Allegato "2"

Asl 3
Sistema Sanitario Regione Liguria

ALLEGATI AL DOCUMENTO PROGRAMMATICO

DELLA SICUREZZA 2018-2019

DEI TRATTAMENTI DATI PERSONALI

Aggiornato a marzo 2019

ALLEGATO A: AUTORIZZAZIONE AL TRATTAMENTO DATI

Direzione Generale/
Dipartimento……..
Struttura Complessa ……..

Genova, lì

Prot.n. /

Al Dott/Sig.

AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

ai sensi del Regolamento Europeo n. 2016/679 e norme di armonizzazione

ASL 3 quale Titolare, in persona del legale rappresentante pro tempore Dott. ……, Direttore Generale/in persona del Referente, Dott./Sig. ……..Direttore ……., delegato alla firma dal Titolare, legale rappresentante pro tempore, con il presente atto **designa la S.V. Dott../Sig……, in qualità di Dirigente responsabile della Struttura……..(oppure DIPENDENTE -ruolo – eventuale P.O. oppure figure assimilate es. tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti, lavoratori interinali, etc.), "autorizzato al trattamento dei dati personali"**, con riferimento ai trattamenti svolti nell'ambito delle funzioni e competenze cui è preposto e/o assegnato, per la relativa durata di preposizione-assegnazione, compresi, i trattamenti effettuati nell'ambito di servizi di supporto e/o attività sostitutiva, di attività libero professionale, anche in convenzione, o di attività di sperimentazione autorizzate, nonché con riferimento ai trattamenti svolti nell'ambito delle **specifiche funzioni e competenze** di REFERENTE PRIVACY del sistema Privacy /DIRIGENTE PRIVACY E DIPENDENTE **(e eventualmente FACILITATORE DEL DIRIGENTE DELLA SC/SSD/STRUTTURA ASSIMILATA) /** DIPENDENTE (**e eventualmente FACILITATORE DEL DIRIGENTE DELLA SC/SSD/STRUTTURA ASSIMILATA/DEL REFERENTE)**, come da D.P.S. aziendale .

Tale nomina è in relazione alle operazioni di trattamento dei dati personali e categorie particolari di dati personali ai quali la S.V. ha accesso nell'espletamento delle funzioni proprie e presuppone la conoscenza degli obblighi di legge e delle disposizioni aziendali in materia e l'impegno a trattare i dati personali nel pieno rispetto di tali obblighi e delle istruzioni impartite.

In ottemperanza al Regolamento Europeo n. 679/2016 e norme di armonizzazione, che regolano il trattamento dei dati personali, laddove costituisce trattamento " *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*", ed in relazione al presente atto di nomina, la S.V. è autorizzata a trattare i dati personali (*qualsiasi informazione riguardante una persona fisica identificata o identificabile*

«interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale") strettamente necessari allo svolgimento delle mansioni proprie assegnate, ed in particolare:

a) trattarli in modo lecito, corretto e trasparente ed, in generale in conformità ai principi del Regolamento UE 679/2016 (con particolare riguardo agli artt.5-6) e norme di armonizzazione;
b) a raccoglierli e registrarli per finalità determinate, esplicite e legittime, e successivamente a trattarli in modo che non siano incompatibili con tali finalità;
c) a verificare la loro esattezza e, se necessario, aggiornarli;
d) a verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare del trattamento dei dati, anche per il tramite del Dirigente/Direttore responsabile della struttura-area di afferenza;
e) a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte in Azienda. In ogni operazione di trattamento andrà garantita la massima riservatezza;
f) ad implementare e/o aggiornare costantemente e tempestivamente i contenuti del "registro dei trattamenti" ed i format afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, per la parte di competenza della struttura-area di afferenza, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto nell'ambito delle funzioni privacy specifiche del ruolo ricoperto, con le modalità previste dal D.P.S. aziendale (che mantiene i relativi adempimenti di responsabilità del Dirigente/Direttore responsabile della struttura di diretta afferenza) e dalla vigente normativa. Pertanto dette attività rimangono sotto esclusiva responsabilità (compresa redazione, aggiornamento, conservazione e pubblicità) dei Dirigenti/Direttori responsabili delle singole strutture aziendali , per gli ambiti di rispettiva competenza) e del Titolare, tenendo il R.P.D. solo in copia informatizzata quanto da detti Dirigenti/Direttori trasmessogli;
g) a rispettare ed adottare le misure di sicurezza predisposte (nel rispetto in particolare dei principi di cui all'art.32 del Regolamento UE 679/2016 e norme di armonizzazione) dal Titolare del trattamento dei dati e riportate nel Registro dei trattamenti e relative schede allegate, nonché nel Documento Programmatico sulla Sicurezza aziendale, entrambi pubblicati sulla intranet aziendale nella sezione "Normativa/Privacy";
h) a fornire l'idonea informativa agli interessati ed acquisirne il relativo consenso, laddove necessario ai sensi della vigente normativa, nei casi di raccolta del consenso al trattamento dei dati;
i) a collaborare con il Responsabile per la Protezione dei Dati (R.P.D.) aziendale ed il Titolare per ogni eventuale istruttoria o chiarimento dovesse essere disposta in materia di protezione dei dati personali;
j) ad osservare le disposizioni e/o indicazioni del R.P.D. Aziendale e del Titolare (fornite anche per il tramite del Dirigente/Direttore responsabile della struttura-area di afferenza) in materia di protezione dei dati personali;

k) ad osservare le disposizioni e gli obblighi derivanti dal Regolamento Europeo 679/2016 e norme di armonizzazione, in particolare per quelli inerenti la comunicazione e la diffusione dei dati.
l) ad attenersi alla puntuale adozione delle istruzioni impartite dal Titolare direttamente o tramite delegato alla firma ed anche per il tramite dei Dirigenti/Direttori responsabili della struttura-area di afferenza circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza.

Per ogni altra misura si rinvia alle disposizioni di cui alle citate normative, ivi compresi i provvedimenti e linee guida disposti dall'Autorità Garante per la protezione dei dati personali nelle specifiche materie oggetto di trattamento, fatti propri dal Titolare quali policy aziendali, in quanto compatibili con dette norme, ed al Documento Programmatico sulla Sicurezza aziendale (D.P.S. pubblicato sulla rete Intranet Aziendale nella sezione "Normativa/Privacy) nonché alle allegate istruzioni operative.

Sulla base di quanto sopra, in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'autorizzato dovrà verificare che non vi sia la possibilità da parte di terzi, anche dipendenti, di accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.

Nessun dato potrà essere comunicato a terzi o diffuso senza la specifica autorizzazione del Titolare. E' comunque sempre vietata la diffusione dei dati inerenti lo stato di salute e la vita sessuale degli interessati.
(in caso di tirocinio e/o frequenze assimilate aggiungere: "La validità ed efficacia della presente autorizzazione terminerà con la conclusione del periodo di tirocinio/frequenza effettuato presso la struttura……..di questa ASL.
In ogni caso gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito al termine del rapporto di tirocinio/frequenza con questa ASL.")

La S.V. con il presente atto viene contestualmente delegata (qualora REFERENTE/subdelegata qualora DIRIGENTE/DIPENDENTE COORD.) alla sottoscrizione, per conto del Titolare, delle autorizzazioni al trattamento dati personali dei Dirigenti-Dipendenti (od assimilati) di diretta afferenza ed autorizzata a subdelegare i Dirigenti di afferenza responsabili di struttura (S.C., SSD o SS) e/o Dipendenti del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa, alla sottoscrizione, per conto del Titolare, delle autorizzazioni al trattamento dati personali dei Dirigenti-Dipendenti (od assimilati) di loro diretta afferenza ed a sottoscrivere, sempre per conto del Titolare, la nomina dei responsabili esterni del trattamento (conferita o ricevuta da ASL3), che collaborano ai trattamenti della struttura-area di competenza, nonché degli accordi di contitolarità di afferenza (sulla base della competenza tecnico-economico-gestionale).

La presente autorizzazione ricomprende la designazione all'espletamento di **specifici compiti** infra precisati per la gestione del "Sistema privacy" nella struttura-area dalla S.V. diretta (oppure di afferenza della S.V. quale DIPENDENTE od assimilato).
Limitatamente all'area di competenza della Struttura-Area che Dirige e delle funzioni e competenze correlate, e/o nell'ambito ed in coerenza con le funzioni privacy specifiche del ruolo rico-

perto, la S.V., **quale REFERENTE/DIRIGENTE/DIPENDENTE (od assimilato) del sistema Privacy aziendale**, dovrà:

1. collaborare con il R.P.D. Aziendale e con il Titolare ed il Referente per l'attuazione delle prescrizioni in materia di privacy, con particolare riguardo a quelle previste per Dirigenti, Referenti e dipendenti (od assimilati) del sistema privacy aziendale;
2. **individuare se REFERENTE/DIRIGENTE o Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa,** *i dipendenti (o assimilati), afferenti alla struttura-area diretta-coordinata dalla S.V. da autorizzare al trattamento dei dati di competenza e sottoscrivere le relative autorizzazioni al trattamento dati personali e categorie particolari di dati personali* **per conto del Titolare, che all'uopo delega (o subdelega per il tramite del Direttore-Dirigente dell'are di afferenza), con il presente atto, la S.V. alla sottoscrizione stessa, fornendo a detti dipendenti (o assimilati) le necessarie istruzioni** circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza , con le modalità previste dal DPS aziendale. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché si dovrà vigilare, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni bisognerà anche verificare la permanente sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto procedere alla revoca delle stesse. La nomina ad autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassuntineo assegnati assegnati alla struttura-area, che effettuano trattamento dei dati;
3. **sottoscrivere, se REFERENTE/DIRIGENTE o Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa, la nomina dei responsabili esterni del trattamento che collaborano ai trattamenti della struttura-area (per competenza tecnico-economico-gestionale), conferita o ricevuta dal ASL3, nonché gli accordi di contitolarità di afferenza (per competenza tecnico-economico-gestionale), secondo le procedure, tempistiche e modalità previste dal D.P.S., per conto del Titolare, che all'uopo delega (o subdelega per il tramite del Direttore-Dirigente dell'are di afferenza) la S.V. alla sottoscrizione stessa con il presente atto, fornendo a detti responsabili esterni e contitolari le necessarie istruzioni** circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, vigilando sull'osservanza delle stesse e della normativa in materia, anche attraverso **audit e controlli periodici** ed aggiornando in punto il R.P.D. e la S.C. Affari Generali**;**
4. *garantire,* **se REFERENTE/DIRIGENTE (e collaborare con il dirigente se DIPENDENTE od assimilato),** per la parte di competenza della struttura-area diretta, *l'*implementazione e/o aggiornamento costante e tempestivo dei contenuti del "registro dei trattamenti" e dei format afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto con le modalità previste dal D.P.S. aziendale e dalla vigente normativa, con le modalità ivi previste, che confermano la responsabilità di detta attività in capo ai Dirigenti/Direttori responsabili delle strutture-aree di afferenza. Pertanto dette attività rimangono sotto esclusiva responsabilità (compresa redazione, aggiornamento, conservazione e pubblicità) dei Dirigenti/Direttori responsabili delle singole strutture-aree aziendali , per gli ambiti di rispettiva competenza) e del Titolare, tenendo il R.P.D. solo in copia informatizzata quanto da detti Dirigenti/Direttori trasmessogli;

5. *concorrere alla definizione di misure idonee a prevenire il rischio di violazione privacy, alla valutazione del rischio di violazione privacy e monitoraggio del sistema privacy per la struttura-area diretta-coordinata o di afferenza ed a controllare, qualora* **REFERENTE/*DIRIGENTE*** *o* **Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa,** *il rispetto da parte dei dipendenti (o assimilati) della struttura-area stessa delle suddette misure, coordinandosi con il referente di area ed il R.P.D.;*
6. *provvedere al monitoraggio delle attività svolte nella struttura-area con particolare attenzione a quelle nell'ambito delle quali è più elevato il rischio privacy;*
7. *fornire le informazioni richieste dal R.P.D. a seguito dell'individuazione delle attività nell'ambito delle quali è più elevato il rischio di violazione privacy e formulare specifiche proposte volte alla prevenzione del rischio medesimo;*
8. **curare il processo della gestione del rischio nella struttura-area diretta-coordinata ed il suo aggiornamento, attraverso un'attività di analisi meditata e partecipativa o collaborare a tal fine con il REFERENTE/DIRIGENTE – Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa se DIPENDENTE od assimilato;**
9. **individuare un proprio facilitatore della prevenzione del rischio privacy come previsto dal D.P.S. aziendale se REFERENTE/DIRIGENTE;**
10. **verificare la presenza, la correttezza, la completezza, l'aggiornamento, la semplicità di consultazione, l'omogeneità di tutte le informazioni ed i dati della struttura-area, necessarie per la concreta applicazione delle misure di prevenzione del rischio in materia privacy;**
11. **accertare che l'aggiornamento e trasmissione dei dati al R.P.D. avvenga secondo la procedura e le tempistiche prevista nel D.P.S. aziendale se REFERENTE/DIRIGENTE o Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa o collaborare con loro a tal fine se DIPENDENTE od assimilato;**
12. garantire un adeguato sostegno ai Referenti riguardo a tutti i compiti loro assegnati, sulla prevenzione del rischio, come indicato nel D.P.S. Aziendale;
13. trasmettere tempestivamente (e comunque entro 15 giorni dalla variazione) al Referente (se DIRIGENTE) ed al R.P.D. e per conoscenza alla S.C. Affari Generali i dati di gestione del rischio privacy della propria struttura-area ed i relativi aggiornamenti **se REFERENTE/DIRIGENTE**;
14. **promuovere ed accertare la conoscenza della normativa privacy e del D.P.S. aziendale, da parte del proprio personale, se REFERENTE/DIRIGENTE o Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa, relazionando il Referente di area ed il R.P.D. sulle criticità accertate;**
15. Collaborare con il Referente (se DIRIGENTE) ed il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati ed ulteriori esercizi di diritti su istanza dall'interessato ai sensi del Regolamento UE 679/2016 e norme di armonizzazione;
16. presentare al Referente (se DIRIGENTE) e, per conoscenza al R.P.D ed alla S.C. Affari Generali, ogni richiesta di valutazione di impatto preventiva al trattamento dei dati sensibili (quando necessaria) da inviare eventualmente al Garante e collaborare con detti soggetti per la sua effettuazione;
17. In caso di violazione di dati personali di cui si sia venuti a conoscenza, segnalare immediatamente, e comunque entro 24 ore, al referente e per conoscenza al R.P.D. (all'email dedicata rpd@asl3.liguria.it) ed alla S.C. Affari Generali (e mail segreteria.contratticonvenzioni@asl3.liguria.it) qualsiasi violazione privacy in cui ritenga

probabile che per tale violazione vi siano rischi per i diritti e le libertà degli interessati, con le modalità previste dal D.P.S. aziendale e dalla normativa vigente;

18. Vigilare sull'attuazione da parte dei *dipendenti afferenti alla struttura-area diretta-coordinata,* **se REFERENTE/DIRIGENTE o Dipendente del Comparto con funzioni di Coordinamento-Responsabilità Organizzativa***,* degli obblighi di informazione ed acquisizione del consenso, quando richiesto dalla normativa vigente, nei confronti dell'interessato, secondo i formati e le modalità previste nel D.P.S. aziendale e policy aziendali attuative e sull'adozione delle cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari)".

Il Titolare/Il delegato/Il sub delegato alla firma del Titolare

Dott/Sig.

Ricevo copia della presente autorizzazione e correlate deleghe-subdeleghe[1] alla sottoscrizione di autorizzazioni per conto del Titolare ed a sottoscrivere per conto del Titolare la nomina dei responsabili esterni del trattamento che collaborano ai trattamenti della struttura-area di competenza e gli accordi di contitolarità (effettuati o ricevuti dal ASL3)[1], che consta di n. ……pagine. Presane completa visione, accetto formalmente, con la sottoscrizione, dette deleghe-subdeleghe alla sottoscrizione.

IL DIRIGENTE/DIRETTORE
DIPARTIMENTO/DIPENDENTE COORD/TIROCINANTE
S.C./SSD/STR ASS ……..
Dott./Sig.

[1] **Le deleghe-subdeleghe non sono previste per tirocinanti e figure assimilate**

Allegato alla nomina ad autorizzato al trattamento dei dati personali ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione:

INFORMAZIONI, MISURE DI SICUREZZA ED ISTRUZIONI OPERATIVE

Il Regolamento Europeo 679/2016 e norme di armonizzazione prevedono precisi obblighi per coloro che intendono procedere ad un trattamento di dati personali.

