Repubblica di San Marino
ISTITUTO PER LA SICUREZZA SOCIALE
IL COMITATO ESECUTIVO

SEDUTA DEL 30 novembre 2023 – seduta straordinaria

DELIBERA N. 5
PAG. N. 6 - 7 - 8

Oggetto: adozione del modello organizzativo privacy, del registro delle attività di trattamento dei dati personali e nomina dei Responsabili interni all'I.S.S. del trattamento art. 29 legge n. 171/2018

Il Comitato Esecutivo,

validamente riunito ai sensi dell'articolo 18 della Legge 30 novembre 2004 n. 165;
verificato che non sussiste in capo ai membri conflitto di interessi in merito all'oggetto della presente deliberazione;

vista la delibera del Congresso di Stato n. 23 del 6 luglio 2022, con la quale veniva espresso parere favorevole: "*……omissis,,,,,al conferimento, da parte dell'I.S.S., di un incarico professionale in favore della SFERA Professionisti Associati…omissis….*";

vista la successiva delibera n. 9 del Comitato Esecutivo del 24 novembre 2022 in seduta straordinaria, a parziale modifica della precedente del 27 luglio 2022 n. 14, con la quale autorizzava il Direttore Generale a conferire a SFERA Professionisti Associati un incarico professionale per la progettazione di: un modello organizzativo di privacy, il registro delle attività di trattamento dei dati personali e quanto previsto ex L. 21 dicembre 2018 n. 171;

vista la relazione finale trasmessa dal dott. Andrea Cecchetti SFERA Professionisti Associati via e – mail in data 8 settembre 2023, di seguito in stralcio riportata: "*…omissis…..si ricorda che il modello organizzativo e correlata documentazione rappresentano le fondamenta della compliance dell'Istituto per la Sicurezza Sociale alle disposizioni normative in materia di trattamento dei dati personali e che, in conformità con il principio del miglioramento continuo, si rende necessaria, ove approvata, la prosecuzione dei lavori su base continuativa che permettano di affrontare tematiche di dettaglio a supporto dell'Ufficio Affari Generali e del futuro Responsabile della protezione dei dati personali quali a titolo esemplificativo ma non esaustivo le valutazioni d'impatto, l'aggiornamento del registro dei trattamenti, l'assistenza e consulenza di dettaglio su determinati trattamenti di dati personali, l'aggiornamento del risk assesment, la formazione continua del personale dipendente, la funzione di punto di contatto per l'Ufficio Affari Generali e il Responsabile della protezione dei dati personali…omissis…*";

visto l'art. 78 della Legge n. 171/2018 che stabilisce come l'I.S.S. in qualità di Ente facente parte del sistema sanitario della Repubblica di San Marino tratta i dati personali ed in particolare, i dati relativi alla salute;

visto l'art. 2 lett. g) della Legge n. 171/2018 che indica nel titolare del trattamento la persona fisica o giuridica, che singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento di dati personali e gli strumenti utilizzati, ivi compreso il profilo di sicurezza;

vista la delibera del Congresso di Stato n. 5 della seduta del 11 marzo 2019 avente ad oggetto la nomina dei titolari dei trattamenti dei dati personali e che fra l'altro nomina il Direttore Generale dell'I.S.S. quale titolare del trattamento dei dati personali sanitari per conto dell'Ente pubblico stesso;

visto l'art. 2 lett. h) della legge n. 171/2018 che intende quale responsabile del trattamento la persona fisica o giuridica, che tratta dati personali per conto del titolare del trattamento;

Repubblica di San Marino
ISTITUTO PER LA SICUREZZA SOCIALE
IL COMITATO ESECUTIVO

considerato che secondo quanto previsto dall'art. 29 comma 1 della legge n. 171/2018:*"...omissis qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti della presente legge e garantisca la tutela dei diritti dell'interessato……omissis…"*;

vista la relazione dell'Esperto Amministrativo Legale avv. Marco Ghiotti, incaricato quale Responsabile della protezione dei dati pervenuta al Direttore Generale in data 27 novembre 2023 prot. n. 4453, con la quale comunica che: *"…omissis… SFERA Professionisti Associati ha condotto e portato a termine l'incarico in merito alla progettazione di una bozza di modello organizzativo privacy per l'Istituto di Sicurezza Sociale …omissis…"*, che si allega alla presente delibera;

vista la e – mail pervenuta in data 28 novembre 2023 da parte del dott. Andrea Cecchetti SFERA Professionisti Associati, con la quale comunica che a seguito delle attività svolte, sono stati individuati gli autorizzati di primo livello, quali Responsabili interni all'I.S.S. del trattamento ai sensi dell'art. 29 della legge n. 171/2018, già precedentemente indicati nel registro delle attività di trattamento dei dati personali e nel Modello organizzativo privacy, nelle seguenti funzioni:

