allegato 1*** alla presente nomina, oltre che della Normativa Privacy.

Art.6
Tipologie di dati, finalità e Categorie di interessati

Il Responsabile svolge per conto del Titolare le attività di Trattamento dei Dati Personali relativamente alle tipologie, alle finalità ed alle categorie di soggetti esplicitate nella Convenzione/Contratto, presupposto inscindibile del presente Atto di nomina.

Art.7
Nomina di ulteriori responsabili

In esecuzione e nell'ambito dei Servizi, il Responsabile, ai sensi dell'art. 28 comma 2 del GDPR, è autorizzato, salva diversa comunicazione scritta del Titolare, a ricorrere alla nomina di Ulteriori Responsabili ad esso subordinati, previo esperimento delle necessarie procedure di selezione dei fornitori applicabili di volta in volta.

Il Responsabile sarà tenuto, in sede di individuazione degli eventuali Ulteriori Responsabili e/o della loro sostituzione, ad informare preventivamente il Titolare, al fine di consentire a quest'ultimo, in attuazione dell'art. 28 comma 2 summenzionato, di poter manifestare eventuale formale opposizione alla nomina entro e non oltre il congruo termine di 20 (venti) giorni dalla ricezione della comunicazione. Decorso detto termine, il Responsabile potrà procedere all'effettuazione delle nomine, normativamente previste, nei confronti degli Ulteriori Responsabili individuati.

La nomina di un Ulteriore Responsabile da parte del Responsabile sarà possibile a condizione che sull'Ulteriore Responsabile siano imposti , mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalla Normativa Privacy.

Qualora l'Ulteriore Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'Ulteriore Responsabile.

Il Responsabile, infine, si obbliga a comunicare al Titolare, con cadenza annuale, eventuali modifiche ed aggiornamenti dei trattamenti di competenza dei propri Ulteriori Responsabili.

Art.8
Vigilanza, sanzioni e responsabilità

Ai sensi e per gli effetti dell'art. 29, comma 5 del Codice della Privacy e dall'art. 28, comma 3 del *GDPR*, al fine di vigilare sulla puntuale osservanza della Legge Applicabile e delle istruzioni impartite al Responsabile, il Titolare, anche tramite il proprio Responsabile della Protezione Dati e/o altro soggetto allo scopo individuato, potrà effettuare periodiche azioni di verifica. Tali verifiche, che potranno anche comportare l'accesso a locali o macchine e programmi del Responsabile Esterno, potranno aver luogo a seguito di comunicazione da parte del Titolare, da inviare con un preavviso di almeno cinque giorni lavorativi. Nell'ambito di tali verifiche, il Responsabile fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste del Titolare, in relazione ai dati e ai trattamenti rispetto ai quali ha valore il presente atto di nomina.

Le Parti del presente Atto sono soggette, a cura dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo - anche in relazione a quanto previsto dal Contratto/Convenzione di riferimento - all'applicazione di penali e/o alla risoluzione del Contratto o della Convenzione.

Il Responsabile assume piena responsabilità diretta verso gli Interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del titolare.

Il Responsabile si obbliga a manlevare il Titolare e tenere quest'ultimo indenne da qualsiasi tipo di conseguenza, sia civile che amministrativa, responsabilità, perdita, onere, spesa, danno o costo da quest'ultimo sopportato che sia la conseguenza di comportamenti a attribuibili al Responsabile,

ASL Roma 2 P.Iva 13665151000
Sede Legale Via Filippo Meda 35 00157 Roma
Sede Operativa Via Primo Carnera 1 00142 Roma

ovvero di violazioni agli obblighi o adempimenti prescritti dalla Normativa Privacy ovvero di inadempimento delle pattuizioni contenute nel presente Atto di nomina, ovvero dei compiti assegnati dal Titolare.

Art. 9
Disposizioni Finali

Il presente Atto di nomina, comprensivo del suo Allegato 1, deve intendersi quale contratto formale, anche in formato elettronico, che lega il Responsabile al Titolare del trattamento e che contiene espressamente le Istruzioni documentate del Titolare, le modalità di gestione dei dati, la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento, così come le responsabilità in ambito privacy.

Con la sottoscrizione, il Responsabile accetta la nomina e si dichiara disponibile e competente alla piena attuazione di quanto nella stessa previsto.

La presente nomina ha carattere gratuito ed ha durata pari alla durata del Contratto/Convenzione a cui accede o, comunque, dell'atto giuridicamente vincolante che ne forma presupposto indefettibile e, fermo quanto indicato al precedente art. 3, si intenderà, pertanto, revocata al venir meno dello stesso, indipendentemente dalla causa.