Tali obblighi si sostanziano in adempimenti dettagliati, omessi i quali scattano le sanzioni sia penali, sia amministrative, sia civili, poste a salvaguardia dei diritti tutelati.

La normativa in materia di protezione dei dati personali in oggetto individua tre figure fondamentali:

1. Il Titolare del trattamento;
2. Il Responsabile esterno del trattamento;
3. Gli autorizzati al trattamento
4. Il Responsabile per la Protezione dei Dati (R.P.D.).

Il **Titolare del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed 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 od i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.. E' Responsabile dell'attuazione dei precetti normativi previsti dalla Legge.

Il Titolare del trattamento è la A.S.L. 3.

Il **Responsabile esterno del trattamento,** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. E' designato dal Titolare, in persona del legale rappresentante pro tempore, anche tramite delega alla sottoscrizione, e deve provvedere all'applicazione di tutti i compiti impartiti dal Titolare, nonché fornire, agli autorizzati al trattamento istruzioni in merito alle operazioni di raccolta e trattamento dei dati, nonché vigilare sulla corretta applicazione delle medesime.

L'**autorizzato al trattamento**, nominato dal Titolare, anche tramite delega alla sottoscrizione, deve elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite.

All'autorizzato del trattamento sono devoluti compiti**, anche specifici**, volti a garantire una puntuale applicazione della vigente normativa in materia di protezione dei dati.

Sulla base di quanto sopra, si rende necessario provvedere all'individuazione dei soggetti autorizzati del trattamento, onde garantire la puntuale ed ottimale applicazione del Regolamento Europeo 679/2016 e norme di armonizzazione.

Gli autorizzati al trattamento assumono la responsabilità di tutti i dati trattati per lo svolgimento delle mansioni loro assegnate all'interno del servizio di appartenenza in merito all'applicazione delle disposizioni relative alla tutela dei dati personali, nonché alla loro gestione, trattamento e custodia, secondo le indicazioni impartite dal Titolare, anche per il tramite dei Dirigenti/Direttori responsabili delle strutture di afferenza, designati questi ultimi allo svolgimento di specifici compiti nell'ambito del "sistema privacy" aziendale per l'ambito di competenza della struttura-area dagli stessi diretta.

Dell'espletamento di tali funzioni **rispondono direttamente e personalmente al Titolare**, anche per il tramite dei Dirigenti/Direttori responsabili delle strutture di afferenza.

Il Responsabile per la Protezione dei dati Personali (R.P.D.): è una figura obbligatoria prevista dal Regolamento U.E. 679/2016 e norme di armonizzazione, che sovraintende a tutte

le attività di protezione dei dati e che costituisce il soggetto di raccordo con l'autorità di controllo (Autorità garante per la Protezione dei dati) e con gli interessati/utenti.

Questa comunicazione è l'allegato dell'atto formale di nomina della S.V. ad autorizzato al trattamento dei dati personali nell'ambito del servizio cui si è preposti e/o assegnati.

Tale nomina è in relazione alle operazioni di trattamento dei dati personali ai quali la S.V. ha accesso nell'espletamento delle funzioni proprie e presuppone la conoscenza degli obblighi di legge in materia e l'impegno a trattare i dati personali nel pieno rispetto di tali obblighi e delle istruzioni che vengono qui di seguito impartite.

A tal fine, si ricorda che per trattamento si intende " 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".

Si fa presente che, per quanto riguarda il trattamento dei dati personali, lo stesso si considera lecito se ricorre almeno una delle seguenti condizioni (art. 6 comma 1 Regolamento Europeo 679/2016 e norme di armonizzazione):

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, salvi i casi in cui non è richiesto ai sensi della medesima normativa (tra gli altri art.9.2 Regolamento UE n.679/2016) e disposizioni di armonizzazione;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Gli autorizzati possono trattare i dati personali soltanto se designati ed istruiti formalmente da ASL3 ancorchè, nell'ambito della sfera di competenza e dei connessi trattamenti, comprensivi dell' accesso alle relative banche dati, siano dotati di autonomia gestionale ed organizzativa.

Essi sono tenuti a:

1. rispettare e garantire, relativamente ai trattamenti assegnati, l'applicazione delle norme in materia di protezione delle informazioni, delle linee guida in materia di riservatezza dei dati, ed inerenti l'amministrazione digitale ovvero previste nella policy privacy e/o nel D.P.S. aziendale;
2. rispettare e garantire, relativamente ai trattamenti assegnati, l'applicazione delle misure di sicurezza previste nel Registro dei trattamenti, adottando ogni misura necessaria, con particolare attenzione all'erogazione di prestazioni e servizi sanitari ;

3. trattare i dati alla luce dei principi di cui all' art.5 del Regolamento UE n.679/2016 e norme di armonizzazione nazionali, regionali e/o policy e D.P.S. aziendali ed in particolare secondo il criterio di indispensabilità , per il solo tempo necessario al ricovero /all' erogazione di prestazioni /cura / terapia ed attività correlate;
4. vigilare :
   a. su eventuali altri autorizzati, sottoposti alla propria autorità (se Referenti, Dirigenti o Dipendenti con coordinamento nel "Sistema privacy" aziendale), affinchè applichino pari principi e rispettino il diritto degli interessati ad essere informati, a manifestare liberamente il proprio consenso, e ad esercitare il diritto di oscuramento sui singoli documenti ;
   b. sul corretto uso di sistemi e procedure digitali utilizzati dai sottoposti per gestire i dati necessari all'attività lavorativa;
5. mettere a disposizione dell'azienda tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di legge e contribuire alle attività di revisione, comprese le verifiche / audit, da questa effettuate;
6. verificare :

   a) che la documentazione cartacea e digitale e le procedure informatizzate, a supporto dell'attività di trattamento dati di propria competenza, rispondano ai principi di necessità, pertinenza e non eccedenza;

   b) periodicamente, l'esattezza e l'aggiornamento dei dati personali, nonché la loro pertinenza, completezza, non eccedenza e necessità, rispetto ai fini perseguiti, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa;

7. collaborare con il RPD aziendale comunicando:
   a) i dati e le informazioni necessarie per valutare le richieste avanzate dagli interessati, con particolare riferimento all'esercizio dei diritti, all'accesso ai propri dati, alla revoca dei consensi, etc.;
   b) le misure organizzative adottate ovvero le istruzioni interne e le indicazioni di comportamento per il proprio personale, per i pazienti e per i visitatori (ad es.se Referenti, Dirigenti o Dipendenti con coordinamento nel sistema privacy aziendale) ;
   c) che un'istruzione ricevuta viola il presente regolamento o altre disposizioni vigenti relative alla protezione dei dati personali, ovvero eventuali difficoltà emerse nell'applicazione di norme e procedure , utilizzando e- mail appositamente predisposta,
   d) periodicamente in merito allo svolgimento dei compiti specifici assegnati, inclusa ogni problematica ad essi riferita;
   e) l'inizio o la cessazione di trattamenti di dati personali, aggiornando anche il Registro delle attività di trattamento dei dati personali;
8. redigere (se Referenti, Dirigenti nel "Sistema privacy" aziendale) il registro dei trattamenti svolti nella propria struttura-area di competenza, i suoi aggiornamenti tempestivi ed il censimento delle procedure e delle banche dati utilizzate, tenendone informata la direzione aziendale ed il RPD aziendale ;
9. sottoscrivere ed aggiornare costantemente, sulla base delle deleghe o subdeleghe di sottoscrizione ricevute dal Titolare (se Referenti, Dirigenti nel "Sistema privacy" aziendale o Dipendenti con coordinamento nel "sistema privacy aziendale") le designazioni, per iscritto, degli operatori che agiscono sotto la propria direzione, ad autorizzati del trattamento, secondo livelli differenziati e profili omogenei ed avendo cura di individuare compiti e mansioni cui sono adibiti al fine di formulare correttamente le istruzioni da impartire per trattare i dati;

10. tenere la documentazione delle designazioni sottoscritte ed aggiornarla, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento dei sottoposti. La documentazione delle designazioni sottoscritte ed aggiornate, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento, deve essere conservata sotto la responsabilità del Dirigente-responsabile, presso la struttura-area diretta e presso quella di assegnazione dell'autorizzato e, per quanto possibile, correlata dal Dirigente-responsabile stesso al registro dei trattamenti di afferenza della struttura-area, e pubblicata sul sito intranet aziendale nella specifica cartella condivisa (Normativa/Privacy/Registro Trattamenti/Politiche Privacy) nonchè messa a disposizione di RPD aziendale e S.C. Affari Generali, su loro richiesta;
11. custodire gli atti di cui ai punti 9 e 10 in apposito contenitore e/o cartella informatizzata da esibire in caso di verifica interna ovvero di ispezione del Garante;
12. curare (se Referenti, Dirigenti o Dipendenti con coordinamento nel sistema privacy aziendale), fra gli autorizzati al trattamento sottoposti alla propria autorità, la diffusione di norme, linee guida e di ogni altra disposizione impartita dall'Azienda anche organizzando la formazione di reparto/ dipartimento mirata all'aggiornamento continuo ed obbligatorio in materia di privacy, previsto per legge
13. designare un Facilitatore (se Referenti, Dirigenti) con finalità di supporto indicandone il nominativo al RPD, come previsto dal D.P.S. aziendale
14. rispondere al Titolare, secondo le vigente normative contrattuali, di ogni violazione o mancata attivazione di quanto previsto dal sistema privacy aziendale e dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale, per gli ambiti di rispettiva competenza.

Le persone fisiche che, nelle singole Strutture, svolgono materialmente le operazioni di trattamento dati devono essere designate in tal senso come "DIPENDENTI (o assimilati) autorizzati al trattamento dati" dal Titolare (con esercizio di delega alla sottoscrizione ricevuta dal Referente/Dirigente/Dipendente con coordinamento competente ad individuarli). Sono da designare Autorizzati i dipendenti dell'azienda ed i collaboratori che, a qualsiasi titolo, prestano la loro opera, anche in via temporanea, all'interno delle strutture aziendali e, pertanto, assimilati ai Dipendenti nel "Sistema privacy" aziendale (ad esempio: tirocinanti, studenti, stagisti, volontari, liberi professionisti, borsisti, consulenti, lavoratori interinali) o che, comunque, agiscono sotto l' autorità dell' Azienda .

Per la designazione scritta è utilizzata apposita modulistica, da produrre, caso per caso, elaborata anche in ragione di compiti e funzioni proprie di determinate categorie, secondo il format previsto dal D.P.S. aziendale.

Essa prevede:

- ✓ la data di inizio ed eventuale termine dell' attività all'interno della struttura e/o il riferimento al rapporto che lega la persona all'Azienda
- ✓ in modo sintetico, i trattamenti dati autorizzati , le banche dati e le procedure informatizzate cui si ha accesso in ragione del profilo e delle mansioni assegnate, anche per relationem in riferimento al rapporto che lega la persona all'Azienda
- ✓ specifiche e dettagliate istruzioni operative, riguardo alle corrette modalità di trattamento dati, in ragione del profilo ricoperto ,dell' attività svolta, delle funzioni e delle competenze attribuite con particolare riguardo alle misure di sicurezza da osservare.

Gli Autorizzati possono accedere ai soli dati indispensabili per assolvere alle attività istituzionali cui sono preposti che e debbono trattare in conformità alla vigente normativa, alla presente policy, al D.P.S. aziendale ed alle disposizioni impartite dal Referente/Dirigente /Dipendente con coordinamento del "Sistema privacy" di afferenza.

Essi sono tenuti a :

- ✓ comunicare dati personali e/o sensibili agli altri soggetti autorizzati al trattamento solo in caso di necessità, ovvero quando non sia possibile perseguire gli stessi fini con dati anonimi o aggregati
- ✓ conservare i dati personali sia su supporto analogico che digitale solo per il tempo previsto dalla normativa vigente e successivamente devono sottoporli a scarto d'archivio o distruzione
- ✓ non permettere il trattamento dei dati personali che, anche a seguito di verifica, risulti eccedente, non pertinente ovvero non necessario, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene
- ✓ trattare i dati osservando le istruzioni ricevute, anche con riferimento agli aspetti relativi alla sicurezza
- ✓ qualora trattino dati con l'ausilio di strumenti informatici sono personalmente responsabili della gestione riservata della password loro assegnata, con divieto di cederla a terzi ovvero a colleghi
- ✓ sono responsabili della custodia riservata dei documenti cartacei loro affidati per effettuare le operazioni di trattamento con l' onere di restituirli e conservarli al termine dell'attività / orario di lavoro
- ✓ sono responsabili di ogni attività sui dati inerente/ derivate dall' attività di servizio.

L'atto di designazione ad Autorizzato costituisce l'unico presupposto di liceità per il trattamento dei dati personali.

L'originale di tale atto, controfirmato per presa visione dall'autorizzato ed aggiornato, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento, deve essere conservata sotto la responsabilità del Dirigente-responsabile, presso la struttura-area diretta e presso quella di assegnazione dell'autorizzato e, per quanto possibile, correlata dal Dirigente-responsabile stesso al registro dei trattamenti di afferenza della struttura-area, e pubblicata sul sito intranet aziendale nella specifica cartella condivisa (Normativa/Privacy/Registro Trattamenti/Politiche Privacy) nonchè messa a disposizione di RPD aziendale e S.C. Affari Generali, su loro richiesta.

In ottemperanza al Regolamento Europeo 679/2016 e norme di armonizzazione, che regolano il trattamento dei dati personali ed in relazione alla presente designazione , la S.V. è autorizzata, pertanto, a trattare i dati personali *(qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale)* ed i dati c.d. "particolari" (che il D. Lgs. 196/2003 e s.m.i definiva quali"dati sensibili" e richiamati dall'art.9 del Regolamento Europeo 2016/679), *cioè i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche,*

le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona in modo lecito, corretto e trasparente e nel rispetto dei principi sanciti dal Regolamento UE 679/2016 e norme di armonizzazione ed, in particolare, come detto infra:

a) a raccoglierli e registrarli per finalità determinate, esplicite e legittime, e successivamente a trattarli in modo che non siano incompatibili con tali finalità;
b) a verificare, ove possibile, la loro esattezza e, se necessario, aggiornarli;
c) a verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare;
d) a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte in Azienda. In ogni operazione di trattamento andrà garantita la massima riservatezza;
e) a osservare scrupolosamente tutte le misure di sicurezza predisposte in Azienda, o che verranno comunicate in seguito dal Titolare o dal R.P.D.. aziendale, anche per il tramite dei Dirigenti responsabili della struttura-area di afferenza, nonché le previsioni del D.P.S. aziendale e policy aziendali attuative.