- Direttore Amministrativo
- Direttore delle Attività Sanitarie e Socio Sanitarie
- Direttori di Dipartimento
- (Dirigenti) Direttori U.O.C.
- Responsabili U.O.S.
- Responsabili M.F.
- (Responsabili) Esperti uffici

e nel contempo, trasmette in allegato, l'ordine di servizio e le "istruzioni di trattamento dei dati personali sanitari" da adottare nei confronti dei sopra riportati professionisti dell'I.S.S., ai quali vanno aggiunti anche i Responsabili delle U.O.S.D., tutti da incaricare, entrambi allegati alla presente delibera;

tutto quanto sopra premesso e considerato;

delibera

di adottare il "Modello organizzativo privacy" e il registro delle attività di trattamento dei dati personali dell'I.S.S. presentato da SFERA Professionisti Associati;

delibera altresì

di conferire mandato al Direttore Generale per quanto di sua competenza, quale Titolare del trattamento dei dati ai sensi e per gli effetti dell'art. 29 1° comma della legge n.171/2018 (Responsabili interni del trattamento), per la nomina degli "*autorizzati di primo livello*" nelle funzioni di: Direttore Amministrativo, Direttore delle Attività Sanitarie e Socio Sanitarie, Direttori di Dipartimento, Direttori di U.O.C., Responsabili U.O.S., Responsabili di U.O.S.D., Responsabili M.F., Esperti uffici, come da tabella allegata alla presente delibera;

Repubblica di San Marino
ISTITUTO PER LA SICUREZZA SOCIALE
IL COMITATO ESECUTIVO

Manda

all'Esperto Amministrativo Legale dell'I.S.S. quale Responsabile della protezione dei dati per il seguito di competenza e per predisporre una proposta di piano di formazione.

Manda altresì

all'Ufficio del Personale e Libera Professione affinché, al momento della firma del contratto di nomina o rinnovo degli incarichi apicali di cui sopra, venga sottoscritto l'ordine di servizio "primo livello", la consegna delle istruzioni generali sul trattamento dei dati personali e la relativa informativa.

IL DIRETTORE GENERALE
- Dr. Francesco Bevere -

IL DIRETTORE AMMINISTRATIVO
- Dott. Marcello Forcellini -

IL DIRETTORE DELLE ATTIVITA' SANITARIE E SOCIO SANITARIE
- Dr. Sergio Rabini -

Atto deliberativo trasmesso a: Segreteria di Stato per la Sanità, Esperto Amministrativo Legale RPD, Direttori Dipartimento, Direttori UOC, Responsabili UOS, Responsabili MF, Esperti Uffici, Ufficio del Personale, Collegio dei Sindaci Revisori.
Pubblicazione: divulgabile tramite sito web dell'ISS.

c) comunica tempestivamente al Responsabile della Protezione dei dati personali, informando il Titolare del trattamento, eventuali casi di violazione dei diritti della libertà delle persone fisiche;

d) Propone al Responsabile della Protezione dei dati personali eventuali nuovi Autorizzati di Secondo Livello.

Il soggetto Autorizzato di Primo Livello esegue e gestisce internamente i trattamenti dei dati nel rispetto delle prescrizioni della Normativa Interna e del presente ordine di servizio, secondo le condizioni e i termini generali (**Istruzioni generali sul trattamento dei dati personali)** e alle ulteriori istruzioni, anche in materia di sicurezza, riportate nei documenti aziendali messi a disposizione.

Condizioni generali

1. L'aggiornamento del presente Ordine di Servizio, che permane valido fino a revoca o al verificarsi di uno degli eventi di cui al successivo p.to 3, avrà luogo esclusivamente nel caso di cambio di mansione o di livello gerarchico all'interno dell'organigramma aziendale;
2. Nel caso di cambiamento della mansione, nella continuità del rapporto di lavoro, le istruzioni e i correlati obblighi contenuti nel presente ordine di servizio si intendono automaticamente trasferiti al nuovo incarico, qualora permanga il medesimo livello di responsabilità nella gerarchia aziendale così come definita dall'organigramma;
3. Il presente ordine di servizio può essere revocato in ogni momento, con effetto immediato e senza obbligo di preavviso e si intende revocato automaticamente in caso di interruzione del rapporto di lavoro per dimissioni / licenziamento / chiusura del rapporto;
4. Resta altresì inteso che nessun ulteriore compenso o rimborso sarà garantito per l'assunzione della funzione di Autorizzato al Trattamento dei dati personali di cui al presente atto, essendo tale attività parte integrante della mansione di lavoro;
5. Per qualsiasi ulteriore informazione in merito alle istruzioni di cui al presente atto, l'autorizzato potrà rivolgersi al Titolare del trattamento e al Responsabile della protezione dei dati personali;
6. Nell'ambito dei compiti assegnati, l'Autorizzato sarà assistito continuativamente dal Responsabile della Protezione dei dati personali designato e contattabile al seguente indirizzo di posta elettronica marco.ghiotti@iss.sm;
7. Il mancato rispetto delle presenti istruzioni potrà comportare la violazione degli obblighi previsti dalla Normativa Interna ed esporre il Titolare, i relativi delegati ed anche i singoli incaricati a rischi sul piano delle responsabilità e delle sanzioni a livello civile e amministrativo.