Una copia della presente nomina, debitamente timbrata e sottoscritta in originale, dovrà essere trasmessa/consegnata all' UOC Affari Generali- Ufficio Privacy Asl Roma 2 presso la sede legale della ASL Roma 2, Via Filippo Meda, n. 35- 00167 Roma.

Si allega: ***Allegato 1*** "*Compiti ed istruzioni per i Responsabili del trattamento dei dati personali*".

Roma lì_____

LETTO CONFERMATO E SOTTOSCRITTO

Il Responsabile Esterno

_____

Su delega del Titolare del trattamento
ASL ROMA 2

Il Direttore Amministrativo
Dott.ssa Silvia Cavalli
(giusta delibera n 784/Cs del 23/06/2016)

_____

Allegato 1
"COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI"

ASL ROMA 2	PRIVACY ASL ROMA 2	Revisione n. 1 01/2018	REGIONE LAZIO

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

(Allegato 1 alla nomina)

Indice

Ambito

Il presente documento si inquadra nell'ambito delle Misure di Sicurezza, previste dagli artt. 31 e ss. del D.Lgs. 196/2003 e s.m.i. e dal suo allegato (B in relazione alle misure minime di sicurezza (*infra*, complessivamente, detto "**Codice della Privacy**"), nonché, a far data dal 25.05.2018, all'atto della sua definitiva esecutività, ai principi contenuti nell'art. 32 del Regolamento 2016/679/UE (*infra* detto "**GDPR**"), applicabili alla Azienda Sanitaria Locale Roma 2.
Si rammenta che, ai sensi del GDPR, le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento e che, in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva.
Inoltre, pur non potendo sussistere, dopo il 25 maggio 2018, obblighi generalizzati di adozione di misure "*minime*" di sicurezza (ex art. 33 Codice della Privacy), si ritiene, allo scopo di assicurare un livello minimo di protezione dei dati personali, che le misure di cui agli artt. 34 e 35 del Codice della Privacy come meglio precisate nell'allegato B, debbano in ogni caso essere garantite in riferimento a qualsiasi trattamento di dati personali di cui la ASL Roma 2 sia titolare.
Si rammenta, infine, che, su indicazione del Garante, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del GDPR) possono restare in vigore le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice della Privacy), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.
Con la sottoscrizione della nomina, il Responsabile la accetta e si dichiara disponibile e competente alla piena attuazione di quanto nella stessa previsto. Il Responsabile dichiara, inoltre, di conoscere quanto previsto dal GDPR, impegnandosi sin d'ora ad applicarlo integralmente, senza bisogno di alcuna richiesta da parte del Titolare, al momento della sua definitiva vigenza.

Scopo e campo di applicazione

Il presente documento ha l'obiettivo di specificare le istruzioni operative a cui si devono attenere i Responsabili del trattamento dei dati personali della ASL Roma 2 (*infra* detti "**Responsabile**" o "**Responsabili**"), in conformità con la normativa vigente in materia di trattamento dei Dati Personali e con la nomina in tal senso ricevuta dalla ASL Roma 2 in qualità di titolare del trattamento (*infra* detto "**Titolare**") di cui costituisce parte integrante e inscindibile.

Si precisa, comunque, che nel rispetto delle norme e delle istruzioni in tal senso fornite dal Titolare, possono essere eseguite dai Responsabili attività in autonomia purché non comportino una diminuzione del livello generale e specifico di sicurezza né la modifica delle finalità dei trattamenti loro affidati.

L'ASL Roma 2, tramite verifiche periodiche affidate al proprio Responsabile per la Protezione dei Dati (*infra* detto "**Dpo**") e/o altro soggetto allo scopo individuato, effettuerà i controlli che riterrà opportuni per vigilare sulla puntuale osservanza della normativa vigente, della nomina e delle presenti istruzioni operative.

Documenti di riferimento

Costituiscono riferimento imprescindibile per questo documento:

- Il D.Lgs. 196/2003 e s.m.i. e i suoi allegati
- Il Regolamento 2016/679/UE
- Ogni altra normativa nazionale e/o dell'Unione Europea rilevante in materia di tutela della riservatezza e dei dati personali
- I provvedimenti generali e particolari, le linee guida e le autorizzazioni generali emanate dall'Autorità Garante per la protezione dei dati personali e/o dal Gruppo dei Garanti Europei della privacy
- La procedura informatica aziendale
- Il regolamento aziendale sulla privacy
- La delibera n. 1791 - Procedura aziendale in materia di *data breach* per la gestione delle violazioni di dati personali, ai sensi e per gli effetti degli artt. 33 e 34 del regolamento europeo 679-2016.