Nell'espletamento del proprio incarico la S.V. dovrà, in relazione agli obblighi correlati allo stesso, attenersi, tra l'altro, alle seguenti istruzioni:

1. collaborare col Titolare al fine di consentire di catalogare analiticamente le banche dati (sia informatiche sia basate su supporti tradizionali) all'interno del servizio di appartenenza, comunicando tutte quelle presenti all'interno dello stesso, con le modalità previste dal D.P.S. aziendale e policy aziendali attuative;
2. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto dalla normativa vigente, nei confronti dell'interessato, secondo i formati e le modalità previste nel D.P.S. aziendale e policy aziendali attuative;
3. *garantire,* **se REFERENTE/DIRIGENTE (e collaborare con il dirigente se DIPENDENTE od assimilato),** per la parte di competenza della struttura-area diretta, l'implementazione e/o aggiornamento costante e tempestivo dei contenuti del "registro dei trattamenti" e dei format afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto con le modalità previste dal D.P.S. aziendale e dalla vigente normativa, che confermano la responsabilità di detta attività in capo ai Dirigenti/Direttori responsabili delle strutture di afferenza. Pertanto dette attività rimangono sotto esclusiva responsabilità (compresa redazione, aggiornamento, conservazione e pubblicità) dei Dirigenti/Direttori responsabili delle singole strutture aziendali , per gli ambiti di rispettiva competenza) e del Titolare, tenendo il R.P.D. solo in copia informatizzata quanto da detti Dirigenti/Direttori trasmessogli;
4. presentare al Referente ed al Dirigente/Direttore di riferimento e , per conoscenza (o direttamente se REFERENTE) al R.P.D ed alla S.C. Affari Generali, ogni richiesta di valutazione di impatto preventiva al trattamento dei dati sensibili (quando necessaria) da inviare eventualmente al Garante e collaborare con detti soggetti per la sua effettuazione;

5. collaborare (anche per il tramite del proprio tutor, se tirocinante o figura assimilata) con il R.P.D. Aziendale e con il Titolare ed il Referente ed il Dirigente/Direttore di riferimento per l'attuazione delle prescrizioni in materia di privacy;
6. attuare le misure di sicurezza informatiche e non informatiche idonee a rispettare le indicazioni del Regolamento Europeo 679/2016 e norme di armonizzazione , nonché il D.P.S. e le policy aziendali;
7. comunicare tempestivamente, con le modalità ed i tempi stabiliti dal D.P.S. aziendale e dalle policy aziendali (anche per il tramite del proprio tutor, se tirocinante o figura assimilata) al Referente ed al Dirigente/Direttore di riferimento e , per conoscenza (o direttamente se REFERENTE) al R.P.D ed alla S.C. Affari Generali, ogni violazione privacy, difficoltà o irregolarità delle procedure di applicazione e collaborare con gli stessi per i correlati adempimenti di competenza;
8. accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
9. conservare gli atti e documenti, contenenti dati personali utilizzati per lo svolgimento dei compiti propri, in contenitori muniti di serratura (cassetti, armadi, ecc.) e restituirli al termine delle operazioni affidate. Sulla base di quanto sopra, in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'autorizzato dovrà verificare che non vi sia la possibilità da parte di terzi, anche dipendenti, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
10. Le riproduzioni di documenti contenenti dati personali da eliminare durante le operazioni di trattamento non devono essere lasciate incustodite sia in caso di allontanamento temporaneo dalla stazione di lavoro sia al termine della giornata qualora il trattamento non sia ancora terminato e devono essere distrutte con modalità tali da non rendere intellegibili i dati personali ivi riprodotti;
11. testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative volte a garantire la sicurezza dei trattamenti espletati, espletando e/o partecipando anche a sistematiche attività di audit;
12. partecipare alle attività formative aziendali in materia di privacy ed all'attività di auditing in materia;
13. in caso di utilizzo di strumento elettronico, lo stesso non dovrà mai essere lasciato incustodito e accessibile durante una sessione di trattamento. In particolare si ricorda che anche in caso di abbandono temporaneo della postazione di lavoro, il personal computer con il quale si sta operando un'operazione di trattamento dei dati dovrà essere spento, dopo aver effettuato il salvataggio dei dati oppure dovrà essere attivato lo screensaver con inserimento di password personale al fine di evitare la riapertura a terzi della sezione di trattamento in corso;
14. Sempre in caso di utilizzo di strumento elettronico, nel caso di informazioni memorizzate sulle memorie locali dei personal computer e affidate esclusivamente agli utenti, effettuare il salvataggio dei dati con cadenza almeno settimanale;
15. Qualora il trattamento dei dati, la formazione e la comunicazione di documenti ed atti, avvenga con strumenti elettronici dovranno essere accuratamente applicate, tra le altre, le seguenti misure di sicurezza:
    a) dovranno essere predisposte tutte le cautele necessarie per assicurare la segretezza della componente riservata della credenziale di autenticazione (codice

associato a parola chiave o dispositivo di autenticazione conosciuto o in possesso e uso esclusivo dell'autorizzato);

b) la password personale dovrà essere modificata ogni tre mesi e ogni qualvolta l'autorizzato al trattamento abbia motivo di ritenere che non sia di sua esclusiva conoscenza;
c) i supporti rimovibili (floppy disk, cd rom, chiavette USB, ecc.) su cui sono memorizzati copie di dati dovranno essere custoditi in appositi contenitori muniti di serratura (armadi, cassetti, ecc.), al fine di evitare accessi non autorizzati e trattamenti non consentiti o comunque custoditi in locali ad accessi autorizzati e chiusi a chiave;
d) i supporti rimovibili contenenti dati sensibili, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri autorizzati solo se le informazioni precedentemente in essi contenute non sono intelligibili e in nessun modo tecnicamente ricostruibili;

16. Sempre allo scopo di conformarsi alle disposizioni in materia di privacy e a quanto contenuto nel Documento Programmatico sulla Sicurezza aziendale (D.P.S.) aziendale, si indica la procedura che viene utilizzata per consentire operazioni di trattamento dei dati in caso di prolungata assenza o di impedimento dell'autorizzato e/o qualora si renda indispensabile ed indifferibile l'accesso allo strumento elettronico per esclusive necessità di operatività e sicurezza del sistema informatico. Tale procedura prevede che la Struttura Complessa Sistemi Informativi Aziendali, attraverso i propri amministratori di sistema ed a seguito di richiesta scritta del Direttore della Struttura/Dipartimento (o suo sostituto) cui afferisce o dal Direttore della Direzione Strategica dell'area di afferenza, nel caso di documentata necessità di accedere ai dati gestiti da un autorizzato, è in grado di rimuovere la password di quell'utente, generandone una nuova che viene consegnata al Direttore della Struttura (o suo sostituto) esclusivamente per effettuare l'accesso straordinario. In ogni caso, gli amministratori di sistema non possono utilizzare la password originale dell'utente in sua vece. L'accesso straordinario sarà, quindi, effettuato, dopo la rimozione delle credenziali dell'utente, con nuove credenziali. Di detta procedura sarà tenuto uno specifico verbale che dovrà essere conservato presso la struttura nella quale si è reso necessario l'accesso. Il Direttore che ha richiesto la procedura di accesso straordinario è tenuto ad avvertire tempestivamente l'autorizzato che è stata attivata la procedura di generazione di nuove credenziali d'accesso.
    In ogni caso l'autorizzato non potrà più utilizzare le precedenti credenziali e per accedere al sistema dovrà richiederne di nuove.

17. Rispettare le modalità di utilizzo di posta elettronica ed internet (disposte nel vigente Regolamento pubblicato nel sito intranet aziendale sezione "Normativa/Privacy").

18. Collaborare con il Referente, il Dirigente/Direttore di riferimento ed il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati ed ulteriori esercizi di diritti su istanza dall'interessato ai sensi del Regolamento UE 679/2016 e norme di armonizzazione.
19. Procedere all'individuazione di eventuali dipendenti (o assimilati), sotto propria responsabilità di struttura-area, se Dirigente o Dipendente con coordinamento o responsabilità organizzativa, da autorizzarsi al trattamento dei dati personali o di cate-

gorie particolari di dati personali e sottoscriverne per delega/subdelega di firma del Titolare la nomina, completa di specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, utilizzando i modelli allegati al D.P.S. aziendale. La documentazione delle designazioni sottoscritte ed aggiornate, ogni qual volta si renda necessario per avvicendamento / sostituzione/ trasferimento, deve essere conservata sotto la responsabilità del Dirigente-responsabile, presso la struttura-area diretta e presso quella di assegnazione dell'autorizzato e, per quanto possibile, correlata dal Dirigente-responsabile stesso al registro dei trattamenti di afferenza della struttura-area, e pubblicata sul sito intranet aziendale nella specifica cartella condivisa (Normativa/Privacy/Registro Trattamenti/Politiche Privacy) nonchè messa a disposizione di RPD aziendale e S.C. Affari Generali, su loro richiesta. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché si dovrà vigilare, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni bisognerà anche verificare la permanente sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto procedere alla revoca delle stesse. La nomina ad autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti assegnati alla struttura-area, che effettuano trattamento dei dati;

20. **In caso di designazione di responsabili esterni del trattamento che collaborano ai trattamenti della struttura-area di afferenza (per competenza tecnico-economico – gestionale), secondo le procedure, tempistiche e modalità previste dal D.P.S., e/o di accordi di contitolarità, per conto del Titolare, che all'uopo abbia delegato la S.V. alla sottoscrizione stessa, fornire a detti responsabili esterni/contitolari le necessarie istruzioni** circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, vigilando sull'osservanza delle stesse e della normativa in materia, **anche con periodici e sistematici audit e controlli**, **ed aggiornando in punto il R.P.D. e la S.C. Affari Generali;**
21. Adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitu; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari).

La S.C. Sistemi Informativi Aziendali esegue le incombenze di salvataggio dei dati per le applicazioni di rilevanza aziendale quali:

- le applicazioni transattive i cui dati risiedono sui server del Centro Elaborazione Dati;
- i file (documenti, fogli di calcolo, etc.) che risiedono sulle cartelle condivise e intestate alle Strutture e ai Dipartimenti.

Per quanto concerne la gestione degli archivi cartacei (archivio clinico, etc.) dovranno essere adottate le seguenti misure di sicurezza:

1. Tutti i documenti dovranno essere accuratamente custoditi all'interno degli appositi locali o contenitori amovibili muniti di serratura;
2. L'accesso all'interno degli archivi dovrà essere rigorosamente limitato alle persone autorizzate dal responsabile ed addette a tale attività;
3. È vietato allontanarsi dagli archivi, dalla segreteria e dagli uffici lasciando i locali incustoditi;
4. Gli atti ed i documenti contenenti dati personali, utilizzati per lo svolgimento dei compiti propri devono essere conservati accuratamente in contenitori e/o locali muniti di serratura e restituiti al termine delle operazioni affidate;
5. Le riproduzioni di documenti contenenti dati personali da eliminare durante le operazioni di trattamento non devono essere lasciate incustodite sia in caso di allontanamento temporaneo dalla stazione di lavoro sia al termine della giornata qualora il trattamento non sia ancora terminato e devono essere distrutte con modalità tali da non rendere intellegibili i dati personali ivi riprodotti;
6. Nessun dato potrà essere comunicato a terzi o diffuso senza la specifica autorizzazione del Titolare;
7. E' comunque vietata la diffusione dei dati inerenti lo stato di salute e la vita sessuale degli interessati;
8. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

E' fatto assoluto divieto di comunicare, diffondere, utilizzare i dati personali provenienti da banche dati aziendali, in assenza dell'autorizzazione del Titolare.

Nel formalizzarLe l'assegnazione del ruolo di autorizzato al trattamento dei dati è fondamentale precisare l'importanza e la responsabilità che tale ruolo comporta all'interno dell'applicazione della normativa vigente in materia di privacy. Infatti Le ricordo che tale normativa prevede gravi sanzioni in caso di illecito trattamento dei dati, variabili, secondo la tipologia e la gravità.

Per ogni difficoltà o per qualsiasi chiarimento la S.V. potrà rivolgersi allo scrivente e/o al Titolare e/o al R.P.D. aziendale che sono disponibili per ogni eventuale ulteriore delucidazione in merito.

Il Titolare/Il delegato/Il sub delegato alla firma del Titolare
Dott./Sig……

ALLEGATO B: ***NOMINA RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI***

AI SENSI DELL´ART. 28 REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

ASL3 , con sede in GENOVA, via Bertani n.4, in qualità di Titolare del trattamento dati personali e particolari relativi ai propri interessati/utenti, in persona del dott…… , delegato alla firma dal Titolare Direttore Generale pro tempore, (di seguito **TITOLARE/AZIENDA**)

PREMESSO CHE

a) .....come da contratto/convenzione adottato con deliberazione ASL3 n……..del…… ;
b) [**********] necessita dei dati strettamente necessari e specificamente indicati relativamente alle finalità ed attività di trattamento relative al servizio di ……., meglio appresso identificate, comprese le correlate attività amministrativo contabili;
c) L'Azienda, quale Titolare di tali dati, è necessitata a conferirli, al fine di consentire la corretta erogazione del servizio;
d) ASL3 ha accertato che [**********] è in grado di fornire, per esperienza, capacità ed affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela della privacy e protezione dei dati, ivi compresi gli aspetti relativi alla sicurezza, in modo tale che il trattamento svolto per conto del Titolare sia conforme alla normativa in materia di protezione dei dati personali e garantisca, nell'organizzazione dei servizi resi, il rispetto delle libertà fondamentali e della dignità degli interessati;

Designa

[**********], con sede ……., …….. - Partita I.V.A. ……Codice fiscale: …….. nella persona del Rappresentante Legale pro tempore, …… (di seguito **RESPONSABILE) ,**Responsabile del trattamento dei dati personali e categorie particolari di dati personali degli interessati/utenti, effettuato in forza dello stesso rapporto contrattuale/convenzionale, se necessari ed indispensabili, a dar corso allo stesso, secondo le istruzioni di seguito riportate.

1. Premesse

Le premesse costituiscono parte integrante e sostanziale del presente incarico.

2. Definizioni

Ai fini del presente incarico per Titolare del Trattamento si intende 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.

Ai fini del presente incarico per Responsabile del Trattamento si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.

3. Oggetto

L'oggetto della presente designazione è il conferimento da parte dell'Azienda a [**********] dell'incarico di Responsabile del Trattamento ai sensi e per gli effetti dell'art. 28 del Regolamento UE 2016/679 Regolamento Generale per la protezione dei dati (in seguito "Regolamento") e norme di armonizzazione. La presente designazione individua inoltre la materia disciplinata, la durata, la natura e la fi-

nalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento. Specifica le istruzioni a cui il Responsabile deve attenersi nello svolgimento dei compiti ad esso affidati.

Con la sottoscrizione della presente designazione [**********] accetta l'incarico di Responsabile del Trattamento, senza corrispettivo, riserva o eccezione alcuna alle condizioni di seguito riportate.

Ciascuna parte è esclusivamente responsabile per il proprio rispetto delle disposizioni di legge applicabili in materia di protezione dei dati personali.

4. Natura e finalità del trattamento

Nell'ambito del rapporto sostanziale di cui in premessa, [**********] eroga un servizio di ……..., (eventualmente comprese le correlate attività amministrativo contabili), finalizzato ……..(eventualmente mediante l'applicazione ……..per la gestione di……..).

Il trattamento è finalizzato esclusivamente a…….

L'acquisizione dei dati personali (ed eventualmente particolari ex art.9 RGPD) è pertanto strettamente necessaria per il conseguimento delle predette finalità.

Nell'ambito delle proprie attività, [**********] tratta i dati di ……

La natura del trattamento è pertanto ……. e prevede i seguenti livelli di accesso e visualizzazione:

- ✓ ……..

(eventualmente "Il traffico da e verso l'applicazione ……. è cifrato tramite ……., supportato da un certificato …….. di una importante Certification Authority. Il backup avviene …….. ed è completo di tutto il materiale trattato, i documenti e il codice sorgente dell'applicazione….. I dati online e di backup sono anch'essi cifrati. Un firewall effettua costantemente un controllo del traffico avvisando il supporto in caso di attacchi o comportamenti illeciti).

5. Durata

La durata del presente incarico, efficace dalla data di sottoscrizione di entrambe le parti, è fissata dal contratto sostanziale richiamato in premessa la cui caducazione, anche per decorrenza termini, inficia la validità del presente incarico.

6. Tipo di dati personali

Le informazioni conferite e trattate rientrano nella definizione di "dato personale", di cui all'art. 4 par. 1 n.1 (quali a titolo esemplificativo nome, cognome, indirizzo e dati di contatto in generale, codice fiscale, coordinate bancarie od assimilabili), (eventualmente di "dato relativo alla salute", di cui al par. 1 n. 15, e nell'ambito dell'art. 9, nonché dati relativi a condanne penali e reati di cui all'art.10 del Regolamento Europeo e possono altresì riguardare dati soggetti a maggior tutela quali previsti dalle disposizioni nazionali).

7. Categorie di interessati

Gli interessati sono …….. (eventualmente Tra gli interessati possono comparire anche minori e soggetti vulnerabili).

Non è consentito il trattamento di dati di altre persone fisiche al di fuori di quelle espressamente previste dalla presente designazione.

8. Obblighi del Responsabile

[**********] è tenuto a trattare i dati personali esclusivamente per erogare i servizi di cui al precedente articolo 4, nel rispetto di quanto disposto dalla normativa applicabile in materia di protezione dei dati personali, nonché nei termini delle istruzioni ricevute dal Titolare riportate nei successivi articoli e di ogni altra norma di legge ovvero indicazione scritta, nei limiti fissati dalle vigenti norme di settore ivi incluse quelle specifiche particolari attinenti la protezione di particolari categorie di dati.