Il Titolare del Trattamento

Direttore Generale

Oggetto: Ordine di servizio in materia di trattamenti di dati personali in conformità alla Legge 21 dicembre 2018 n.171

L'Istituto per la Sicurezza Sociale, con sede legale a Borgo Maggiore (RSM) in Via Scialoja n. 20, in qualità di Titolare del trattamento dei dati personali, ai sensi della Legge 21 dicembre 2018 n.171 (di seguito "Normativa Interna") nella persona del Direttore Generale pro-tempore.

PREMESSO

a) Che in data 5 gennaio 2019 è entrata in vigore la Legge 21 dicembre 2018 n.171 (Protezione delle persone fisiche con riguardo al trattamento dei dati personali).

b) Che ai sensi dell'art.30 della Legge 21 dicembre 2018 n.171 "il titolare o il responsabile del trattamento possono prevedere, nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche espressamente designate che operano sotto la loro autorità" e "il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta."

c) Che Lei risulta essere dipendente dell'Istituto con ruolo di _____

d) Che il Titolare del trattamento dei dati personali intende adeguarsi alle disposizioni contenute nella Normativa Interna, provvedendo, in tale fase, all'individuazione dei soggetti Autorizzati di Primo Livello al trattamento di dati personali.

LA IDENTIFICA

quale soggetto Autorizzato di Primo Livello a trattare i dati personali esclusivamente nell'ambito delle competenze e mansioni a Lei assegnate e nel rispetto dei perimetri di accesso alle banche dati aziendali a Lei attribuite.

Il soggetto Autorizzato di Primo Livello Dottor _____:

a) assiste il Responsabile della Protezione dei dati personali e il Titolare nell'adozione delle procedure in ottemperanza al Modello Organizzativo Privacy aziendale nonché in ogni altra attività o intervento richiesto al fine di adeguare l'organizzazione aziendale alle disposizioni normative in materia di protezione dei dati personali;

b) comunica preventivamente al Titolare del trattamento e al Responsabile della Protezione dei dati personali, eventuali nuovi trattamenti di dati personali, la cessazione di trattamenti in corso e l'acquisizione di nuove tecnologie che prevedano il trattamento dei dati personali;

Istruzioni Generali per il Trattamento dei Dati Personali

INDICE

1. SCOPO

In questo documento sono descritte le modalità operative generali adottate dalla scrivente Azienda, in qualità di Titolare del Trattamento, nell'ambito dell'applicazione delle misure adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi di trattamento dei dati personali degli Interessati, non in conformità alle norme di Legge, nonché alle istruzioni che il personale dipendente deve rispettare in ottemperanza alle disposizioni della normativa sulla protezione dei dati personali ed in relazione alle attività svolte nell'ambito della struttura aziendale in cui opera.

2. APPLICABILITÀ

Le istruzioni contenute nel presente documento riguardano tutto il personale dipendente della scrivente Azienda.

In ottemperanza alle disposizioni della normativa sulla protezione dei dati personali ed in relazione alle attività svolte nell'ambito della struttura aziendale in cui opera, la persona autorizzata al trattamento dei dati personali, dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal Titolare

I dati personali devono essere trattati:

a) in osservanza dei criteri di riservatezza;

b) in modo lecito e secondo correttezza;

c) per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità prefissate;

d) nel pieno rispetto delle misure di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di divulgazione o accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Le misure di sicurezza previste dalle policy aziendali in relazione agli obblighi di legge sono per maggior chiarezza distinte in funzione delle seguenti modalità di trattamento dei dati:

1. senza l'ausilio di strumenti elettronici (es. dati in archivi cartacei o su supporto magnetico/ottico);

2. con strumenti elettronici (PC e sistemi informatici).