Definizioni

Ai fini del presente documento, richiamate quelle in tal senso presenti nella nomina, si intendono applicabili, secondo ragione, le definizioni riportate all'art. 4 del Codice della Privacy e all'art. 4 del GDPR cui espressamente si rimanda ricordando, in particolare, che:

- per **"Legge Applicabile"** o **"Normativa Privacy"**, si intende 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 a far data dal 25.05.2018, il D.Lgs. 196/2003 e s.m.i. e i suoi allegati, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, anche emanata ai sensi dell'art. 13 della Legge n. 163 del 25 ottobre 2017, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali (**"Garante"**);
- per **"Dati Personali"**: si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 comma 1 lett. b) del Codice della Privacy e dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi di cui alla Convenzione/Contratto stipulata/o con l'Azienda;
- per **"Interessato"**: si intende la persona fisica cui si riferiscono i Dati Personali;
- per **"Servizi"**: si intendono i Servizi resi dal Responsabile oggetto della Convenzione/Contratto nonché il relativo trattamento dei dati personali, così come meglio descritto nel presente Atto di nomina e nei suoi allegati;
- per **"Titolare"**: si intende, ai sensi dell'art. 4 comma 1 lett. f) del Codice della Privacy, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza e, ai sensi dell'art. 4, par. 7 del GDPR, 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;
- per **"Responsabile del Trattamento"**: si intende, ai sensi dell'art. 4 comma 1 lett. g) del Codice della Privacy, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro

ente, associazione od organismo preposti dal titolare al trattamento di dati personali e, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

- per **"Ulteriore Responsabile"**: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte dei Servizi e che quindi tratta dati personali;
- per **"Incaricato"** o **"Persona autorizzata al trattamento"**: si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- per **"Amministratore di sistema"** o **"ADS"**: si intende la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi *software* complessi quali i sistemi ERP (*Enterprise resource planning*) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- per **"Misure di Sicurezza"**: si intendono le misure di sicurezza di cui alla Normativa privacy;
- per **"Trattamento"**: si intende, ai sensi dell'art. 4 comma 1 lett. a) del Codice della Privacy, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati e, ai sensi dell'art. 4, par. 2 del GDPR, 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.

Principi generali da osservare

Ogni trattamento di dati personali affidato al Responsabile e ad ogni eventuale Ulteriore Responsabile deve essere svolto nel rispetto dei principi di ordine generale_come contemplati dall'art. 11 del Codice della privacy (*"Modalità del trattamento e requisiti dei dati"*) nonché dell'art. 5 del GDPR (*"Principi applicabili al trattamento di dati personali"*) e, dunque, per ciascun trattamento di propria competenza, questi deve fare in modo che siano sempre rispettati i seguenti presupposti:

I dati devono essere trattati:

- ✓ secondo il principio di liceità, vale a dire conformemente alle disposizioni della Normativa Privacy, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- ✓ secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

i dati devono essere raccolti solo per scopi:

- ✓ determinati, vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- ✓ espliciti, nel senso che il soggetto interessato va sempre informato sulle finalità e modalità del trattamento;
- ✓ legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
- ✓ compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

i dati devono, inoltre, essere:

- ✓ esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
- ✓ pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali del Titolare, in relazione all'attività che viene da questi svolta;
- ✓ completi: nel senso di raccogliere tutte (e solo) le informazioni necessarie a raggiungere le finalità indicate e tutelare contemporaneamente il concreto interesse e diritto del soggetto interessato;
- ✓ non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
- ✓ conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione applicabili alla tipologia di dati trattati. Trascorso detto periodo, i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

I dati idonei a rivelare lo stato di salute o la vita sessuale di una persona, ove possibile, devono essere conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi delle informazioni trattate.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dalla Normativa privacy, anche su istanza dell'interessato, è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento ove possibile (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Ciascun Responsabile deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste gravi sanzioni amministrative e penali nonché il risarcimento in sede civile di qualsivoglia danno, patrimoniale e non, eventualmente cagionato all'interessato.
In ogni caso si rammenta che la responsabilità penale per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.
Mentre, in merito alla responsabilità civile, si fa rinvio all'art. 2050 c.c., che disciplina la responsabilità per esercizio di attività pericolosa e i conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, chiunque tratti dati altrui è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee/adeguate a garantire appunto la sicurezza dei dati detenuti.