La società, e per essa i suoi operatori, è tenuta a:

- ✓ non utilizzare, per nessun motivo, i dati conferiti o comunque di cui sia venuta a conoscenza in ragione dell'incarico per finalità diverse da quelle oggetto di incarico. Qualora senza autorizzazione dell'Azienda determini autonomamente le finalità e i mezzi del trattamento, è considerato Titolare del trattamento;
- ✓ attenersi, nel trattare i dati personali, anagrafici, particolari, al principio di indispensabilità, evitando di detenere, utilizzare o visualizzare informazioni eccedenti rispetto all'attività concordata;
- ✓ non trattare i dati dell'interessato/utente oltre al tempo strettamente necessario ad espletare le citate attività;
- ✓ informare l'Azienda sulle modalità utilizzate per conservare i dati ed in particolare sulle modalità utilizzate per consentire l'identificazione dell'interessato/utente per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e/o successivamente trattati, avendo cura di applicare, in caso di conservazione digitalizzata, le norme vigenti in materia di sicurezza ivi incluse quelle previste per le banche dati;
- ✓ garantire l'aggiornamento normativo dei software e degli strumenti informatici relativi al servizio erogato di cui in premessa;
- ✓ (eventualmente garantire che l'applicazione …….. sia preconfigurata, in ossequio al già citato principio della "privacy per impostazione predefinita", riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, escludendone il trattamento quando le finalità perseguite possano essere realizzate mediante, rispettivamente, dati anonimi o modalità che permettano di identificare l'interessato solo in caso di necessità);
- ✓ ottemperare al divieto di trasferire dati personali verso un paese terzo extra UE o un'organizzazione internazionale ovvero con modalità elusive delle statuizioni vigenti in materia;
- ✓ garantire che le persone autorizzate al trattamento dei dati personali siano vincolate alla riservatezza o abbiano un adeguato obbligo legale in tal senso;
- ✓ adottare le misure di sicurezza richieste ai sensi dell'art. 32 del Regolamento (RGPD)come meglio descritto al successivo articolo 10;
- ✓ adottare, se previsto per legge, il Registro delle attività di trattamento ai sensi dell'art. 30 par. 2 del Regolamento;
- ✓ rispettare le condizioni previste dal Regolamento in caso di ricorso ad un altro Responsabile del trattamento, come meglio descritto al successivo articolo 12;
- ✓ adottare, tenendo conto della natura del trattamento stesso, misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di adempiere alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento ;
- ✓ garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 (con particolare riferimento all'art. 33, par. 2 "data breach") del Regolamento e norme di armonizzazione, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento, come meglio declinato all'art. 15;
- ✓ garantire la cancellazione o la restituzione di tutti i dati personali, al termine del rapporto sostanziale in essere ed in particolare la cancellazione delle copie esistenti, fatti salvi i termini

inerenti la conservazione per legge di particolari documenti che di norma andrebbero rimesse al Titolare;

- ✓ mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento, non espressamente richiamate;
- ✓ consentire e contribuire alle attività di revisione e verifica, anche sul posto, realizzate dal Titolare del trattamento o da soggetto da questi delegato;
- ✓ avvisare il titolare di eventuali incongruenze tra le richieste/procedure/sistemi gestiti e le disposizioni di legge vigenti, suggerendo correttivi idonei;

[**********]garantisce inoltre che i dati personali inerenti le attività poste in essere:

- ➢ non siano utilizzati in altre operazioni salvo per quelle i compatibili con gli scopi determinati, espliciti e legittimi sopra individuati, ed in ogni caso nei limiti in cui il trattamento sia necessario ad erogare il servizio;
- ➢ siano archiviati come sopra e comunque in una forma che ne consenta la cancellazione, la rettifica (nonché la conseguente notificazione agli eventuali destinatari a cui sono stati trasmessi i dati personali oggetti di richiesta di rettifica o cancellazione), nonché la limitazione o l'opposizione al relativo trattamento;
- ➢ siano conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati, fatto salvo quanto previsto in ordine alla cancellazione a norma dell'art.22;
- ➢ siano accessibili al solo personale autorizzato al trattamento dati in ragione dei diversi profili strettamente connessi alle mansioni svolte e per il solo tempo necessario all'erogazione dei servizi previsti dalla fornitura;
- ➢ non vengano adottati processi decisionali automatizzati e/o profilanti gli interessati.

9. Autorizzati al trattamento e rispetto della riservatezza

[**********] è altresì obbligata a:

- far sottoscrivere ai propri dipendenti o soggetti comunque sottoposti alla sua autorità, che trattano i dati oggetto di conferimento/conoscenza, un patto di riservatezza, individuando altresì, per ciascuno di essi, uno specifico ambito di trattamento dati collegato alle mansioni ricoperte ed in relazione alle funzioni attribuite per lo svolgimento del presente incarico;
- a produrre ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati dei pazienti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati;
- stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio incombente su diritti e libertà delle persona fisiche.

Di quanto precede, deve essere dato riscontro scritto al Titolare entro 60 giorni dalla sottoscrizione della presente designazione.

10. Misure di sicurezza

[**********] deve adottare preventivamente e mantenere, per tutta la durata della presente designazione, costantemente aggiornate misure di sicurezza tecniche ed organizzative idonee e/o che si rendano tali, in ragione del progresso tecnologico, al fine di contrastare i rischi che minacciano le informazioni oggetto di trattamento e di garantire un livello di sicurezza adeguato ai rischi individuati, quali – a titolo

esemplificativo e non esaustivo – i rischi di errore, di perdita, modifica, divulgazione ovvero accesso non autorizzato, accidentale o illegale, diffusione, cancellazione, distruzione o perdita accidentale dei dati trattati.

Tali misure comprendono, di norma, ed ove opportuno:

i) la capacità di assicurare la continua riservatezza, integrità, disponibilità dei dati e resilienza dei sistemi e dei servizi che trattano i dati personali;
ii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
iii) una procedura adeguata (messa a disposizione del Titolare su richiesta) per provare, verificare e valutare regolarmente l'efficacia delle misure adottate al fine di garantire la sicurezza del trattamento (con particolare riguardo alla gestione delle credenziali di accesso di tutti gli operatori della [**********] e degli utenti registrati ai servizi erogati dalla medesima Società);
iv) ove necessario, l'anonimizzazione, la pseudonimizzazione o la cifratura dei dati personali trattati;
v) ove necessario ed in particolare in caso di dati soggetti a maggiori tutela, quali previsti dall'ordinamento nazionale, le tutele previste dalle norme di settore.

Entro 60 giorni dalla sottoscrizione della presente designazione, il Responsabile si impegna a comunicare al Titolare:

- ulteriori misure di sicurezza adottate non indicate nella presente designazione comprese quelle di nuova adozione al fine di consentire a quest'ultimo la verifica del mantenimento di un livello di sicurezza adeguato ai rischi ed alla natura dei dati trattati;
- di essere in possesso di idonea polizza assicurativa per il risarcimento di danni inerenti/derivanti dall'attività in parola e per quelli inerenti/derivanti da eventuali violazioni della Privacy;
- la gestione dei "data breach" di cui al successivo articolo 15 e dei file di log relativi alla tracciabilità degli accessi.

In caso di variazione della localizzazione del server e delle modalità di back up, di eventuali allocazioni su cloud, ne deve essere data preventiva comunicazione al Titolare, fatto salvo quanto previsto all'art. 20 sul trasferimento dei dati all'estero.

Qualora il Titolare ritenga necessaria, da parte del Responsabile, l'adozione di una specifica misura di sicurezza in seguito all'evoluzione del quadro tecnologico in grado di garantire un maggior contrasto ad uno o più rischi specifici, da cui è ragionevole attendersi un aumento della probabilità di verificazione dell'evento dannoso o illecito, il Responsabile ha l'obbligo di adeguarsi, fatto salvo l'esercizio di recesso dalla presente designazione nel termine di 60 giorni, e fatta salva la garanzia della continuità del servizio per il tempo occorrente al Titolare ad adottare i provvedimenti necessari.

Qualsiasi istruzione aggiuntiva o diversa rispetto a quanto previsto nella presente designazione deve essere fornita al Responsabile per iscritto e diviene efficace solo a seguito di ricezione da parte dell'Azienda della conferma scritta del Responsabile. Il Responsabile si impegna a informare l'Azienda laddove, a ragionevole giudizio del Responsabile, un'istruzione dell'Azienda possa violare le disposizioni del Codice o del Regolamento.

11. Amministratori di Sistema

[**********] si conforma al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27

novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità con particolare riguardo alle norme del CAD quali declinate dall' AGID.

In particolare, [**********] è onerato di:

i) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
ii) provvedere alla formazione ed all'aggiornamento normativo degli amministratori di sistema;
iii) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite, con evidenza delle attività formative e di aggiornamento normativo erogate ai medesimi;
iv) comunicare con cadenza annuale, entro il 31.12 di ciascun anno ed ogniqualvolta si renda necessario, al Titolare l'elenco aggiornato degli amministratori dei sistemi;
v) verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
vi) mantenere i file di log previsti in conformità a quanto previsto dai sopraccitati provvedimenti.

12. Condizioni per la nomina di sub responsabile

Qualora si rendesse necessario, il Responsabile è tenuto a nominare i sub responsabili del Trattamento, solo con la preventiva autorizzazione del Titolare a seguito di comunicazione. Nella comunicazione devono essere specificate le motivazioni che rendano necessaria tale attività, indicando caratteristiche e requisiti del sub responsabile, nonché, tipologia dei dati oggetto del sub-trattamento, modalità di loro gestione e conservazione, al fine di consentire al Titolare l'accertamento della sussistenza dei requisiti strutturali, di capacità economica, di affidabilità, morali, tecnici ecc. non inferiori a quelli garantiti dal Responsabile stesso, nonché l'assenza di conflitto di interesse anche potenziale in ordine ad eventuali altre finalità di trattamento svolte dal nominando sub responsabile per conto di terzi, ovvero in contrasto con le finalità oggetto del presente incarico.

Tale obbligo si applica anche per i sub-responsabili designati antecedentemente alla data della presente nomina, per i quali [**********] si impegna a far pervenire l'atto di nomina di Responsabile del Trattamento entro 60 giorni dalla sottoscrizione della presente designazione o qualora non ricorrano i presupposti, autocertificazione ex artt. 46 e 47 D.P.R. 445/2000 che i predetti soggetti non svolgono un ruolo inquadrabile come Responsabile del Trattamento. Il Responsabile è tenuto ad inviare, con cadenza annuale, all'Azienda l'elenco complessivo degli eventuali terzi affidatari designati sub responsabili del trattamento.

Nel caso in cui un Responsabile del trattamento ricorra, previa specifica autorizzazione, ad un Sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda, al Sub-Responsabile sono imposti, mediante specifico atto , gli stessi obblighi a cui soggiace il Responsabile. Qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti di ASL3 l'intera responsabilità per l'inadempimento .

13. Responsabile della protezione dati (RPD)/Referente Privacy

[**********] ha nominato il Responsabile per la protezione dati, contattabile all'indirizzo e-mail ……..

Il Responsabile per la protezione dati dell'Azienda è contattabile all'indirizzo e-mail rpd@asl3.liguria.it a cui il Responsabile fa riferimento in relazione agli obblighi di comunicazione**.**

14. Obbligo del responsabile di assistere il titolare nel caso di esercizio dei diritti dell'interessato

Qualora al Responsabile pervenissero richieste degli interessati per l'esercizio dei diritti di cui agli artt. 15, 16, 17, 18, 20 e 21 del Regolamento e norme di armonizzazione, lo stesso deve darne tempestiva comunicazione al Titolare, e comunque entro e non oltre 5 giorni dal ricevimento della richiesta, preferibilmente via pec e via posta elettronica ordinaria indirizzata al Responsabile della Protezione dei dati dell'Azienda al fine di consentire a quest'ultima di adempiere agli obblighi stabiliti dai richiamati articoli, nonché dall'art. 19.

In sintesi quindi [**********] s'impegna fin da ora sui dati gestiti direttamente, ad individuare, osservare, applicare e garantire, anche per conto di eventuali terzi affidatari, le misure idonee a sicurezza del dato a norma del Regolamento UE, con particolare riferimento alla loro cernita, al loro trasferimento, alla loro conservazione, al loro ripristino, alla gestione dei "data breach" e dei file di log traccianti gli accessi, applicando il criterio di indispensabilità del dato nonché di conformare ogni procedura alle disposizioni fissate al proposito dal Regolamento e dalle norme europee nonché a quelle del Codice di Amministrazione Digitale (CAD), di cui al D. L.gs. n. 82/2005, applicabili con particolare riferimento alle misure standard, dandone contezza all'Azienda per iscritto entro 60 giorni dalla sottoscrizione della presente designazione.

Il Responsabile è obbligato a collaborare con il Titolare nel fornire le informazioni di cui questo non dispone, necessarie ad assolvere gli obblighi di cui al paragrafo precedente. Si impegna, inoltre, qualora richiesto dall'interessato, ad eseguire direttamente e tempestivamente le operazioni di rettifica, cancellazione, limitazione del trattamento, portabilità dei dati (qualora possibile) che si rendessero necessari, e ad astenersi dal trattarli ulteriormente in caso dell'esercizio di opposizione da parte dell'interessato ex art. 21 Regolamento e norme di armonizzazione.

15. Obbligo del responsabile di notifica e comunicazione violazione dei dati (data breach), valutazione di impatto, consultazione preventiva

In caso di violazione dei dati personali che inerisca dati conferiti dal Servizio Sanitario Regionale, il Responsabile ne dà al Titolare, comunicazione immediata e comunque entro e non oltre 24 ore dalla conoscenza della violazione, fornendo tutte le informazioni a disposizione in grado di consentire al Titolare la valutazione della violazione, la conferma o meno che tale violazione presenti un rischio per i diritti e le libertà degli interessati, e quindi, qualora ne ricorrano i presupposti, effettuare le notifiche ai sensi degli artt. 33 e 34 del Regolamento e norme di armonizzazione, che rimangono comunque a carico del responsabile, qualora dovute.

La suddetta comunicazione deve contenere almeno le seguenti informazioni:

1. la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. le probabili conseguenze della violazione dei dati personali;
3. le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi;
4. il contatto presso cui ottenere più informazioni.

[**********] s'impegna fin da ora a fornire al Titolare, se necessario, ogni elemento utile ad effettuare la valutazione di impatto nonché ogni collaborazione per un'eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del Regolamento stesso e norme di armonizzazione.

16. Attività di revisione e verifica

Qualora richiesto, il Responsabile dovrà fornire al Titolare i report sull' attività svolta ed oggetto del presente incarico.

Il Responsabile consente sin d'ora al Titolare, o soggetto da questi delegato, di eseguire controlli su tali informazioni, nonché eventuali "Audit" di verifica. Il Titolare dà comunicazione al Responsabile della propria intenzione di svolgere un Audit con ragionevole anticipo. Prima dell'Audit, le Parti devono concordare l'oggetto, la tempistica e la durata dello stesso.

17. Comunicazione dei dati

[**********] non comunica i dati a terzi, salvo espressa autorizzazione del Titolare.

In relazione alla natura dei danni lamentati, i dati possono essere comunicati se strettamente necessari all'assolvimento dell'incarico a:

- Soggetti pubblici e privati ai quali la comunicazione sia dovuta a termini di legge, regolamento o normativa comunitaria, quali (a titolo esemplificativo): ……..;
- Altri soggetti, quali:…….. Tali soggetti potranno a loro volta trasmettere i dati a consulenti e società specializzate per le medesime finalità.

E' fatto divieto cedere i dati a qualsiasi titolo ovvero utilizzarli per le finalità differenti ancorché affini nonché ai fini commerciali, pubblicitari ovvero di marketing.

18. Informazione tempestiva

Qualora una o più disposizioni della presente designazione e di quelle successive contrasti con le norme attuali o future del Regolamento, con direttive o con le Linee Guida stabilite dal Garante della Privacy italiano o dal Comitato Europeo per la Protezione dei dati, il Responsabile dovrà tempestivamente informare il Titolare, prima di procedere alla loro applicazione.

19. Codici di condotta o a meccanismi di certificazione

E' facoltà di [**********]aderire a codici di condotta o a meccanismi di certificazione di cui agli artt. 40 e 42 del Regolamento rispettivamente. Il Responsabile deve comunicare preventivamente al Titolare l'eventuale adesione ai predetti Codici di condotta o il probabile conseguimento di certificazioni.

20. Trasferimento dei dati all'estero e processi decisionali automatizzati

[**********] conferma che tutte le operazioni di trattamento previste dalla presente designazione sono e saranno effettuate in territorio italiano. E' fatto espresso divieto di trattare i dati extra UE, fatta salva l'applicazione delle garanzie dell'art. 44 e seg. del Capo V del Regolamento e norme di armonizzazione.

21. Responsabilità civile e sanzioni

Fermo restando che il Regolamento Europeo (UE) 2016/679 conferma nel trattamento dei dati personali l'attività pericolosa di cui all'art. 2050 del C.C., la relativa responsabilità per danni, patrimoniali e non, provocati all'interessato in conseguenza del trattamento stesso grava in capo a chi detiene i mezzi per gestire le modalità di trattamento (ossia al Titolare/al Responsabile del trattamento o ad entrambi in solido).

Il Responsabile Esterno risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi e per gli effetti di cui agli artt. 1218 e 1223 del Codice Civile.