3. DEFINIZIONI

Termine	*Definizione*
Titolare del trattamento o suo delegato	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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Responsabile della protezione dei dati personali	Il soggetto esterno che sorveglia sull'osservazione delle disposizioni di legge, fornisce pareri al Titolare, agisce quale punti di contatto con tutti i soggetti coinvolti nei trattamenti di dati personali;
Autorizzato di primo livello	Un soggetto interno all'organizzazione a cui sono attribuiti specifiche istruzioni operative sulla gestione delle procedure, della documentazione e degli atti contenuti nel Modello organizzativo privacy;
Autorizzato (primo e secondo livello)	Ciascun dipendente aziendale che riceve le corrette istruzioni per effettuare trattamenti di dati personali;
Amministratore di sistema (brevemente "ADS"):	la persona fisica interna o esterna all'organizzazione aziendale che ha il compito di sovrintendere alle risorse attinenti ai sistemi operativi e/o i sistemi di base dati degli elaboratori ovvero degli apparati/sistemi di rete o di sicurezza in uso presso l'azienda e più specificamente, funzionali ai trattamenti svolti internamente in azienda o da essa operati;
Modello Organizzativo privacy	Un sistema integrato aziendale che evidenzia in modo sinottico le procedure, la documentazione e gli atti inerenti ai trattamenti di dati personali.

4. ORGANIZZAZIONE PRIVACY

Termine	*Definizione*
Titolare del trattamento	Istituto per la Sicurezza Sociale, nella persona del Direttore Generale
Responsabile della protezione dei dati personali	Ufficio del Responsabile Protezione Dati (Avv. Marco Ghiotti)
Amministratori di sistema	Ufficio Informatica
Autorizzati di primo livello	Direttori/Responsabili Dipartimenti/Unità/Uffici

5. TRATTAMENTI DI DATI PERSONALI EFFETTUATI CON STRUMENTI ELETTRONICI

5.1 Protezione dei PC e dei dati

Per svolgere la propria attività lavorativa la scrivente Azienda ha affidato al proprio Autorizzato un personal computer (fisso o mobile) ed i relativi programmi/applicazioni. Essi sono strumenti di lavoro e, pertanto, devono essere:

a) utilizzati solo per scopi inerenti alle mansioni lavorative attribuite;

b) custoditi in modo appropriato;

c) utilizzati, se non previsto diversamente, in modo esclusivo da un solo utente;

d) configurati in modo che sia presente esclusivamente software fornito/approvato dalla scrivente Azienda;

e) coerenti ai requisititi hardware e software definiti in relazione alle finalità aziendali.

f) dotati di software antivirus aziendale aggiornato costantemente e con la funzione "Monitor" attiva.

g) Oggetto di installazione di tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.

Sulla base di quanto sopra detto gli Incaricati che accedono a dati personali in formato elettronico devono adottare le seguenti cautele:

a) utilizzare una password di accesso alle risorse di rete insieme alla propria user-id, conforme alle politiche aziendali

b) non lasciare incustodita la postazione di lavoro senza prima aver bloccato l'account; è opportuno che il salva schermo venga impostato in modo che si attivi automaticamente dopo circa 15 minuti di inattività;

c) segnalare prontamente il furto, il danneggiamento o lo smarrimento di tali strumenti.

Non è consentito:

a) modificare le configurazioni impostate secondo gli standard della scrivente Azienda sul PC in uso senza la preventiva autorizzazione;

b) installare sul PC software privo di licenza, non relativo alla propria attività o pericoloso;

c) installare sul PC mezzi di comunicazione propri (ad es. chiavette UMTS, Wi-Fi, 3G, ecc.);

d) ascoltare programmi, file audio o musicali, se non a fini prettamente lavorativi.

In caso di prolungata assenza o impedimento dell'Autorizzato, qualora fosse indispensabile e indifferibile intervenire per garantire la disponibilità dei dati personali, su indicazione del Responsabile della Protezione dei dati personali, gli amministratori di sistema potranno accedere alla postazione di lavoro affidata per mantenere la necessaria operatività e sicurezza del sistema attraverso una forzatura e riassetto della relativa password di accesso. Al suo rientro, all'Autorizzato verrà assegnata una nuova password.

In caso di mancato utilizzo per un periodo superiore a sei mesi la user-id è disabilitata.