Compiti particolari del Responsabile

Ogni Responsabile ed eventuale Ulteriore Responsabile, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare. Lo stesso, quindi:

A. rientrando la ASL tra i soggetti normativamente in tal senso tenuti, provvede, quantomeno per le attività di trattamento che gli sono demandate in virtù del Contratto/Convenzione; a dotarsi di un Responsabile della Protezione dei Dati (artt. 37 e ss. del GDPR), del Registro delle attività di trattamento (art. 30 comma 2 del GDPR) da tenere a disposizione del Titolare e/o delle Autorità che lo richiedano e di una procedura per i casi di Violazione dei dati personali che preveda espressamente l'adempimento di cui al comma 2 dell'art. 33 del GDPR;

B. definisce di comune accordo col Titolare, per ciascun trattamento di dati personali, la durata del trattamento stesso e la cancellazione o anonimizzazione dei dati obsoleti, anche nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

C. nel prestare la propria attività così come pattuita nel Contratto/Convenzione, compie le operazioni di trattamento, informatico e cartaceo, affidategli nel rispetto del Codice della privacy e successivamente del GDPR, delle misure di sicurezza ivi previste, dei pertinenti Provvedimenti emanati/emanandi dal Garante e delle presenti istruzioni, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive/adeguate misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

D. provvede a che venga fornita l'informativa elaborata dal Titolare ai soggetti interessati in special modo ogni qualvolta gli venga demandata la raccolta diretta di dati personali;

E. modifica e tiene costantemente aggiornate le proprie misure di sicurezza mediante l'applicazione di ogni ulteriore accorgimento tecnico, logistico, organizzativo e procedurale, eventualmente prescritto dal Titolare, o dal Garante e, in ogni caso, in funzione del progresso tecnologico e della natura dei dati trattati. Di volta in volta il Responsabile darà tempestiva segnalazione al Titolare delle variazioni apportate. Resta fermo il diritto del Titolare di richiedere al Responsabile l'adozione di misure ulteriori.
Al momento della definitiva vigenza del GDPR, il Responsabile è tenuto ad adottare autonomamente tutte le misure richieste ai sensi dell'articolo 32 di detta norma nonché ad assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 30 e da 33 a 36 del GDPR, tenendo

conto della natura del trattamento e delle informazioni a sua disposizione. In particolare, tenuto conto della natura, dell'oggetto, del contesto e delle finalità di trattamento, il Responsabile, nei termini della discrezionalità normativamente concessagli, si impegna ad adottare, tra l'altro, se del caso, le seguenti misure di sicurezza, in quanto ritenute adeguate per garantire un livello di sicurezza adeguato al rischio:

- misure minime di cui all'Allegato B) del Codice della privacy.
- Cifratura o pseudonimizzazione dei dati personali.
- Backup e disaster recovery.
- Audit interni ed esterni in materia di privacy;

F. laddove pertinente in relazione all'oggetto del Servizio, in relazione all'attuazione del Provvedimento Generale del Garante del 27 novembre 2008 e s.m.i. relativo alla figura professionale dell'Amministratore di Sistema, il Responsabile si adegua tempestivamente al predetto provvedimento e procede, tra l'altro, a:

a. designare individualmente i propri Amministratori di Sistema incaricati dell'esecuzione delle attività del Servizio, previa valutazione delle rispettive caratteristiche di esperienza, affidabilità e capacità di garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

b. verificare almeno annualmente l'attività dei propri Amministratori di Sistema circa la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali;

c. mantenere un elenco completo e aggiornato contenente gli estremi identificativi e le funzioni attribuite alle persone fisiche nominate quali Amministratori di Sistema dal Responsabile. Il Responsabile si impegna a tenere tale elenco in ogni caso costantemente aggiornato ed a disposizione del Titolare, ovvero del Garante o altra Pubblica Autorità, su richiesta, in qualunque momento;

d. predisporre e utilizzare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) effettuati dagli Amministratori di Sistema ai sistemi di elaborazione e agli archivi elettronici; tali registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste e provvedere alla loro conservazione per un periodo congruo di minimo 6 (sei) mesi;

G. si assicura che il trattamento dei dati per lo svolgimento di prestazioni sanitarie finalizzate alla tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, sia subordinato alla preventiva acquisizione del consenso, salvi i casi di emergenza ed incolumità fisica. In caso di trattamento di dati genetici, la preventiva acquisizione del consenso deve avvenire obbligatoriamente in forma scritta;

H. provvede e garantisce che tutte le operazioni di trattamento di dati di cui è Titolare la ASL si svolgano, salvo espressa autorizzazione scritta di quest'ultima, solo in territorio UE e che i dati siano protetti da ogni accorgimento informatico, tecnico, logistico, procedurale e organizzativo necessario a garantirne sicurezza e confidenzialità, attestando la piena conformità della sua

attività e di detti sistemi come minimo alle disposizioni previste dal Codice della privacy e dal suo Allegato B);