Il Responsabile del trattamento risponde direttamente per il danno causato dal trattamento qualora non abbia adempiuto agli obblighi previsti dal Regolamento ovvero abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare del trattamento, manlevando l'Azienda per eventuali violazioni di norme, inadempimenti giuridici, inosservanza regolamentari, nonché per i danni inerenti/derivanti dai trattamenti dati di cui trattasi, per i quali l'Azienda possa essere chiamata a rispondere, sia civilmente, sia in punto privacy. Identico riparto si configura in ipotesi di sanzioni amministrative.

Come detto, qualora il Responsabile violi una delle disposizioni della presente designazione, determinando le finalità e i mezzi del trattamento, è considerato Titolare delle attività di trattamento per le quali ha determinato in autonomia finalità e mezzi del trattamento e come tale risponde a sensi di legge.

Il Responsabile garantisce ai sensi e per gli effetti dell'art. 1936 codice civile e seguenti tutte le obbligazioni cui è tenuto l'eventuale sub responsabile o eventuali sub responsabili, compreso il risarcimento dei danni per trattamento illecito dei dati personali ai sensi del Regolamento (UE) 2016/679.

22. Cancellazione/Restituzione dei dati trattati

Al termine della prestazione dei servizi che comportano l'attività di trattamento, il Responsabile dovrà in alternativa e su richiesta del Titolare:

- restituire i dati personali al Titolare del Trattamento ed eliminarli dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati;
- eliminarli in maniera permanente dalla propria infrastruttura informatica ed archivi cartacei, fornendo al Titolare idonea dichiarazione scritta dell'avvenuta distruzione dei dati.

23. Diritto di informare le persone interessate

(Eventualmente spetta a ……., l'obbligo di fornire agli interessati le informazioni di cui agli artt. 13-14 del Regolamento ed acquisirne il relativo consenso, se dovuto, con obbligo di conservazione insieme alla documentazione relativa all'interessato/utente).

24. Trattamento illecito, risoluzione di diritto e conseguenze giuridiche

L'inadempimento di quanto previsto nel presente atto nella sua interezza e con particolare riferimento ai punti 8, 9, 10, 11, 12, 14, 15 e 23 comporta la revoca di diritto del presente incarico con contestuale caducazione del rapporto contrattuale/convenzionale sostanziale per violazione privacy, fatte salve, come detto, le responsabilità inerenti e/o derivanti da tali violazione ed il relativo ristoro di eventuali danni. In caso di contrasto con le disposizioni contrattuali prevalgono quelle della presente designazione. Eventuali accordi in contrasto ovvero in deroga con le disposizioni del presente atto debbono essere concordate per iscritto tra le Parti, richiamando espressamente quelle derogate avvertendo che ciò connota responsabilità diretta dei contraenti.

25. Disposizioni finali

Per tutto quanto non previsto dalla presente designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia di protezione dei dati personali.

Il presente accordo potrà essere oggetto di revisione qualora successivamente alla sottoscrizione intervengano modifiche normative che comportino il suo adeguamento alla normativa nazionale e/o a quella europea.

Il presente atto è composto da n. …. facciate.

Data _____

AZIENDA SOCIOSANITARIA LIGURE 3

in personale del Legale Rappresentante/Titolare

Il Direttore Generale

Dott. ……..

Firma _____

Per accettazione di quanto sopra

[**********]

in persona del Legale Rappresentante/Titolare

Dott. / Sig . …….

Firma _____

ALLEGATO C:

INFORMAZIONI GENERALI

AL TRATTAMENTO DEI DATI PERSONALI

DEGLI ASSISTITI

(Artt. 12, 13 e 14 Regolamento UE 2016/679)

TITOLARE DEL TRATTAMENTO L'**ASL N. 3** comunica agli **ASSISTITI** ovvero a coloro che, in base alle vigenti disposizioni normative, hanno diritto o bisogno di assistenza sanitaria e ai quali sono assicurati i livelli uniformi ed essenziali d'assistenza (anche attraverso il ricorso all'attività libero-professionale intramuraria, anche allargata) ovvero hanno richiesto prestazioni extra-S.S.N., le seguenti **INFORMAZIONI** (disponibili anche alla pagina http://www.asl3.liguria.it/siti-tematici/privacy.html):

- Il **TITOLARE DEL TRATTAMENTO** dei dati personali è **ASL N. 3** nella persona del Direttore Generale legale rappresentante *pro-tempore* (**DATI DI CONTATTO**: *pec* protocollo@pec.asl3.liguria.it, centralino telefonico 010 84911). Nel rispetto della normativa vigente, qualora il trattamento debba essere effettuato in contitolarità ovvero in corresponsabilità per conto del Titolare ASL3, i dati personali degli **ASSISTITI** potranno essere trattati dai seguenti ulteriori soggetti autorizzati (**CONTITOLARI** o **RESPONSABILI DEL TRATTAMENTO)** e a tal fine istruiti mediante il ricorso a contratti o ad atti giuridici vincolanti:

* Soggetti erogatori pubblici o equiparati;

* Soggetti erogatori privati accreditati e/o iscritti in specifico registro per gli Enti del Terzo Settore che abbiano stipulato accordi contrattuali e/o convenzioni con il Servizio Sanitario Regionale;

* Operatori economici che offrono a seguito di appalto pubblico la fornitura di prodotti o la prestazione di servizi.

- I **DATI DI CONTATTO** del **RESPONSABILE PER LA PROTEZIONE DEI DATI (R.P.D.)** presso la ASL3, quale garante e facilitatore nell'ambito del **SISTEMA PRIVACY AZIENDALE** a cui si possono rivolgere tutti gli **INTERESSATI** per tutte le questioni relative al trattamento dei dati personali e all'esercizio dei conseguenti diritti, sono:

Via Bertani, 4 16125 Genova (GE)

PEC protocollo@pec.asl3.liguria.it,

EMAIL rpd@asl3.liguria.it;

BASE GIURIDICA DEL TRATTAMENTO

Il trattamento dei dati personali degli ASSISTITI trova fondamento e LICEITA' in:

- ✓ Adempimento degli obblighi legali ai quali è soggetto il Titolare del trattamento ASL3 (art. 6, paragrafo 1, lett. c) del "Regolamento");
- ✓ Salvaguardia degli interessi vitali dell'assistito o di un'altra persona fisica (art. 6, paragrafo 1, lett. d) del "Regolamento");
- ✓ Esecuzione dei compiti di interesse pubblico o connessi all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento ASL3 (art. 6, paragrafo 1, lett. e) del "Regolamento");
- ✓ Esecuzione di un contratto in cui l'interessato è parte o adozione di misure precontrattuali adottate su richiesta dello stesso (art. 6, paragrafo 1, lett. b) del "Regolamento").

A titolo esemplificativo e non esaustivo di seguito si riportano le più importanti **BASI GIURIDICHE** sulle quali si fonda il trattamento dei dati da parte del Titolare :

- art. 32 della Costituzione; dalla legge n. 833/78 e s.m.i. "Istituzione del SSN"; dal D. Lgs. n. 502/1992 e s.m.i.; dal D. Lgs. n. 229/99 Riordino della disciplina in materia sanitaria; dalla Legge Regionale n. 41/2006 e s.m.i. "Riordino del SSR"; dalla L.R. n. 17/2016 e s.m.i. "Istituzione dell'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.) ed indirizzi per il riordino delle disposizioni regionali in materia sanitaria e sociosanitaria; dai vigenti piani sanitari nazionali e regionali;
- normativa europea, nazionale e regionale in materia di privacy (rispettivamente, Regolamento generale sulla protezione dei dati UE 2016/679, d'ora in poi per brevità semplicemente "Regolamento" e relative norme di armonizzazione - Codice in materia di protezione dei dati personali di cui al D. L.gs. 196/2003, così come modificato dal D.lgs. n. 101/2018;
- Linee Guida e dei Provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali, volte a disciplinare i trattamenti di dati personali e categorie particolari di dati personali effettuati nel complesso delle strutture facenti capo alla ASL3, anche in regime libero professionale intramoenia, anche allargata;
- norme di settore volte a disciplinare l'attività sanitaria quale attività di rilevante interesse pubblico quali a titolo esemplificativo e non esaustivo; quelle richiamate dal Regolamento Regionale 9 aprile 2013 n. 2 "Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione. In detto Regolamento ed, in particolare, nelle relative schede dei trattamenti sono indicate le normative di riferimento che, nella misura in cui sono tutt'ora vigenti, costituiscono la base normativa dei trattamenti effettuati, da intendersi qui richiamate e fatte proprie dal Titolare, in quanto compatibili con la normativa europea e con le disposizioni di armonizzazione della stessa, a livello nazionale e/o regionale.

LE FINALITÀ PERSEGUITE, per l'insieme dei trattamenti di dati personali e categorie particolari di dati personali effettuati nel complesso delle strutture facenti capo alla ASL3, anche in regime libero professionale intramoenia, anche allargata, sono di rilevante interesse pubblico ossia volte alla prevenzione, diagnosi e cura, attività di ricerca scientifico-statistica, prescrizione di farmaci, anche off label, dispositivi – presidi medici , esami diagnostici, accertamento e certificazione dello stato di salute attività formative e didattiche e connessi adempimenti amministrativi, contabili, di archiviazione, di programmazione, gestione, controllo, valutazione e vigilanza, indispensabili ad espletare le correlate attività aziendali.

Si informa in particolare che i **DATI PERSONALI,** (*es.* i dati anagrafici, codice fiscale, tipo di esenzione, dati assicurativi, dati bancari, etc.) forniti dagli **ASSISTITI** nell'ambito delle richieste

di assistenza per erogare servizi e prestazioni adeguate alle necessità rilevate o espresse, saranno utilizzati dal Titolare/ASL3 per le FINALITA' di tutela della salute, fondamentale diritto dell'individuo ed interesse della collettività.

Eventuali ulteriori informazioni relative all'utilizzazione dei suddetti dati potranno essere specificamente declinate nelle **INFORMATIVE AGGIUNTIVE** pubblicate alla pagina web http: http://www.asl3.liguria.it/siti-tematici/privacy.html del sito aziendale ed esposte nei locali delle singole strutture aziendali erogatrici delle prestazioni sanitarie.

CATEGORIE PARTICOLARI DI DATI PERSONALI La LICEITA' del trattamento dei **DATI GENETICI, BIOMETRICI, RELATIVI ALLA SALUTE O ALLA VITA SESSUALE O ALL'ORIENTAMENTO SESSUALE DELLA PERSONA**, nonché delle eventuali altre categorie particolari di dati personali da parte del Titolare del trattamento ASL3 è ammessa al verificarsi di uno dei seguenti casi:

- **L'ASSISTITO** ha prestato il proprio consenso esplicito, di norma facoltativo, al trattamento di tali dati personali per una o più **FINALITÀ** peculiari (art. 9, paragrafo 2, lett. a) del "Regolamento") come, tra gli altri, nei casi di costituzione del Dossier Sanitario Elettronico (DSE), del Fascicolo Sanitario Elettronico (FSE) o di comunicazione dei dati al Medico curante (cfr informazioni di dettaglio DSE e FSE ex artt. 13 e 14 del Regolamento).

- Tutela di un interesse vitale dell'**ASSISTITO** o di un'altra persona fisica qualora il primo si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (art. 9, paragrafo 2, lett. c) del "Regolamento");

- Motivi di interesse pubblico rilevante sulla base del diritto (art. 9, paragrafo 2, lett. g) del "Regolamento");

- Finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto (art. 9, paragrafo 2, lett. h) del "Regolamento");

- Motivi di interesse pubblico nel settore della sanità pubblica (art. 9, paragrafo 2, lett. i) del "Regolamento");

- Archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base del diritto (art. 9, paragrafo 2, lett. j) del "Regolamento").

Per le finalità di ricerca scientifico-statistica il trattamento viene effettuato solo in forma aggregata e con modalità tali da garantire l'anonimato.

E' comunque possibile che i dati possano essere in futuro trattati non in forma anonima a fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, o a fini statistici non ritenute incompatibili con la finalità iniziale, come espressamente previsto dall'art. 5 par. 1 lett.b) e dall'art. 9 par. 2 lett. j) del Regolamento UE 679/2016, fatte salve le previsioni degli artt. 110 e 110 bis del D.Lgs. 196/2003 e s.m.i. per le finalità di ricerca.

Per quanto sopra, in particolare ai sensi e per gli effetti del combinato disposto dagli artt. 9, paragrafo 2, lett. g) del "Regolamento" e 2sexies, comma 2, lett. v) del sopraccitato D. Lgs. n. 101/2018, non-

chè dall'art. 3 della L.R. n. 17/2016 che attribuisce all'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.) competenza nelle attività di programmazione sanitaria e sociosanitaria, coordinamento, indirizzo e governance, e dal D.P.C.M. 3-3-2017 in tema di "*Identificazione dei sistemi di sorveglianza e dei registri di mortalità, di tumori e di altre patologie*":

- il Titolare del trattamento ASL3 ricorrendo a dati anonimi in forma aggregata, utilizza metodologie tese allo studio dei processi interni al fine di migliorare la qualità delle prestazioni erogate nonché individuare le criticità più frequenti anche in relazione ai casi correlati di cui ai citati sistemi di sorveglianza.

In tale ottica e in linea generale, il Titolare del trattamento ASL3 effettua verifiche volte a valutare allineamenti e scostamenti della prassi clinica rispetto a buone pratiche, linee guida, protocolli operativi etc .

Tale attività condotta, in forma completamente anonima e nel rispetto dei principi di minimizzazione, indispensabilità e non eccedenza del dato, potrà essere integrata, a richiesta e valutata per ciascun singolo caso, con i dati sanitari in possesso delle Aziende ed Enti/Istituti del S.S.R. ligure, ancorché in forma non anonima e qualora tali dati siano in grado di integrare il quadro clinico necessario alla valutazione.

- il Titolare ASL3 in concorso con le CONTITOLARI Aziende ed Enti/Istituti del S.S.R. ligure e al RESPONSABILE del trattamento IRCCS Ospedale Policlinico San Martino, tiene il "Registro Tumori" quale sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di tumore che insorgono nei residenti nel territorio della Regione Liguria. Il Registro è realizzato ai fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché di elaborazione delle informazioni epidemiologiche e statistiche a supporto delle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria.

I dati di salute e soggetti a maggior tutela contenuti nel Registro Tumori, tenuti con l'ausilio di strumenti elettronici, sono trattati mediante l'utilizzo di codici identificativi (pseudonimizzazione) , rendendoli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità, in modo tale da tutelare l'identità e la riservatezza degli ASSISTITI.

MODALITÀ DEL TRATTAMENTO I **DATI PERSONALI** forniti per le finalità di tutela della salute sono trattati secondo le disposizioni di legge vigenti in materia in modalità analogica e digitale tramite software applicativi dedicati.

Sono inoltre raccolti o comunque trattati in banche dati digitali quali ad es *database in-house* e altri *database* ministeriali, regionali e di enti pubblici resi disponibili, in quanto utilizzati nell'esercizio delle attività istituzionali di ASL3.

Possono essere, altresì, conservati in **ARCHIVI CARTACEI**.

La determinazione del **PERIODO DI CONSERVAZIONE** dei dati personali avviene in funzione dei criteri stabiliti dal Ministero dei Beni Culturali – Direzione Generale per gli Archivi nel "*Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere*", che il Titolare del trattamento ha fatto propri con delibera n. 405 del 29 giugno 2016 (pubblicata alla pagina web http: http://www.asl3.liguria.it/siti-tematici/privacy.html). Infatti, i documenti generati e/o custoditi dall'ASL3 possono avere contenuto eterogeneo potendo comprendere: dati impersonali, dati personali non particolari, dati personali particolari, dati personali genetici. …

L'accesso alle suddette banche dati ovvero **ARCHIVI CARTACEI** contenenti dati personali degli ASSISTITI è consentito soltanto al **PERSONALE AUTORIZZATO** al trattamento sotto l'autorità diretta del Titolare ASL3 o del Responsabile del trattamento designato da ASL3 per le finalità sanitarie di tutela della salute ed amministrativo-contabili –di gestione, controllo, valutazione e vigilanza correlate.

Per finalità statistica e/o di ricerca il Titolare ASL3 può autorizzare i soggetti richiedenti all'accesso con modalità tali da garantire l'anonimato.

Il Titolare ASL3 può stipulare appositi atti convenzionali/Contratti con i soggetti richiedenti al fine di definire le modalità di accesso ai dati e/o loro trattamento da parte di studenti/tirocinanti/specializzandi/frequentatori volontari, previa loro specifica autorizzazione.