I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

5.2 Gestione delle password

L'accesso alle procedure informatiche che trattano dati personali è consentito alle persone autorizzate in possesso di "credenziali di autenticazione" (es: password) che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione delle persone autorizzate al trattamento dei dati personali (user-id) associato ad una parola chiave riservata (password). Le persone autorizzate al trattamento dei dati personali devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

a) Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se autorizzati al trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione all'accesso da parte dell'Autorizzato di primo livello.

b) Le credenziali di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Esse non vanno mai condivise con altri utenti (anche se persone autorizzate al trattamento dei dati personali). Qualora le credenziali dovessero perdere il grado di segretezza, è opportuno provvedere alla loro modifica.

c) Le password non devono mai essere trascritte su fogli, agende o post-it facilmente accessibili a terzi.

d) Le password devono essere sostituite, a cura della singola persona autorizzata al trattamento dei dati personali, al primo utilizzo e successivamente almeno ogni tre mesi, salvo modalità e periodi più restrittivi di volta in volta comunicati dagli autorizzati di primo livello o previsti da specifiche procedure.

e) Le password devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le password non devono contenere riferimenti agevolmente riconducibili alla persona autorizzata al trattamento dei dati personali (es. nomi propri o di familiari, data di nascita) e devono essere scelte nel rispetto della normativa aziendale sulla costruzione ed utilizzo delle password (si veda vedi anche il successivo punto 7.1).

5.3 Protezione dei dispositivi portatili (notebook, smartphone, tablet)

Gli incaricati che hanno in dotazione dispositivi portatili devono osservare le seguenti regole:

a) non lasciarli mai incustoditi;

b) durante la guida assicurarsi che le porte dell'auto siano chiuse e comunque non lasciarli mai in vista;

c) limitarne l'utilizzo alle attività strettamente necessarie alle mansioni lavorative attribuite;

d) operare in locali, o in condizioni tali da garantire sempre la riservatezza delle informazioni visibili sul display;

e) effettuare il backup dei dati almeno una volta la settimana secondo le specifiche istruzioni date alla consegna del dispositivo;

f) effettuare il download degli aggiornamenti del programma antivirus secondo le istruzioni ricevute alla consegna del dispositivo;

verificare con frequenza giornaliera la versione e la data dell'ultimo aggiornamento del software antivirus

6. TRATTAMENTI DI DATI PERSONALI CONTENUTI IN DOCUMENTI ED ARCHIVI CARTACEI

6.1 Come custodire i documenti cartacei

Ciascun Autorizzato deve adottare le seguenti cautele:

a) I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili alle persone non autorizzate al trattamento dei dati stessi (es. armadi o cassetti chiusi a chiave).

b) I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.

c) I documenti contenenti dati personali non devono rimanere incustoditi sulle scrivanie o tavoli di lavoro durante il giorno e occorre verificare che, in caso di allontanamento anche temporaneo dalla propria postazione di lavoro, non vi sia possibilità, da parte di colleghi non autorizzati o di terzi, di accedere ai dati personali per i quali sia in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

d) Assicurarsi che i documenti cartacei non siano suscettibili di indebita e non autorizzata visione durante l'accesso agli uffici da parte di terzi estranei alla scrivente Azienda (es. visitatori, consulenti, dipendenti di Aziende esterne, addetti alle pulizie, ecc.); in quest'ottica, è importante limitare l'accesso e la permanenza dei suindicati soggetti e, laddove necessario, vigilare sugli stessi.

La scrivente Azienda ha messo a disposizione degli Incaricati dei luoghi sicuri (armadi/cassetti chiusi a chiave, locali archivio) ove custodire i documenti contenenti dati personali.

6.2 Quando condividere o comunicare i documenti cartacei

L'Autorizzato deve, inoltre, utilizzare i dati personali in base al principio del *"need to know"* e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie attività lavorative (anche se queste persone sono a loro volta persone autorizzate al trattamento dei dati personali). I dati non devono essere comunicati all'esterno dell'Azienda e comunque a soggetti terzi se non previa autorizzazione.

6.3 In che modo distruggere i documenti cartacei

L'Autorizzato deve conservare i documenti per il tempo necessario per adempiere ad obblighi di legge e/o alle finalità di trattamento perseguite dalla scrivente Azienda trascorso il quale essi devono essere distrutti con le modalità decise dal Titolare.

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

6.4 Come gestire le copie, le stampe, i fax

L'Autorizzato deve adottare le seguenti cautele:

a) limitare al massimo il numero delle stampe o fotocopie effettuate. Una volta effettuate le medesime debbono essere immediatamente prese in carico da chi le ha prodotte evitando che restino incustodite.

b) i documenti sottoposti a scannerizzazione debbono essere immediatamente riposti nei fascicoli di competenza.

c) occorre presidiare quanto spedito o ricevuto via fax, riponendo i correlati documenti negli appositi fascicoli, rispettivamente, di origine o di "distribuzione posta interna" in modo tale che giungano a chi di dovere;

d) eventuali stampe o fotocopie non riuscite, appunti o bozze in genere, devono essere distrutte con le apposte macchine distruggitrici, se disponibili, altrimenti devono essere ridotte in pezzi tali da non permettere di ricostruirne il contenuto;

e) non utilizzare stampe o fotocopie non riuscite come carta per appunti nonché, per lo stesso fine, trasportarle all'esterno dalla scrivente Azienda.