I. garantisce che, fatto salvo ogni eventuale obbligo di legge – che, laddove esistente, deve comunque essere comunicato preventivamente al Titolare – i dati in questione non siano diffusi e/o vengano comunicati a terzi solo nei limiti di quanto autorizzato dal Titolare, da una norma di legge ovvero secondo le richieste di Pubbliche Autorità;

J. è consapevole che è espressamente vietato al Responsabile ed ai soggetti che con esso eventualmente collaborano, di divulgare, ovvero utilizzare in qualsiasi altro modo, dati personali di terzi dei quali sia venuto a conoscenza nello svolgimento del Servizio, al di fuori delle indicazioni espressamente riportate nella nomina o successivamente ricevute dal Titolare. È parimenti consapevole del fatto che è espressamente vietato cedere a terzi, anche a titolo gratuito, i dati personali oggetto di trattamento, anche se non organizzati in una banca dati e per qualsiasi finalità diversa da quelle contemplate nel Contratto/Convenzione e/o nella nomina;

K. avvisa senza ingiustificato ritardo, scrivendo all'indirizzo "dpo@aslroma2.it", e comunque entro un (1) giorno lavorativo, il Titolare di qualsivoglia, anche solo potenziale, violazione di dati personali di cui abbia conoscenza o sospetto fornendo tempestivamente ogni collaborazione a quest'ultimo anche ai fini del rispetto di quanto previsto dagli artt. 33 e 34 del GDPR;

L. avvisa immediatamente, scrivendo all'indirizzo "dpo@aslroma2.it", e comunque entro un (1) giorno lavorativo, il Titolare di ogni richiesta, ordine od attività di controllo di cui venga fatto oggetto da parte del Garante, dell'Autorità Giudiziaria o di altra Pubblica Autorità. Il Responsabile, che in tal senso fin d'ora si impegna, dovrà senza ritardo eseguire gli ordini del Garante, dell'Autorità Giudiziaria o di altra Pubblica Autorità, con il supporto del Titolare;

M. informa, altresì, tempestivamente, scrivendo all'indirizzo "dpo@aslroma2.it", e comunque entro un (1) giorno lavorativo, il Titolare di qualunque istanza formulata nei suoi confronti, ai sensi dell'art. 7 del Codice e successivamente degli artt. 15 e ss. del Regolamento, con qualunque mezzo venga inoltrata, da parte degli interessati dalle operazioni di trattamento connesse all'esecuzione del Servizio e di ogni altra istanza ricevuta da qualsiasi soggetto in materia di privacy ed in riferimento ai dati personali trattati per conto del Titolare al quale fornirà ogni necessario supporto per garantire il corretto riscontro. Il Responsabile, tenendo conto della natura del trattamento, è tenuto ad assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

N. incarica, sotto la propria responsabilità, dell'esecuzione di operazioni di trattamento informatico e manuale previste dal Contratto/Convenzione, i propri dipendenti nonché, ove espressamente autorizzato dal Titolare, eventuali terzi scegliendo fra soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto del Codice della privacy, del GDPR e delle presenti istruzioni, con particolare riguardo alla sicurezza dei dati. È in ogni caso esclusa qualsiasi utilizzazione dei dati da parte degli incaricati al di fuori delle finalità previste per il

trattamento di cui alla nomina: il Responsabile dovrà vigilare su di essi impartendo tutte le necessarie istruzioni per la protezione dei dati. Il Responsabile terrà sempre a disposizione del Titolare l'elenco nominativo aggiornato degli incaricati. A far data dalla definitiva vigenza del Regolamento, il Responsabile garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza anche a mezzo di nomina avente le medesime caratteristiche di cui all'art. 30 del Codice della privacy.

Istruzioni nel caso di cessazione della nomina

All'atto della cessazione della nomina, per qualsiasi causa avvenga, il Responsabile dovrà interrompere immediatamente ogni trattamento di dati acquisiti nell'esercizio dell'attività concordata e distruggerli fornendo al Titolare idonea attestazione di tale attività, salvo diverse indicazioni esplicite da parte del Titolare di trasferire ad un nuovo soggetto le informazioni stesse. In ogni caso, il Responsabile si impegna sin d'ora al rispetto delle prescrizioni e dei divieti di cui al Codice e al Regolamento anche per il tempo successivo alla scadenza o cessazione della nomina.