I dati personali necessari ad assolvere una funzione, un servizio ovvero per l'esecuzione di prestazioni richieste o necessarie per l'interessato, possono essere comunicati a medici convenzionati, strutture convenzionate, farmacie convenzionate, consulenti, broker, compagnie di assicurazione, loss adjuster ovvero, conformemente ad un obbligo legale, ai fini dell'esercizio della missione istituzionale o per richiesta dell'interessato, a Soggetti erogatori pubblici o equiparati, Comuni, anche in forma anonima o sotto forma di reportistica epidemiologico-statistica, ad altre Amministrazioni pubbliche, quali, tra le altre, il Ministero della Salute, il Ministero dell'Economia e delle Finanze, la Regione Liguria, l'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.).

Nell'ambito della suddetta missione istituzionale, il Titolare ASL3, mediante il proprio personale medico/sanitario opportunamente individuato, partecipa alle attività dei Dipartimenti Interaziendali Regionali (DIAR) declinati nelle varie aree specialistiche, costituiti ai sensi dell'art. 40 bis della Legge Regionale n. 41/2006 e s.m.i. come introdotto dall'art. 1 della L.R. n. 27/2016, quali strumenti organizzativi del sistema sanitario regionale per la programmazione strategica e l'integrazione dei diversi livelli di assistenza delle attività sanitarie e sociosanitarie in ambito regionale.

In tale contesto, con l'obiettivo di promuovere la qualità, l'appropriatezza delle cure, l'omogeneità sul territorio, l'efficacia delle attività sanitarie e sociosanitarie, possono essere trattati dati anche in forma anonima per finalità epidemiologico-statistiche e programmatorie-organizzative.

Non è intenzione del Titolare del trattamento ASL3 trasferire dati personali degli **ASSISTITI** a Paesi terzi o a organizzazioni internazionali. Nel caso in cui ciò sia previsto contrattualmente nell'ambito di tecnologie utilizzate da ASL3, quest'ultima adotterà misure tecniche di sicurezza adeguate per garantire l'ASSISTITO dai rischi ai suoi diritti e libertà.

DIRITTI DELL'ASSISTITO Per garantire un trattamento dei dati corretto e trasparente, l'**ASSISTITO** ha diritto di chiedere al Titolare ASL3:

- Accedere ai propri dati e conoscere chi vi ha avuto accesso (art. 15 del Regolamento);
- Richiedere l'aggiornamento, la rettifica o l'integrazione dei dati (art. 16 del Regolamento);
- Richiedere la cancellazione, la trasformazione in forma anonima dei dati, il loro blocco e la limitazione del trattamento se trattati in difformità dalla legge, fatti salvi gli obblighi legali di conservazione (artt. 17 e 18 del Regolamento);
- Ricevere, (se possibile) in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento unitamente al diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

- ✓ il trattamento si basi sul consenso ai sensi dell'art. 6, paragrafo 1, lettera a), o dell'art. 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'art. 6, paragrafo 1, lettera b) del Regolamento;
- ✓ il trattamento sia effettuato con mezzi automatizzati (art. 20 del Regolamento).

- Opporsi, per motivi legittimi, al trattamento dei dati (art. 21 del Regolamento);

Le modalità di esercizio dei diritti sono disponibili al link http://www.asl3.liguria.it/siti-tematici/privacy.html del sito aziendale.

Ai sensi dell'art.2 terdecies del D.lgs. 196/2003 e s.m.i. , i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione. L'esercizio dei suddetti diritti non e' ammesso nei casi previsti dalla legge.

È inoltre facoltà dell'interessato vietare in tutto o in parte l'esercizio dei suddetti diritti da parte di terzi come previsto dall'art. 2- terdecies del D.Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018 e s.m.i..

Nei casi in cui il trattamento sia basato sul consenso esplicito, l'**ASSISTITO** ha diritto di revocarlo in qualsiasi momento senza che ciò pregiudichi la liceità del trattamento basata sul consenso prestato prima della revoca.

Poiché una corretta e sicura identificazione dell'ASSITITO da parte del PERSONALE AUTORIZZATO di ASL3 è di fondamentale importanza, soprattutto per ridurre il **RISCHIO CLINICO** durante la somministrazione di farmaci e trasfusioni, esami diagnostici ed interventi chirurgici, durante il ricovero potrà essere apposto al polso dell'ASSISTITO un **BRACCIALETTO IDENTIFICATIVO** contenente unicamente dati personali anagrafici (non sanitari) la cui finalità è l'aumento della sicurezza clinica dell'ASSISTITO.

In caso di prenotazione di visita attraverso il sistema CUP, oltre ai dati personali, potrà essere richiesto all'interessato anche un numero di telefono personale, fisso o cellulare, che verrà utilizzato, fino a diversa indicazione dello stesso, per confermargli o ricordargli il giorno della prenotazione o per avvisarlo in caso di annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica.

In caso di ricovero ospedaliero i dati anagrafici ed il reparto di degenza in cui l'assistito è ricoverato saranno disponibili per agevolare l'accesso ai reparti di degenza da parte dei visitatori; nel caso in cui lo stesso non intenda renderli disponibili, può in occasione di ogni ricovero, manifestare l'eventuale specifico dissenso.

Sebbene il trattamento dei dati personali per la tutela della salute discenda da un obbligo legale, l'**ASSISTITO** non ha l'obbligo di fornirli. Il loro mancato conferimento, tuttavia, può non consentire l'erogazione corretta delle prestazioni e nel caso di non conferimento dei dati anagrafici, mancando la possibilità di identificare la persona fisica, il diritto alle cure resta precluso, tranne nel caso di urgenza - emergenza.

Nel caso in cui i dati personali dell'**ASSISTITO** non siano stati ottenuti direttamente presso l'interessato, nell'ambito delle pertinenti **INFORMATIVE AGGIUNTIVE**, da esporre nei locali delle strutture aziendali erogatrici delle prestazioni sanitarie, sarà indicata la fonte da cui hanno origine i dati personali medesimi a meno che il loro ottenimento o la loro comunicazione al Titolare ASL3 siano espressamente previsti dal diritto.

Se l'**ASSISTITO**, nonostante l'intervento espressamente richiesto per il tramite del suddetto **RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)**, considerasse leso un proprio "**DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI**" durante un trattamento effettuato dal Titolare ASL3, ai sensi dell'art. 13 par 2 lett. d) e dell'art. 14 par. 2 lett. e) del Regolamento, rimane impregiudicato il suo diritto di rivolgere reclamo al Garante della protezione dei dati personali secondo le modalità descritte nel sito www.garanteprivacy.it.

ALLEGATO D: RACCOLTA CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E CATEGORIE PARTICOLARI DI DATI PERSONALI

ai sensi del Regolamento Europeo n. 679/2016 e norme attuative

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i(1)

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno,) (2)

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa di cui agli artt. 13 e 14 del Regolamento U.E. 679/2016 e norme attuative in materia di protezione dei dati personali ed **esprimo il consenso** al trattamento dei dati personali e categorie particolari di dati personali, così come illustrati nella predetta informativa.

SI ☐ NO ☐

Per quanto attiene all'utilizzo del numero di telefono personale, fisso o cellulare, per confermare o ricordare il giorno della prenotazione o per avvisare in caso di annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica, **esprimo il consenso**

SI ☐ NO ☐

Chiedo infine che le categorie particolari di dati personali inerenti il mio stato di salute mi siano resi noti per il tramite del personale medico dipendente od in consulenza designato dal Titolare del trattamento

Ovvero

Del medico di mia fiducia Dott.. _____con studio in_____

Via_____n_____

designato dal sottoscritto

Genova, ___/___/___ Firma dell'interessato

_____

_____

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat…….....n…….

Rilasciata da …….....il……

Firma dell'operatore incaricato

[1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: "Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera."

Art. 76, D.P.R. n. 445/2000 e s.m.i.: "Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L'esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[2] Precisare la qualità ed allegare documentazione comprovante la qualità.

ALLEGATO E: RACCOLTA CONSENSO OSPEDALIERO AL TRATTAMENTO DEI DATI PERSONALI E CATEGORIE PARTICOLARI DI DATI PERSONALI AI SENSI DEL REGOLAMENTO EUROPEO N. 679/2016 E NORME DI ARMONIZZAZIONE

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i(1)

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno,) (2)

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa di cui agli artt. 13 e 14 del Regolamento U.E. 679/2016 e norme attuative in materia di protezione dei dati personali ed **esprimo il consenso** al trattamento dei dati personali e categorie particolari di dati personali, così come illustrati nella predetta informativa.

SI ☐ NO ☐

Per quanto attiene all'utilizzo del numero di telefono personale, fisso o cellulare, per confermare o ricordare il giorno della prenotazione o per avvisare in caso di annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica, **esprimo il consenso**

SI ☐ NO ☐

Inoltre **esprimo il consenso** alla ASL3 a:(barrare le voci che interessano)

- comunicare il mio ricovero e la sede a chi ne faccia richiesta; SI NO
- comunicare i dati personali, riguardanti il mio stato di salute SI NO

ai seguenti familiari/conviventi/persone di fiducia:

1) Cognome e Nome _____n. di telefono_____

2) Cognome e Nome _____n. di telefono_____

Chiedo infine che i dati sensibili inerenti il mio stato di salute mi siano resi noti per il tramite del personale medico dipendente od in consulenza designato dal Titolare del trattamento

ovvero

Del medico di mia fiducia Dott.. _____ con studio in _____Via_____ _____n_____ designato dal sottoscritto.

Genova, ___/___/___ Firma del paziente

_____

_____

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat…….....n…….

Rilasciata da ……......il……

Firma dell'operatore incaricato

1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: "Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera."

Art. 76, D.P.R. n. 445/2000 e s.m.i.: "Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L'esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[2] Precisare la qualità ed allegare documentazione comprovante la qualità.

ALLEGATO F:

Informazioni ex art. 13 e 14 Regolamento Unione Europea 679/2016 del 27 aprile 2016 e norme di armonizzazione (D. Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018 e s.m.i.) per il trattamento dei dati personali e categorie di dati personali dei dipendenti

Il Regolamento Unione Europea 679/2016 del 27 aprile 2016 (nel proseguo Regolamento UE 679/2016) e le relative norme di armonizzazione (D. Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018 e s.m.i.) riconoscono e disciplinano il diritto alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché la libera circolazione degli stessi.

In base a detta normativa è "titolare" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

La ASL 3 , in quanto titolare del trattamento, in attuazione della citata normativa e nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale, La informa, con le seguenti informazioni, su come vengono trattati i Suoi dati quale dipendente presso questa azienda sociosanitaria.

1) Perché trattiamo i suoi dati?

Le presenti informazioni vengono fornite per l'insieme dei trattamenti di dati personali e categorie particolari di dati personali effettuati nel complesso delle strutture facenti capo alla A.S.L. 3, anche in regime libero professionale *intramoenia*, anche *allargata*, per le sole finalità di adempiere agli obblighi ed ai compiti in materia di instaurazione e gestione del rapporto di lavoro e di impiego alle dipendenze della amministrazione pubblica, nonché per adempiere a specifici obblighi previsti dalla normativa comunitaria, da leggi, da regolamenti o da disposizioni in materia di igiene e sicurezza sul luogo di lavoro.

Il trattamento dei dati personali e particolari, ivi compresi quelli idonei a rivelare lo stato di salute, è effettuato relativamente a quelli effettivamente necessari ed indispensabili a dare esecuzione agli obblighi derivanti dal rapporto di lavoro con la ASL3, anche ex art.6, comma 1 lettera b) ed ex art.9, comma 2 lettere b), f), g) del Regolamento UE 679/2016 e norme di armonizzazione.

2) In base a quali norme trattiamo i suoi dati?

ASL3 tratta le categorie particolari di dati personali ed i dati personali in base al Regolamento Regionale 9 aprile 2013 n. 2 "Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione". In detto Regolamento (pubblicato sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) ed, in particolare, nelle relative schede dei trattamenti, sono indicate le normative di riferimento che costituiscono la base normativa dei trattamenti effettuati da questa ASL3, da intendersi qui richiamate dal titolare.

Detto Regolamento viene allo stato mantenuto e fatto proprio dal titolare, per quanto possa occorrere, quale elenco di trattamenti, tipologie di dati, finalità di trattamento, riferimenti normativi che legittimano i trattamenti e destinatari di comunicazioni afferenti i dati trattati dall'ASL3, nelle aree di afferenza ed a miglior dettaglio del registro dei trattamenti, agli atti in formato elettronico dell'Azienda, in quanto compatibili con la normativa europea e le disposizioni di armonizzazione della stessa a livello nazionale e/o regionale.

3) Quali sono i suoi dati che trattiamo?

La ASL3 , in quanto titolare del trattamento, ai sensi degli artt. 13 e 14 Regolamento Unione Europea 679/2016 del 27 aprile 2016 e norme di armonizzazione ed in conformità a quanto indicato nelle "Linee guida in materia di trattamento dei dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", di cui

alla Deliberazione n. 23 del 14/6/2007 dell'Autorità Garante della Privacy, fatte proprie dal titolare, in quanto compatibili con detta normativa, quali policy aziendali, informa i dipendenti che tratta nel rispetto della normativa vigente:

- I dati personali (qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale)
- ed i dati c.d. "particolari" (i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona),

direttamente forniti dal/dalla dipendente o raccolti presso terzi (in questo caso l'Azienda provvederà ai sensi dell'art.14 del Regolamento UE 679/2016 e norme di armonizzazione "Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato") o attraverso altre fonti.

In particolare il trattamento effettuato da ASL 3 ha come oggetto ogni attività ed operazione concernente la gestione giuridica, economica, previdenziale, fiscale e pensionistica del personale comprese le attività di formazione; ogni attività e operazione necessaria per adempiere agli obblighi derivanti dai contratti di assicurazione, finalizzati alla copertura dei rischi derivanti da danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale; ogni attività e operazione necessaria per le procedure di riconoscimento di diritti ed agevolazioni; ogni adempimento connesso e necessario all'iscrizione ad organizzazioni sindacali ed all'esercizio dei diritti sindacali.
Qualora il dipendente abbia richiesto l'attivazione della modalità di prestazione lavorativa "Lavoro agile", ad integrazione delle informazioni e misure di sicurezza fornite allo stesso quale dipendente ed all'atto dell'autorizzazione al trattamento dati personali nell'ambito lavorativo di assegnazione, si precisa che l'Azienda provvederà al trattamento anche dei dati personali ed identificativi collegati alla postazione-dotazione strumentale mobile utilizzata dallo stesso per il "Lavoro Agile".
Si ricorda che la suddetta modalità di lavoro non prevede vincolo di orario, essendo misurata per obiettivi e si richiamano le misure di sicurezza previste dal D.P.S. ASL3 vigente e dal vigente regolamento aziendale per quanto attiene l'uso degli strumenti informatici e l'effettuazione di eventuali controlli nel rispetto della L.300/1970 e s.m.i.

4) Il conferimento dei dati ha natura obbligatoria o facoltativa?

Il trattamento è tra quelli ammessi per motivi di interesse pubblico rilevante, così come indicato dall'art. 2 sexies del D. Lgs. 196/2003 e s.m.i., in particolare lettera dd) , oltre che per quanto previsto dall'art. 2 octies del D.Lgs. 196/2003 e s.m.i. e lecito ex art.6, comma 1 lett.b) Regolamento UE 679/2016 e norme di armonizzazione.

Il conferimento dei Suoi dati è necessario per l'esecuzione degli obblighi derivanti dal rapporto di lavoro (obbligo contrattuale) e/o comunque per la gestione dello stesso rapporto lavorativo. Il conferimento dei dati relativi ai propri familiari è obbligatorio ai fini della definizione del trattamento economico del dipendente e considerato che, in caso di domande od istanze di prestazioni o agevolazioni specifiche (es. riconoscimento assegno familiare, legge 104/92, etc.), l'eventuale rifiuto potrebbe comportare l'impossibilità di consentire l'adozione dei provvedimenti richiesti.
I dati personali e particolari sono trattati in modo lecito e corretto, raccolti esclusivamente per le finalità infra indicate, costantemente aggiornati e conservati per un periodo non superiore a quello necessario agli scopi per cui i dati vengono raccolti.

5) Per quanto tempo conserviamo i suoi dati?

La A.S.L.3 ha l'obbligo di conservare la documentazione e i dati che riguardano il dipendente per un dato periodo determinato o illimitato in base alla normativa nazionale o qualora il trattamento si renda necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui l'Azienda è investita o per il perseguimento di un legittimo interesse dell'Azienda e comunque in presenza di garanzie appropriate, ai sensi di legge, per i diritti fondamentali e gli interessi del dipendente.