6.5 Come gestire i documenti cartacei all'esterno dell'Azienda

L'Autorizzato in caso di trasporto dei documenti al di fuori della scrivente Azienda deve:

a) tenere sempre con sé la cartella o la borsa contenente i documenti e ove possibile, evitare che sia visibile da terzi anche soltanto la prima pagina o la copertina dei documenti;

b) non lasciare mai incustodite la cartella o la borsa durante il trasporto e, se possibile, chiuderle a chiave o azionare le serrature a combinazione.

6.6 Ulteriori istruzioni in caso di trattamento di categorie particolari di dati personali

Al fine di garantire maggiore tutela e protezione alle categorie particolari di dati l'Autorizzato deve adottare le seguenti misure:

a) I documenti contenenti categorie particolari di dati personali (di seguito "dati particolari"), dati relativi a condanne penali e reati (di seguito "giudiziari") o dati relativi al traffico devono essere controllati e custoditi in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.

b) Per accedere agli archivi contenenti dati particolari e giudiziari fuori orario di lavoro è necessario farsi identificare e registrare sugli appositi registri.

6.7 Divieti e comportamenti non corretti

Infine, è vietato:

a) effettuare copie fotostatiche o di qualsiasi altra natura di documenti, atti, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante dati personali oggetto del trattamento per fini estranei all'attività lavorativa;

b) diffondere dati personali o comunicarli a terzi.

7. ISTRUZIONI GENERALI

7.1 Come scegliere e usare la password

- Usare almeno 8 caratteri
- Usare lettere, numeri e almeno un carattere tra . ; $! @ - > <
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla matricola o alla user-id
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi
- Non condividerla con altri utenti

7.2 Come comportarsi in presenza di ospiti o personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo con password del PC premendo ctrl-alt-canc e selezionando il pulsante "Lock Computer".
- Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- Non rivelare le password al telefono - nessuno è autorizzato a chiederle.
- Segnalare qualsiasi anomalia o stranezza al proprio Autorizzato di primo livello.

7.3 Come gestire la posta elettronica

- Utilizzare l'indirizzo di posta elettronica aziendale solo per scopi lavorativi.
- Non aprire messaggi con allegati di cui non si conosce l'origine, possono contenere virus in grado di alterare i dati sul PC. In questo caso occorre spostare il messaggio nel cestino e svuotare quest'ultimo.
- Evitare di aprire filmati e presentazioni scherzose, possono essere pericolose per i dati contenuti sul vostro PC.
- Evitare l'inoltro automatico dalla propria casella aziendale verso caselle personali esterne.

- non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
- non è consentito partecipare a newsgroup, forum o mailing list non attinenti all'attività lavorativa;
- è bene sapere che i messaggi di posta elettronica sono intercettabili e possono essere utilizzati a favore di una delle parti in caso di diverbio.
- l'uso della mail o dei messaggi vocali di un altro utente è proibito a meno che sia necessario e giustificato ma richiede l'avvertimento, e l'autorizzazione da parte dell'utente interessato;
- non inviare, ove possibile, per posta elettronica documenti od informazioni "Strettamente riservati o confidenziali" dal momento che la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da terzi;
- nel caso in cui debbano essere inviati per posta elettronica documenti/informazioni contenenti dati sensibili (ai sensi del Reg. UE 2016/679 ovvero della Legge n. 171/2018) occorre contattare il proprio Autorizzato di primo livello in maniera che tali dati possano preventivamente essere criptati e/o protetti da password;
- si eviti, quando si risponde ad una e-mail, di replicare in copia a tutti i destinatari in origine indicati, ove ciò non sia indispensabile.

7.4 Come usare correttamente internet

- Evitare di scaricare software da Internet (programmi di utilità, di office automation, file multimediali, ecc.) in quanto questo può essere pericoloso per i dati e la rete aziendale. I software necessari all'attività lavorativa vanno richiesti alle competenti funzioni aziendali.
- Usare Internet entro i limiti consentiti dalle procedure/regolamenti aziendali, i siti web spesso nascondono insidie per i visitatori meno esperti.
- Non leggere le caselle personali esterne via webmail, in quanto i provider esterni potrebbero non proteggere dai virus.