Istruzioni per le credenziali di autenticazione

Lo scopo di questa sezione è di fornire le istruzioni operative riguardanti il processo di autenticazione informatica ai sistemi del Titolare laddove previsto in esecuzione del Servizio, in particolare per l'utilizzo delle credenziali (di seguito indicate come password).
Il Responsabile ha l'obbligo di richiedere per sé e/o per i propri Incaricati, l'assegnazione e/o la disattivazione di una o più utenze informatiche personalizzate che consentano l'accesso, con adeguate misure di sicurezza, agli ambiti di trattamento espressamente e specificamente individuati.
È compito del Responsabile rendere edotti i propri Incaricati del fatto che, qualora si verifichi una prolungata assenza o un imprevisto impedimento dell'Incaricato che, per sopraggiunte necessità di operatività e/o di sicurezza del sistema, renda indispensabile e indifferibile intervenire sulle attività di trattamento/profili allo stesso assegnati, il Responsabile del Trattamento, mediante la collaborazione del Responsabile S.I. del Titolare, ovvero un soggetto terzo allo scopo espressamente autorizzato dal Titolare o dal Responsabile, potrà disattivare la password assegnata all'Incaricato e accedere ai dati. L'Incaricato, al rientro in servizio, verrà avvertito dell'evenienza e sarà tenuto alla sostituzione della password non più attiva.
Il processo di autenticazione descritto in questa sezione prevede l'inserimento di un codice identificativo personalizzato dell'Utente (Incaricato), c.d. "user-id", associato a una parola chiave riservata, c.d. "password".

Password Iniziale

- La prima password viene comunicata dagli ADS in modalità riservata all'Incaricato con comunicazione che invita ad effettuare immediatamente la sostituzione.
- La prima password ha carattere provvisorio; non abilita ad alcuna operazione diversa da quelle strettamente necessarie alla sua sostituzione da parte dell'Incaricato.

- L'Incaricato non può e non deve effettuare alcuna operazione se prima non ha provveduto a sostituire la password iniziale.
- L'incaricato effettua la sostituzione della prima password attenendosi alle raccomandazioni fornite nell'Allegato 1 della presente procedura.

Lunghezza e complessità della password

La lunghezza minima della password deve essere almeno di otto caratteri alfanumerici e deve inglobare almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale (es.: !"£$%&/=?^*§ç). Nel caso in cui il sistema non consenta l'utilizzo di una password di otto caratteri, deve essere utilizzato un numero di caratteri pari al massimo consentito.

Scelta e costruzione della password

La password scelta non deve essere banale o facilmente individuabile o riconducibile all'Interessato (data di nascita, codice fiscale, compleanno dei figli, ecc.) pertanto è necessario attenersi alle raccomandazioni fornite nell'Allegato della presente procedura.

Riservatezza della password

Occorre adottare ogni necessaria cautela per assicurare la segretezza e riservatezza della password. L'Incaricato è tenuto alla custodia delle password attenendosi, in particolare, alle seguenti disposizioni:

- la password è strettamente personale e non può essere comunicata ad altri;
- non è consentita la trascrizione della password su carta o su qualsiasi altro supporto;
- l'Incaricato non deve lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Allontanandosi anche temporaneamente dallo stesso deve provvedere a bloccarlo;
- la perdita, la diffusione o la sospetta compromissione di una password personale deve prontamente essere comunicata al Responsabile ed al Responsabile S.I. della ASL;

Aggiornamento della password

L'aggiornamento password è consentito esclusivamente all'Incaricato attenendosi alle seguenti disposizioni:

- la password deve essere aggiornata dall'Incaricato al primo utilizzo e successivamente almeno ogni tre mesi;
- dove tecnicamente possibile deve essere concessa all'Incaricato la possibilità di sostituire in qualsiasi momento ed autonomamente le password anche in caso di sospetta compromissione della riservatezza. Ove non tecnicamente possibile, l'Incaricato è tenuto a segnalare immediatamente la necessità al Responsabile ed al Responsabile S.I. della ASL;
- L' incaricato aggiorna la propria password personale, avvalendosi delle regole fornite in Allegato 1, al verificarsi di uno dei seguenti eventi:
  - immediatamente in caso di prima attivazione
  - per decorrenza del periodo di validità attribuito alla password (3 mesi)
  - su esplicita richiesta del Responsabile S.I. della ASL.

È vietata, senza espressa autorizzazione del Responsabile S.I. della ASL, la sostituzione di una password con una frequenza superiore alle 2 volte al giorno.