I dati saranno conservati ai sensi dell'art. 5, par. 1, lett. e) del Regolamento Europeo per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e saranno, comunque, conservati tenendo conto di specifici termini di conservazione stabiliti per legge, o conformemente ai criteri di conservazione stabiliti nel prontuario di scarto della documentazione sanitaria e amministrativa di cui alla deliberazione di questa azienda n. 405 del 29/06/2016 e sue successive modifiche (pubblicata sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) o ancora sulla base del principio della necessità del trattamento in relazione alle finalità istituzionali perseguite dalla A.S.L.3 .

6) Come trattiamo i suoi dati e chi può conoscerli ed utilizzarli?

Il trattamento dei dati sarà improntato ai principi di correttezza, liceità, pertinenza, non eccedenza e trasparenza nei confronti dell'interessato, nel rispetto dei diritti riconosciuti a quest'ultimo dalla vigente normativa ed in maniera da garantire un'adeguata sicurezza, integrità e riservatezza dei dati stessi.

I dati rilasciati alla A.S.L.3 potranno essere utilizzati sia in modo manuale che informatizzato dal personale debitamente autorizzato al trattamento dei dati, in qualità di autorizzato al trattamento, e saranno conservati in luogo idoneo ed appropriato, tutelandone la riservatezza, nel rispetto del segreto professionale e d'ufficio.

Potranno inoltre essere trattati da soggetti terzi, previamente nominati quali "responsabili" ai sensi dell'art. 28 del Regolamento Europeo n.679/2016 e norme di armonizzazione, incaricati di svolgere specifiche operazioni necessarie per garantire i servizi dell'Azienda, nei limiti strettamente pertinenti alle finalità di cui sopra.

I dati personali necessari alla predisposizione dei cedolini paga e del CUD sono, ad esempio, a conoscenza della Società INSIEL Mercato S.p.a. per lo svolgimento del relativo servizio e di conseguenza trattati dalla medesima società attraverso i rispettivi dipendenti e collaboratori autorizzati.
In ottemperanza al provvedimento dell'Autorità Garante per la protezione dei dati personali del 27 novembre 2008 e s.m.i. " Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle funzioni di amministratore di sistema", i cui contenuti il Titolare fa propri quali policy aziendali, in quanto compatibili con la normativa vigente, si informano i dipendenti che le attività degli amministratori di sistema riguardano, anche indirettamente, servizi o sistemi che trattano o che permettono il trattamento di dati personali e particolari dei dipendenti. L'elenco degli amministratori di sistema è consultabile nel Documento Programmatico sulla Sicurezza, pubblicato sulla rete Intranet aziendale nella sezione " Normativa/privacy".
I dati potranno inoltre essere comunicati, quando ciò risulti necessario in relazione all'erogazione della prestazione o allo svolgimento dei compiti istituzionali attribuiti all'Azienda alle seguenti categorie di soggetti: a enti ed organismi pubblici nei casi previsti dalla legge , nonché alle forze dell'ordine o all'autorità giudiziaria su richiesta di questi ultimi per finalità di prevenzione, accertamento o repressione di reati, soggetti pubblici e privati su Sua specifica richiesta o indicazione.

L'A.S.L.3 si riserva, inoltre, di effettuare le necessarie comunicazioni di detti dati agli enti competenti, ai sensi di legge o di regolamento.

ASL 3 si riserva, infine, di verificare il rispetto delle misure di sicurezza ambientali, informatiche ed operative sia in ambito privacy sia in ambito di sicurezza sul lavoro indicate alla S.V. infra ed all'atto dell'autorizzazione di particolari modalità di lavoro, parti integranti delle presenti informazioni, nel rispetto delle previsioni della normativa vigente in materia e dell'art.4 della L.300/1070 e s.m.i..

7) Quali sono i suoi diritti in materia di privacy?

In ogni momento potranno essere esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 e norme di armonizzazione, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme di armonizzazione ("Diritto alla cancellazione"-«diritto all'oblio»)- 3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.") , la limitazione del trattamento, se ricorrano le ipotesi di cui all'art. 18 del Regolamento UE 679/2016 e norme di armonizzazione ("Diritto di limitazione di trattamento"), l'opposizione al loro trattamento ai sensi dell'art. 21 del regolamento UE 679/2016 e norme di armonizzazione ("Diritto di opposizione") nonché il diritto alla portabilità dei dati.

È Sua facoltà di vietare in tutto o in parte l'esercizio dei suddetti diritti da parte di terzi come previsto dall'art. 2-terdecies del D.Lgs. 196/2003 così come modificato dal D. Lgs. 101/2018 e s.m.i..

Inoltre ha diritto di proporre reclamo all'autorità di controllo (Autorità Garante per la protezione dei dati personali-secondo le modalità previste sul sito internet dello stesso **www.garanteprivacy.it)**, nei casi previsti dalle disposizioni in materia di protezione dei dati di cui al Regolamento UE 2016/679 e norme di armonizzazione.

8) Chi è il titolare del trattamento ed il responsabile della protezione dei dati di A.S.L.3?

Il Titolare del trattamento è l'Azienda Socio Sanitaria Ligure 3 con sede in Via Bertani 4 – 16125 Genova (**indirizzo PEC:** protocollo@pec.asl3.liguria.it)

Il R.P.D. è contattabile ai seguenti **indirizzi di posta:** Via Bertani 4 – 16125 Genova ed alla **PEC aziendale** protocollo@pec.asl3.liguria.it.

I dati di contatto dello stesso sono pubblicati anche sul sito aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy.

ALLEGATO G: INFORMATIVA SERVIZIO CONSEGNA REFERTI ON LINE

CONSEGNA REFERTI ON LINE

Informativa ex art. 13 e 14 del Regolamento Europeo n. 679/2016 e norme di armonizzazione

Egr. Sig./Sig.ra

La ASL 3, Titolare del trattamento, La informa, **ex art. 13 e 14 del** Regolamento Europeo n. 679/2016 e norme di armonizzazione ed ai sensi delle "Linee Guida in tema di referti on line del 19/11/2009 dell'Autorità Garante per la protezione dei dati personali", fatte proprie dal Titolare, in quanto compatibili con detta normativa, quale policy aziendale, nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale, che è disponibile il servizio di consegna dei referti on line, che consente l'accesso, la consultazione e la stampa dei Suoi referti di laboratorio tramite il portale internet della Regione Liguria, all'indirizzo "refertionline.regione.liguria.it", al fine di rendere più rapidamente conoscibile il risultato clinico dell'analisi effettuata.

ASL 3 tratta le categorie particolari di dati personali ed i dati personali in base al Regolamento Regionale 9 aprile 2013 n. 2 "Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione". In detto Regolamento (pubblicato sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) ed, in particolare, nelle relative schede dei trattamenti sono indicate le normative di riferimento che costituiscono la base normativa dei trattamenti effettuati da questa ASL, da intendersi qui richiamate dal Titolare.

Detto Regolamento viene allo stato mantenuto e fatto proprio dal Titolare quale elenco di trattamenti, tipologie di dati, finalità di trattamento, riferimenti normativi che legittimano i trattamenti e destinatari di comunicazioni afferenti i dati trattati dall'Azienda, nelle aree di afferenza ed a miglior dettaglio del registro dei trattamenti agli atti in formato elettronico dell'Azienda, in quanto compatibili con la normativa europea e le disposizioni attuative della stessa a livello nazionale e/o regionale.

Per utilizzare il servizio di consegna on line, ad ogni accesso per l'esecuzione di esami di laboratorio analisi dovrà essere manifestato uno specifico consenso, a fronte del quale le verrà consegnato uno specifico codice d'accesso al servizio. Trattandosi di un servizio facoltativo, Lei potrà, comunque, scegliere di ritirare il referto con le modalità tradizionali e, pertanto, attraverso il ritiro dello stesso presso gli sportelli dell'Azienda.

I dati da Lei rilasciati per accedere al servizio di consegna on line saranno utilizzati sia in modo manuale che informatizzato dal personale debitamente individuato quale autorizzato al trattamento dei dati e saranno conservati in luogo idoneo ed appropriato, tutelandone la riservatezza, nel rispetto del segreto professionale e d'ufficio.

Il servizio di consegna on line dei referti prevede anche che, a fronte di un Suo specifico consenso, manifestato anch'esso di volta in volta, le venga inviato, al numero di cellulare da Lei indicato, un SMS con il quale verrà avvisato/a che il referto è pronto ed accessibile on line e con il quale Le saranno comunicati i valori INR.

I suoi dati verranno trattati nel rispetto delle misure di sicurezza disposte dal Titolare ASL 3, utilizzando protocolli di comunicazione sicuri, al fine di ridurre al minimo il rischio di perdita o di distruzione dei dati contenuti nei referti. Il referto sarà disponibile per un periodo massimo di 30 giorni, trascorso il quale non sarà più accessibile.

Sono in ogni caso esclusi dalla consegna on-line dei referti quelli relativi ad analisi genetiche e quelli relativi agli accertamenti sull'HIV, nel rispetto della tutela dei diritti della persona e della sua dignità.

In ogni momento potranno essere esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 e norme di armonizzazione, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme di armonizzazione ("**Diritto alla cancellazione"- «diritto all'oblio»)** , la limitazione del trattamento, se ricorrano le ipotesi di cui all'art. 18 del Regolamento UE 679/2016 e norme di armonizzazione **("Diritto di limitazione di trattamento"),** l'opposizione al loro trattamento ai sensi dell'art. 21 del regolamento UE 679/2016 e norme di armonizzazione **("Diritto di opposizione")** nonché il diritto alla portabilità dei dati.

Inoltre ha diritto di proporre reclamo all'autorità di controllo (Autorità Garante per la protezione dei dati personali- secondo le modalità previste sul sito internet dello stesso www.garanteprivacy.it) nei casi previsti dalle disposizioni in materia di protezione dei dati di cui al Regolamento UE 679/2016 e norme di armonizzazione.

Il Titolare del trattamento è l'Azienda Socio Sanitaria Ligure 3 con sede in Via Bertani 4 – 16125 Genova (**indirizzo PEC:** protocollo@pec.asl3.liguria.it)

Il R.P.D. è contattabile ai seguenti indirizzi di posta: Via Bertani 4 – 16125 Genova ed alla **PEC aziendale**: protocollo@pec.asl3.liguria.it.

I dati di contatto dello stesso sono pubblicati anche sul sito aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy.

ALLEGATO H: MODELLO RACCOLTA CONSENSO SERVIZIO CONSEGNA REFERTI ON LINE

MODULO RACCOLTA CONSENSO

ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i(1)

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno, altro –precisare-) (2)

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa di cui agli artt. 13 e 14 del Regolamento U.E. 679/2016 e norme di armonizzazione in materia di protezione dei dati personali ed:

☐ esprimo il consenso alla consegna del mio referto di laboratorio on line

☐ esprimo il consenso al fine di utilizzare il seguente numero di cellulare_____per avvisarmi che il referto di laboratorio è disponibile on line e per comunicarmi i valori INR attraverso SMS

☐ esprimo il consenso al trattamento dei dati personali e/o particolari che verranno trattati per fini diagnostici e terapeutici e per finalità connesse di tipo amministrativo-contabile e di monitoraggio dell'attività. L'eventuale rifiuto da parte dell'interessato di conferire dati personali e particolari per finalità di diagnosi e cura, può comportare l'impossibilità per l'azienda di erogare le prestazioni richieste.

Il trattamento dei dati avverrà mediante supporto cartaceo e mediante strumenti elettronici; l'accesso ed il trattamento dei dati sono consentiti solo al personale autorizzato, nel rispetto delle vigenti disposizioni in materia di tutela dei dati personali e con l'adozione delle misure di sicurezza predisposte dal Titolare ASL 3.

Genova, ___/___/___ Firma dell'interessato

_____

_____

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat…….....n…….

Rilasciata da ……......il……

Firma dell'operatore incaricato

[1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: "Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera."

Art. 76, D.P.R. n. 445/2000 e s.m.i.: "Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L'esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[2] Precisare la qualità ed allegare documentazione comprovante la qualità.

ALLEGATO I: INFORMATIVA CUP UNICO REGIONALE

INFORMAZIONI AGLI UTENTI RIGUARDO AL TRATTAMENTO DATI UTILIZZATI DAL CENTRO UNICO DI PRENOTAZIONE REGIONALE

ex artt. 13 e 14 del Regolamento Europeo 2016/679

Regolamento Generale sulla protezione dei dati personali

Gent.ma/Egregio utente,

ai sensi degli artt. 13 e 14 del Regolamento Europeo 2016/679 Regolamento Generale per la protezione dei dati personali (in seguito Regolamento Europeo) desideriamo informare la S.V. che le AA.SS.LL. e gli Enti/Istituti del Servizio Sanitario Regionale (IRCCS Ospedale Policlinico San Martino, E.O. Ospedali Galliera, Ospedale Evangelico Internazionale), quali Titolari del trattamento, al fine di garantire una miglior integrazione della propria offerta sanitaria ed una risposta più celere ai cittadini, hanno uniformato il servizio CUP a livello regionale e conseguentemente l'erogazione della presente informativa e la raccolta del relativo consenso nonché l'acquisizione e la registrazione dei dati anagrafici, di contatto e di salute indispensabili ad erogare la prenotazione delle prestazioni richieste dal cittadino, nel rispetto degli adempimenti istituzionali, degli obblighi di legge, regolamentari, ovvero previsti da normative nazionali e comunitarie, garantendo il rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato.

1. FINALITÀ DEL TRATTAMENTO

La raccolta dei suoi dati è finalizzata a permettere l'effettuazione e la registrazione delle prenotazioni per prestazioni sanitarie erogate dalle AA.SS.LL. e dagli Enti/Istituti del Servizio Sanitario Regionale nonché dalle farmacie e dai Medici di Medicina Generale (MMG)/Pediatri di Libera Scelta (PLS) aderenti al progetto regionale.

Attraverso il Centro Unico di Prenotazione Regionale (CUP), Lei potrà usufruire, in modo contestuale, delle agende delle Aziende Sociosanitarie e degli Enti/Istituti del Servizio Sanitario Regionale sopra indicati nonché dei soggetti privati convenzionati. Tale modalità operativa permetterà di avere un quadro complessivo delle possibilità esistenti per la prenotazione della prestazione di suo interesse nell'ambito dell'intero territorio regionale.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, di tale ulteriore trattamento fornirà all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

2. BASE GIURIDICA DEL TRATTAMENTO

A titolo esemplificativo si riportano i principali riferimenti normativi.

<u>Normativa nazionale</u>:

Decreto Presidente del Consiglio dei Ministri del 29.11.2001 ad oggetto: "Definizione dei livelli essenziali di assistenza";

Decreto Ministeriale 08.07.2011 ad oggetto "Erogazione da parte delle farmacie, di attività di prenotazione delle prestazioni di assistenza specialistica ambulatoriale, pagamento delle relative quote di partecipazione alla spesa a carico del cittadino e ritiro dei referti relativi a prestazioni di assistenza specialistica ambulatoriale";

Piano triennale 2017 2019 per l'informatizzazione della P.A. di AgID;

Sistema CUP Linee guida nazionali del 27.10.2009 emanato dal Ministero del Lavoro, della Salute e delle Politiche Sociali;

Piano Nazionale di Governo delle liste di attesa 2016-2018.

Normativa regionale:

Legge regionale n. 17/2016 ad oggetto "Istituzione dell'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.) e indirizzi per il riordino delle disposizioni regionali in materia sanitaria e socio-sanitaria";

Deliberazione del Commissario Straordinario di A.Li.Sa. n. 59 del 23.06.2017 ad oggetto "Approvazione nuovo Accordo per la distribuzione di farmaci da parte delle farmacie pubbliche e private convenzionate in nome e per conto del SSR e per lo sviluppo della loro integrazione nella fornitura del servizio CUP-WEB nelle Aziende socio sanitarie locali 1,2,3,4,5 con efficacia dal 1 ottobre 2017 - proroga al 30 settembre 2017 dell'Accordo quadro per la DPC e il servizio CUP-WEB sottoscritto il 31 marzo 2017";

Deliberazione del Consiglio della Regione Liguria n. 21 del 05.12.2017 ad oggetto "Approvazione del Piano Socio Sanitario Regionale 2017-2019".

Accordo integrativo tra Regione Liguria e OO.SS. Medici di Medicina Generale per la realizzazione del progetto di prenotazione CUP presso lo studio del medico di assistenza primaria convenzionato, sottoscritto in data 31.01.2018.

3. TIPOLOGIA DI DATI TRATTATI

Le informazioni conferite e trattate rientrano nella definizione di "dato personale", di cui all'art. 4 par. 1 n.1 (quali nome, cognome, indirizzo e dati di contatto in generale), di "dato relativo alla salute", di cui al par. 1 n. 15, e nell'ambito dell'art. 9 del Regolamento Europeo e possono altresì riguardare dati soggetti a maggior tutela quali previsti dalle disposizioni nazionali.