7.5 Come comportarsi in causa di violazioni di sicurezza

In caso di eventi relativi a possibili violazioni di dati personali (c.d. data breach), costituiti a titolo esemplificativo da **distruzione di dati informatici** o **documenti cartacei, perdita di dati conseguente a smarrimento/furto di supporti informatici o di documentazione contrattuale, modifica non autorizzata di dati, divulgazione di dati e documenti a soggetti terzi non legittimati, accesso non autorizzato a sistemi informatici**, informare prontamente il l'autorizzato di primo livello o il proprio responsabile diretto al fine dell'attuazione degli adempimenti previsti dalle normative aziendali in applicazione delle disposizioni di legge.

8. MISURE GENERALI PER IL RISPETTO DEI DIRITTI DEGLI INTERESSATI

Fatti salvi i requisiti strutturali ed organizzativi dell'Istituto per la Sicurezza Sociale, tutti gli operatori sanitari ed amministrativi che effettuano trattamenti di dati personali nei confronti di utenti e pazienti devono adottare misure adeguate a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati.

Le misure minime da adottare possono comprendere:

- soluzioni anche tecnologiche in grado di definire un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
- l'istituzione di appropriate distanze di cortesia e di soluzioni anche tecnologiche in grado di assicurare la riservatezza nei colloqui tra operatore e paziente;
- cautele volte ad assicurare che le prestazioni sanitarie non siano erogate in condizioni di promiscuità.

9. DISPOSIZIONI DI LEGGE, NORMATIVE E PROCEDURE AZIENDALI

Le disposizioni di legge sulla protezione dei dati personali unitamente alla documentazione utile a individuare una violazione di dati personali sono pubblicate sulla Intranet aziendale attraverso il seguente percorso: (…)

10. SANZIONI

Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di trattamento dei dati personali, l'inosservanza delle quali può comportare sanzioni o provvedimenti disciplinari.

UFFICIO PERSONALE E LIBERA PROFESSIONE
Istituto per la Sicurezza Sociale

TABELLA "A"
AUTORIZZATI DI PRIMO LIVELLO:

Dr.ssa Ivonne Zoffoli – Direttore Dipartimento Prevenzione
Dott.ssa Raffaella Sapigni - Responsabile UOS Laboratorio Sanità Pubblica
Dott. Antonio Putti - Responsabile UOS Sanità Veterinaria e Igiene Alimentare
Dr.ssa Micaela Santini - Responsabile UOS Medicina e Igiene del Lavoro
Ing. Vincenzo Cesarini – Responsabile UOS Sicurezza Antinfortunistica nei luoghi di lavoro
Dr. Pierluigi Arcangeli – Direttore Dipartimento Socio Sanitario
Dott.ssa Francesca Civerchia – Responsabile UOSD Disabilità e Assistenza Residenziale
Dr. Francesco Berti – Direttore UOC Salute Mentale
Dr. Luigi Maria Morganti – Responsabile UOS Servizi Residenziali
Dr. Paolo Normanni – Responsabile UOS Dipendenze Patologiche
Dott.ssa Cinzia Cesarini – Direttore UOC Assistenza Residenziale Anziani
Dott.ssa Simona Casagrande – Direttore UOC Servizio Territoriale Domiciliare
Dr. William Giardi – Direttore UOC Servizio Minori
Dott.ssa Malpeli Elena – Responsabile MF Attività Educative
Dr. Agostino Ceccarini – Direttore UOC Cure Primarie e Salute Territoriale
Dr. Pietro Bugli – Coordinatore Centro Salute Murata
Dr.ssa Elisaveta Hadji - Coordinatore Centro Salute Borgo Maggiore
Dr.ssa Alessandra Zannoni - Coordinatore Centro Salute Serravalle
Dr.ssa Simonetta Palma - Responsabile UOS Salute Donna
Dr.ssa Antonella Sorcinelli – Direttore Dipartimento Ospedaliero
Dr. Pierluigi Arcangeli – Responsabile UOSD Day Surgery
Dott.ssa Giovanna Maria Gatti – COORDINFTECUO GFP Blocco Operatorio
Dr. Alessandro Mularoni – Responsabile MF Chirurgia Avanzata della Cataratta
Dr. Gianfranco Fantini – Direttore UOC Medicina Trasfusionale e Patologia Clinica
Dr.ssa Manoni Samantha – Responsabile MF Microbiologia
Dr. Marino Gatti – Direttore UOC Radiologia
Dr.ssa Stacchini Sara – Responsabile MF Diagnostica Radiologica Generale-Ecografia
Dr.ssa Larghetti Stefania – Responsabile MF Diagnostica Senologica per immagini

REPUBBLICA DI SAN MARINO
Via Scialoja 20- 47893 Borgo Maggiore
T +378 (0549) 994422 F +378 (0549) 994359 –
http://www.salute.sm