Istruzioni per utilizzo Pc

Lo scopo di questa sezione è fornire le istruzioni per la gestione dei Personal Computer sui quali avvengano trattamenti di cui è Titolare la ASL Roma 2.
Non è consentito che due o più Incaricati accedano al sistema informatico, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente e la medesima password.
Il periodo massimo di non utilizzo della password da parte dell'Incaricato è stabilito in tre mesi.
Al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza, l'Incaricato non deve lasciare incustodito e accessibile a terzi lo strumento elettronico. Nel caso in cui, dunque, anche temporaneamente, l'Incaricato debba allontanarsi dalla postazione, dovrà attivare lo screensaver protetto da password, disattivare la propria utenza, o mettere comunque in atto idonei mezzi di protezione che impediscano l'accesso ai dati presenti nel PC. Quando vi sia la necessità di assentarsi in modo prolungato dalla propria postazione di lavoro, oltre che attivare gli idonei mezzi di protezione sopra citati, si consiglia, ove possibile, di chiudere a chiave la porta quando si esce dalla stanza.
Non è consentito archiviare o trattare, neppure temporaneamente, dati personali propri o di terzi non attinenti allo svolgimento dell'attività lavorativa sui sistemi informatici della ASL Roma 2.
L'Azienda Sanitaria Locale Roma 2 non risponderà della perdita di materiale e/o dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro.
Ulteriori disposizioni e/o informazioni in riferimento a quanto precede sono contenute nella procedura informatica pubblicata nell'area Intranet aziendale.

Istruzioni per la gestione dei supporti di memorizzazione rimovibili

Lo scopo di questa sezione è di fornire le istruzioni operative riguardanti la gestione dei supporti di memorizzazione rimovibili: hard disk dei personal Computer, CD ROM, penne USB, ecc.
Prima di procedere al riutilizzo per altri scopi lavorativi e autorizzati dei supporti di memorizzazione e nel caso fosse necessario conservare le informazioni contenute negli stessi, deve essere effettuato il salvataggio dei dati sui sistemi informatici aziendali.
I supporti di memorizzazione prima di essere riutilizzati, devono essere completamente reinizializzati, di modo che le informazioni precedentemente contenute non siano recuperabili e tecnicamente ricostruibili in alcun modo.
I supporti di memorizzazione utilizzati per il trattamento di dati personali di natura sensibile ovvero per la gestione dei dati relativi al personale della ASL Roma 2 non possono essere riutilizzati per scopi diversi e, nel caso di definitiva dismissione, adeguatamente distrutti per rendere assolutamente irricostruibili le informazioni negli stessi anche solo temporaneamente custodite.

Il Responsabile ha la responsabilità di:

- richiedere la riparazione degli hard disk
- richiedere la dismissione degli hard disk, dei CD-ROM, dei supporti USB
- richiedere il riutilizzo degli hard disk e dei supporti USB ove consentito
- decidere sul riutilizzo o meno dei supporti USB

- verificare la reinizializzazione dei supporti USB per poterli successivamente riutilizzare ove consentito.

Gli Incaricati hanno la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk
- segnalare la necessità di un'eventuale dismissione dei supporti USB
- segnalare la necessità di un'eventuale riutilizzo degli hard disk, dei CD-ROM e dei supporti USB
- eseguire la reinizializzazione dei supporti USB per poterli successivamente riutilizzare ove consentito
- effettuare il test sulla reinizializzazione dei supporti USB eseguita precedentemente.

Istruzioni per il trattamento dei documenti cartacei

Il Responsabile dovrà provvedere a:

- identificare gli eventuali soggetti ammessi ad accedere agli archivi cartacei al di fuori dell'orario di lavoro;
- identificare e comunicare al Titolare gli archivi presso l'unità, dove riporre i documenti contenenti i Dati Personali e/o Personali Sensibili (armadi, stanze, casseforti, ecc);
- prevedere la conservazione dei documenti contenenti Dati Personali Sensibili separata dai documenti contenenti Dati Personali comuni;
- verificare, previa consultazione con il Titolare, la corretta esecuzione delle procedure di distruzione dei documenti quando non più necessari o quando richiesto dall'interessato.

Il Responsabile del trattamento, cosi come gli stessi Incaricati dovranno inoltre provvedere a:

- non lasciare incustoditi documenti contenenti Dati Personali e/o Personali Sensibili durante e dopo l'orario di lavoro;
- non lasciare in luoghi accessibili al pubblico i documenti contenenti Dati Personali e/o Personali Sensibili;
- riporre i documenti negli archivi quando non più operativamente necessari;
- limitare allo stretto necessario l'effettuazione di copie e/o la trasmissione all'esterno dei suddetti documenti.

La riproduzione di documenti contenenti Dati Personali Sensibili su supporti non informatici (ad esempio fotocopie) è vietata se non espressamente autorizzata preventivamente e specificatamente dalla Direzione Sanitaria, del Responsabile competente o se richiesta dal paziente. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali.
Nel seguito sono evidenziate le disposizioni che il Responsabile e gli Incaricati devono applicare e rispettare quando trattano documenti cartacei contenenti Dati Personali e/o Personali Sensibili.

Archiviazione dei documenti cartacei

I documenti cartacei devono essere:

- conservati in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti cartacei, garantendo, quindi, la riservatezza e l'integrità dei Dati Personali e/o Personali Sensibili, in essi contenuti
- riposti negli appositi archivi che dovranno essere chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa. Le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse
- trasferiti presso gli archivi centrali quando non più operativamente necessari.

In particolare, per ciò che attiene alle cartelle cliniche, si rammenta che queste devono il più possibile viaggiare insieme al paziente cui si riferiscono. I documenti devono sempre essere utilizzati e conservati in maniera che i dati relativi al paziente siano visibili solo a chi è autorizzato a trattarli (Es. deve essere appoggiato sempre con il frontespizio rivolto verso il basso: ecc.).

Consultazione dei documenti cartacei

La consultazione dei documenti contenenti Dati Personali e/o Personali Sensibili, deve avvenire esclusivamente da parte degli Incaricati, solo quando operativamente necessario e quando possibile *in loco*. L'Incaricato può effettuare la consultazione di tali documenti fuori orario di lavoro solo se preventivamente autorizzato dal Responsabile, identificato e registrato dalla vigilanza.

Consegna dei dati agli Interessati - Incaricati

La consegna dei documenti contenenti Dati Personali e/o Personali Sensibili deve essere effettuata, in modo da garantirne la riservatezza, in busta chiusa indirizzata nominativamente al destinatario (Responsabile, Incaricato e/o Interessato), ovvero a persona da quest'ultimo incaricata a mezzo di espressa delega scritta.

Distruzione dei documenti cartacei

Tutti i documenti che non devono essere conservati per legge, devono essere distrutti al termine della loro utilizzazione.
La distruzione dei documenti nei limiti consentiti dalla legge, deve essere effettuata quando è espressamente richiesto dall'interessato e/o quando comunicato dal Titolare ovvero dal Responsabile, all'interno della propria area di competenza.
I documenti dovranno essere distrutti, sotto la supervisione del Responsabile all'interno della propria unità.
La distruzione dei documenti cartacei contenenti Dati Personali Sensibili deve essere effettuata, attraverso opportuni strumenti (distruggidocumenti a frammento), in modo da rendere impossibile la ricostruzione del documento.

Raccomandazioni per la creazione delle password

1. Le password devono essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.

2. Le password devono contenere almeno un carattere appartenente a ciascuno degli insiemi sopra enunciati.
3. Nei casi in cui non risulti possibile l'utilizzo dei simboli speciali, le password devono contenere caratteri numerici ed alfabetici ripartibili in numero compreso tra un minimo di 3 ed un massimo di 5, ferma restando la lunghezza minima complessiva fissata in 8 caratteri.
4. Le password non devono contenere più di 3 caratteri uguali consecutivi.
5. Le password non devono contenere caratteri di spaziatura.
6. Le password non devono contenere:
   a. nomi propri di persona;
   b. sigle di funzioni organizzative o progetti interni alla ASL;
   c. nomi di giorni della settimana, mesi dell'anno o stagioni;
   d. nomi di riferimenti geografici;
   e. nomi di personaggi della politica, sport, cinema e fumetti.
   f. riferimenti alla user-id;
   g. il nome o cognome dell'incaricato;
   h. le matricola dell'incaricato;
   i. la data di nascita dell'incaricato, del coniuge o dei figli;
   j. esclusivamente date in qualsiasi formato e con qualsiasi separatore di uso comune.
7. Ogni nuova password deve differire dalla precedente perlomeno in 4 caratteri.

Violazione consentita delle password

In casi eccezionali, per garantire la salute dell'interessato, per rispondere a richieste di Pubbliche Autorità, ovvero per ragioni insopprimibili di continuità lavorativa, il Titolare, attraverso gli Amministratori di Sistema, può procedere o acconsentire che un Responsabile proceda alla violazione delle credenziali di accesso di un incaricato.
In tal caso, della violazione e delle ragioni che l'hanno determinata, si redige sintetico verbale che viene conservato agli atti del Titolare.
L'incaricato è informato della violazione nella prima occasione utile ed è tenuto ad effettuare l'inserimento di una nuova password a sistema prima di avviare qualsivoglia operazione di trattamento.

Norma di chiusura

Per tutto quanto non espressamente codificato nel Contratto/Convenzione, nella nomina e nel presente Allegato, il Responsabile, fatta salva la Normativa Privacy, è tenuto a richiedere chiarimenti al Titolare e a uniformarsi a qualsivoglia istruzione dallo stesso ricevuta.

Aggiornamento gennaio 2018