Dr. Battistini Antonio - Responsabile MF Diagnostica Senologica
Dr.ssa Guidi Marilyn Nathalie - Responsabile MF Tomografia Computerizzata
Dr. Luciano Trinchese – Direttore UOC Ortopedia
Dr. Simone Grana - Responsabile MF Traumatologia Dello Sport
Dr. Bruno Esposto – Direttore UOC Anestesia e Terapia Intensiva
Dr. Daniele Bettelli – Responsabile MF Medicina del Dolore e Cure Palliative
Dr. Ataei Faramaz – Responsabile UOS Programmazione Sale Operatorie
Dr. Ataei Faramaz – Responsabile MF Anestesia e Osservazione post Operatoria
Dr. Paolo Barbieri – Responsabile MF Terapia Intensiva
Dr. Giovanni Landolfo – Direttore UOC Chirurgia Generale
Dr. Vitullo Giovanni – Responsabile GFP Urologia
Dr. Alessandro Valentino – Direttore UOC Pronto Soccorso e Degenza Breve
Dr. Cecchetti Claudio – Responsabile MF 118
Dr. Ciacci Alessandro – Responsabile MF Degenza Breve
Dr.ssa Miriam Farinelli – Direttore UOC Ostetricia e Ginecologia
Dr. Maurizio Filippini – Responsabile MF Endoscopia Ginecologica
Dr. Roberto Bini – Direttore UOC Cardiologia ff
Dr. Gabriele Donati – Direttore UOC Medicina Interna
Dr.ssa Susanna Guttmann – Responsabile UOS Neurologia
Dr.ssa Anna Chiara Piscaglia – Responsabile UOS Endoscopia Gastroenterologia
Dr.ssa Anna Maria Ferri – Responsabile UOS Dialisi
Dr.ssa Tatiana Mancini – Responsabile MF Malattie Endocrino Metaboliche
Dr.ssa Stefania Volpinari - Responsabile MF Malattie Reumatologiche e Autoimmuni
Dr.ssa Anna Maria Bugli – Responsabile MF Ematologia
Dr. Enrico Rossi – Direttore UOC Geriatria e Post Acuzie
Dr. Enrico Rossi – Responsabile MF Pneumologia
Dr. Mario Nicolini – Direttore UOC Oncologia
Dr.ssa Ombretta Davoli – Direttore UOC Medicina Fisica e Riabilitativa
Dr.ssa Laura Viola – Direttore UOC Pediatria
Dr.ssa Alessandrini Susanna - Responsabile MF Gastroenterologia ed Endocrinologia Pediatrica

ISTITUTO SICUREZZA SOCIALE - REPUBBLICA DI SAN MARINO

REPUBBLICA DI SAN MARINO
Via Scialoja 20- 47893 Borgo Maggiore
T +378 (0549) 994422 F +378 (0549) 994359 –
http://www.salute.sm

Dott. Simone Bacciocchi - Esperto Ufficio Controllo di Gestione
Luca Terenzi – Esperto Ufficio Servizio Tecnico
Avv. Marco Ghiotti - Esperto Ufficio Affari Generali
Dr.ssa Lucia Bonini – Responsabile UOS Sorveglianza Sanitaria
Ing. Marino Casagrande – Responsabile Servizio Protezione e Prevenzione
Dott. Rossano Riccardi – Direttore UOC Farmaceutica
Ing. Filiberto Casali – Esperto Ufficio Informatico
Rag. Lorenzo Canti – Esperto Ufficio Ingegneria Clinica
Dott. Francesco Biordi – Esperto UOS Formazione Comunicazione URP Qualità e Accreditamento
Dr.ssa Antonella Sorcinelli – Direttore UOC Medicina Legale, Fiscale e Prestazioni sanitarie esterne
Rag. Morena Ragni – Referente CUP e Portineria
Dott.ssa Erica Girometti - Esperto Ufficio Prestazioni Economiche
Dott.ssa Marta Tognacci – Esperto Ufficio Ispettorato
Dott.ssa Sophie Macina – Esperto Ufficio Contributi
Dott.ssa Stefania Frisoni – COORDINFAZ Ufficio Coordinamento Personale Infermieristico
Dott.ssa Cecilia Pedini – Esperto Ufficio del Personale e Libera Professione
Dott.ssa Sara Molinari – Esperto Ufficio Contabilità e Bilanci
Dott. Alex Piselli – Esperto Ufficio Economato
Dott. Marcello Forcellini – Direttore Amministrativo

REPUBBLICA DI SAN MARINO
Via Scialoja 20- 47893 Borgo Maggiore
T +378 (0549) 994422 F +378 (0549) 994359 –
http://www.salute.sm

ISTITUTO SICUREZZA SOCIALE - REPUBBLICA DI SAN MARINO