I dati raccolti concernono, inoltre:

- ✓ Data di nascita;
- ✓ Codice fiscale;
- ✓ Numero e data dell'impegnativa;
- ✓ Codice di esenzione eventualmente presente;
- ✓ Codice di priorità, se barrato dal medico;
- ✓ Tipologia esame/visita richiesti;
- ✓ Eventuale quesito diagnostico;
- ✓ Correttezza dei recapiti telefonici e di altro genere presenti in procedura.

Le informazioni richieste sono necessarie per poter completare il percorso di prenotazione della prestazione sanitaria.

In caso di prenotazione di visita attraverso il sistema CUP oltre ai sopra citati dati personali, Le potrà essere richiesto anche un numero di telefono personale, fisso o cellulare e un indirizzo di posta elettronica che potranno essere utilizzati, tramite il c.d. servizio Recall, fino a Sua diversa indicazione, per confermarLe e/o ricordarLe il giorno della prenotazione, per avvisarLa in caso di annullamento della visita, per consentirLe di disdire in tempo l'appuntamento nel caso non fosse più di suo interesse nonché per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica.

4. AMBITO DI TRATTAMENTO DEI DATI

L'ambito di trattamento dati attraverso il Centro Unico di Prenotazione Regionale, anche tramite servizio di Call Center unificato, riguarda:

a) attività di prevenzione, diagnosi, cura e riabilitazione, ivi compresi servizi diagnostici, programmi terapeutici e qualsivoglia altro servizio erogato dalle Aziende Sociosanitarie e dagli Enti/Istituti del S.S.R. in caso di prestazioni specialistiche ambulatoriali;
b) attività amministrative/contabili e di gestione operativa legate ai servizi forniti, ivi comprese quelle connesse al processo di iscrizione al Servizio Sanitario Regionale, di prenotazione/spostamento/annullamento appuntamenti per visite ed esami;
c) Servizio di Recall attraverso una telefonata automatizzata oppure via mail che Le ricorderà, mediante opportuno messaggio preregistrato, il Suo appuntamento ai fini inerenti la conferma oppure la disdetta dello stesso.
   Ciò allo scopo di ottimizzare i tempi di risposta ai bisogni di salute e ridurre le liste di attesa per le prestazioni specialistiche ambulatoriali.

   Per il buon esito del suddetto servizio, si consiglia, al momento della prenotazione, di confermare all'operatore il proprio numero telefonico.

Per favorirLa nel ritiro dei referti di alcune prestazioni diagnostiche, potranno essere attivati, fino a Sua diversa indicazione, sistemi di consegna presso le farmacie liguri aderenti all'iniziativa ovvero tramite portale.

5. MODALITÀ DEL TRATTAMENTO DEI DATI E MISURE DI SICUREZZA

Il trattamento dei dati è effettuato da personale sanitario ed amministrativo comunque autorizzato.

Il trattamento è eseguito con strumenti manuali ed informatici, osservando misure di sicurezza idonee in grado di garantire che esclusivamente il personale autorizzato possa conoscere le informazioni inerenti il cittadino, necessarie all'attività in parola, secondo il principio di minimizzazione del dato e di ridurre al minimo i rischi di perdita, distruzione o accesso non autorizzato ai suoi dati a norma del Regolamento Europeo con particolare riferimento alla cernita, al trasferimento, alla conservazione e al ripristino, quali fissate dal Regolamento e dalle norme europee, dalle norme italiane con particolare riferimento al Codice di Amministrazione Digitale (CAD ossia al D. Lgs. n. 82/2005 e ss.mm.ii), e specificamente alle cosiddette misure standard, laddove applicabili.

La prenotazione tramite CUP può essere effettuata mediante gli sportelli ubicati presso le AA.SS.LL. e gli Enti/Istituti del Servizio Sanitario Regionale nonché presso le farmacie del terri-

torio, gli studi della Medicina Generale, altri soggetti pubblici e privati aderenti al progetto e tramite servizio di call center unificato.

Nel caso di prenotazione per via telefonica, al numero verde unico regionale, è rilasciata breve informativa vocale pre-registrata che rinvia a quella estesa, pubblicata nei rispettivi siti web istituzionali delle AA.SS.LL. e degli Enti/Istituti del Servizio Sanitario Regionale.

6. NATURA OBBLIGATORIA O FACOLTATIVA DEL CONFERIMENTO DEI DATI

Il conferimento dei dati di cui al precedente punto 3 è facoltativo in relazione alle finalità sopra evidenziate ancorché necessario all'esecuzione della prestazione richiesta. Il mancato conferimento comporterà infatti per i centri di prenotazioni unificati l'impossibilità di procedere alla registrazione della prenotazione e alla erogazione della prestazione richiesta.

Al fine di evitare ripetute richieste di "consenso al trattamento dati a fini privacy" ossia in relazione ad ogni singolo accesso al sistema unificato di prenotazione, in conformità a quanto legislativamente previsto, Lei potrà manifestare il Suo consenso con un'unica dichiarazione. Si evidenzia che tale consenso sarà valido per tutti i centri attivi di prenotazione unificata in Regione Liguria gestiti dal SSR ovvero dai soggetti sopraccitati aderenti al progetto (MMG Farmacie etc.) ed efficace fino a revoca dello stesso e, per i minorenni, fino al compimento del 18° anno di età. La revoca del consenso può avvenire in qualsiasi momento compilando il relativo modulo e consegnandolo presso una delle Aziende/Enti. Presta il consenso o la revoca soltanto l'interessato al quale i dati sanitari si riferiscono. Se si tratta di minore o persona sotto-tutela possono prestare il consenso o revocarlo solo i soggetti che esercitano la legale rappresentanza.

7. CATEGORIE DI INTERESSATI

Gli interessati sono gli utenti registrati presso l'anagrafe sanitaria del Servizio Sanitario Regionale Ligure e, nel rispetto della vigente normativa, di altre Regioni, che richiedono ed a cui vengono erogate le prestazioni sanitarie, ivi inclusi, nell'ambito degli accordi internazionali, i soggetti non aventi nazionalità italiana iscritti presso l'anagrafe sanitaria.

8. CONDIVISIONE E COMUNICAZIONE DEI DATI

I suoi dati possono essere condivisi e comunicati, quando ciò risulti necessario, in relazione all'erogazione del servizio CUP ad altri soggetti compresi nella rete CUP regionale quali, a titolo esemplificativo e non esaustivo, strutture e farmacie convenzionate, altri soggetti pubblici e privati aderenti al progetto, nei casi e con i limiti previsti dalla vigente normativa ovvero obbligatori per legge.

9. PERIODO DI CONSERVAZIONE

Ai sensi dell'art. 5, par. 1, lett. e) del Regolamento Europeo i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali sono conservati sino a revoca e comunque per l'intera durata dell'iscrizione dell'utente alla anagrafe sanitaria Ligure ov-

vero per i fini di cui all'articolo 89, paragrafo 1 del Regolamento Europeo, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal Regolamento Europeo a tutela dei diritti e delle libertà dell'interessato ("limitazione alla conservazione").

10. DIRITTI DELL'INTERESSATO

Di seguito sono indicati e descritti i diritti che Le competono:

- Accedere ai propri dati e conoscere chi vi ha avuto accesso (art. 15 Regolamento Europeo);
- Richiedere l'aggiornamento, la rettifica o l'integrazione dei dati (art. 16 Regolamento Europeo);
- Richiedere la cancellazione, la trasformazione in forma anonima dei dati, il loro blocco e la limitazione del trattamento se trattati in difformità dalla legge, fatti salvi gli obblighi legali di conservazione (artt. 17 e 18 del Regolamento Europeo);
- Ricevere, (se possibile) in formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento unitamente al diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
  - ✓ Il trattamento si basi sul consenso ai sensi dell'art. 6, paragrafo 1, lettera a), o dell'art. 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'art. 6 paragrafo 1, lettera b);
  - ✓ Il trattamento sia effettuato con mezzi automatizzati (art. 20 del Regolamento Europeo);
- Opporsi, per motivi legittimi, al trattamento dei dati (art. 21 del Regolamento Europeo);

Ai sensi dell'art. 13 par. 2 lette. D) e dell'art. 14 par. 2 lett. e) rimane impregiudicato il Suo diritto di rivolgere reclamo al Garante della protezione dei dati personali secondo le modalità descritte nel sito www.garanteprivacy.it.

11. I TITOLARI DEL TRATTAMENTO

- ✓ A.S.L. 1, con sede in Via Aurelia Ponente, 97 18038 Bussana di Sanremo (IM);
- ✓ A.S.L. 2, con sede in Via Manzoni, 14 17100 Savona (SV);
- ✓ A.S.L. 3, con sede in Via Bertani, 4 16125 Genova (GE);
- ✓ A.S.L. 4, con sede in Via G.B. Ghio, 9 16143 Chiavari (GE);
- ✓ A.S.L. 5, con sede in Via XXIV Maggio, 139-19124 La Spezia (SP);
- ✓ IRCCS Ospedale Policlinico S. Martino, con sede in Largo R. Benzi 10- 16132 Genova (GE);
- ✓ Ente Ospedaliero Ospedali Galliera, con sede in Mura delle Cappuccine, 14- 16128 Genova (GE);
- ✓ Ospedale Evangelico Internazionale, con sede in Salita Superiore San Rocchino, 31/A – 16122 Genova (GE).

12. I RESPONSABILI PER LA PROTEZIONI DEI DATI

sono contattabili ai seguenti indirizzi di posta elettronica:

- ✓ A.S.L. 1: f.lotito@asl1.liguria.it;

- ✓ A.S.L. 2: a.calo@asl2.liguria.it;
- ✓ A.S.L. 3: protocollo@pec.asl3.liguria.it;
- ✓ A.S.L. 4: dpo@asl4.liguria.it;
- ✓ A.S.L. 5: privacy@asl5.liguria.it;
- ✓ IRCCS Ospedale Policlinico S. Martino: giovanni.orengo@hsanmartino.it
- ✓ Ente Ospedaliero Ospedali Galliera: dpo@galliera.it;
- ✓ Ospedale Evangelico Internazionale: rpd@oeige.org.

13. IL RESPONSABILE INFORMATICO DEL TRATTAMENTO DATI

Liguria Digitale Via Melen 77 16152 Genova

14. I RESPONSABILI DEL TRATTAMENTO DATI CUP

Farmacie, Medici di Medicina Generale, Pediatri di Libera Scelta, Specialisti aderenti al progetto e la Cooperativa Sociale La Cruna quale gestore del Servizio di Call Center.

15. GLI AUTORIZZATI DEL TRATTAMENTO DATI sono le persone fisiche specificamente designate dalle Strutture Sanitarie Pubbliche e dai soggetti aderenti al progetto comunque vincolate al segreto professionale ovvero tenute alla riservatezza.

ALLEGATO L

ACCORDO TRA CONTITOLARI PER IL TRATTAMENTO DATI

(E*x art. 26 Regolamento U.E. 679/2016 e norme di armonizzazione)*

Parti

Il presente accordo è concluso tra ASL 3, direttamente, in persona del legale rappresentante pro tempore e con delega alla sottoscrizione dello stesso da parte del dirigente responsabile della S.C……., da ora in avanti anche Titolare e [**********], in persona di……../ del legale rappresentante pro tempore……, da ora in avanti anche Contitolare.

Premessa

Con deliberazione [********]

Oggetto del presente Accordo è l'instaurazione di un rapporto di Contitolarità in riferimento ai trattamenti afferenti il rapporto sostanziale contrattuale/convenzionale conseguente alla suddetta deliberazione.

Ciascuno dei Contitolari necessita dei dati strettamente necessari alle finalità di trattamento di cui all'Allegato A ed ivi individuati al fine di dar corso alle prestazioni oggetto di rapporto contrattuale/ convenzionale;
ASL 3 e……., quali Contitolari di tali dati, sono necessitati a conferirli, al fine di consentire la corretta erogazione delle prestazioni di cui trattasi.

L'attività sostanziale, sottesa al presente Accordo, resta nell'esclusiva responsabilità di ciascuno dei Contitolari per quanto di rispettiva competenza, ai sensi del sopra citato rapporto contrattuale/ convenzionale.

Tramite il presente accordo le parti intendono regolare il proprio rapporto in relazione alle attività di trattamento di dati personali e categorie particolari di dati personali, con particolare attenzione alla protezione dei dati.

Gli allegati formano parte integrante del presente Accordo.

Definizioni

La terminologia del Data Processing Agreement si rifà a quanto definito dal Regolamento UE 679/2016 ed alle relative norme di armonizzazione

In particolare si forniscono le seguenti definizioni:

«Regolamento»: REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

«Titolare o Titolare del trattamento»: 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;

«Responsabile o Responsabile esterno 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;

«Subresponsabile o Subresponsabile esterno del Trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto di un Responsabile o Subresponsabile;

«Autorizzati o Autorizzati al trattamento»: le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal responsabile;

«Contitolari del Trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, con conseguente esercizio di potere decisorio, scelte, potere di ordine, di direttiva vincolante e di controllo;

«Accordo»: il presente atto.

Obblighi dei contitolari.

Principi generali

I Contitolari mettono in atto misure tecniche e organizzative affinché i trattamenti svolti sotto la rispettiva responsabilità, in funzione e nel rispetto dei relativi scopi anche istituzionali, ma **in condivisione di dati, finalità e mezzi di trattamento**, soddisfino i requisiti della normativa di settore, con particolare attenzione alla tutela dei diritti e libertà dell'interessato.
Essi utilizzano i dati personali e categorie particolari di dati personali oggetto di trattamento solo per le **finalità** indicate **nell'Allegato A** "Attività di trattamento" in forza del rapporto contrattuale/ convenzionale sopra citato, se necessari ed indispensabili a dar corso allo stesso e con i **mezzi, strumenti e le modalità** evidenziati in esso.
Con la sottoscrizione del presente Accordo i Contitolari si assumono gli impegni a garantire e garantiscono quanto di seguito riportato, mantenendo autonomi poteri decisori, di direttiva e di controllo nei propri ambiti di competenza.

Obblighi generali

I Contitolari si impegnano a garantire e garantiscono:

1. di trattare i dati in ottemperanza ai principi sanciti:
- dall'ordinamento nazionale ed europeo in materia di protezione dei dati;
- dall'articolo 5 del Regolamento UE 679/2016 e norme di armonizzazione;

2. di inviarsi reciprocamente, con cadenza annuale, l'elenco aggiornato degli eventuali Amministratori di Sistema e degli eventuali terzi affidatari, designati Responsabili del trattamento dei dati afferenti al presente Accordo ;

3. di comunicarsi reciprocamente il luogo fisico di archiviazione dei dati sottoposto ad allocazione vincolante all'interno del territorio italiano, nonché le modalità di loro conservazione (backup e architetture di *Disaster Recovery*) ovvero, fermo restando quanto precede, le eventuali allocazioni su *cloud,* i relativi dati di sicurezza, declinando le generalità del provider/gestore responsabile esterno;

4. di attenersi ai criteri di segretezza e tutela nella gestione dei dati di cui trattasi, utilizzandoli al solo scopo di erogare le prestazioni di cui trattasi;

5. di non trattare i dati dell'interessato/utente oltre al tempo strettamente necessario ad espletare l'attività di competenza ed i connessi adempimenti amministrativo-contabili inerenti/derivanti;

6. di somministrare all'interessato/utente adeguata informativa e registrarne/acquisirne il consenso, ove previsto dalla vigente normativa nazionale e/o europea, con obbligo di condivisione preventiva con il Contitolare e conservazione insieme alla documentazione relativa all'interessato/utente per le prestazioni di afferenza e di dare ivi informativa relativamente alla Contitolarità di cui al presente Accordo, con particolare riguardo alle modalità di esercizio dei diritti dell'interessato/utente ed ai dati di contatto del R.P.D e/o referente privacy.

Ciascun Contitolare è tenuto a rispondere direttamente, a tutti gli effetti di legge, con manleva totale del Contitolare per eventuali violazioni di norme, inadempimenti giuridici, inosservanze regolamentari, nonché per i danni inerenti / derivanti dai trattamenti dati di cui trattasi di rispettiva competenza, per i quali l'altro Contitolare possa essere chiamato a rispondere, sia civilmente, sia in punto privacy.

Collaborazione

Ciascun Contitolare mette a disposizione dell'altro tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente accordo.

Tenuta del registro delle attività di trattamento

Ciascun Contitolare si impegna a redigere per iscritto, se previsto per legge, un registro delle attività di trattamento di cui trattasi per i trattamenti di afferenza, che contenga almeno le informazioni di cui all'art 30.2 del Regolamento UE 679/2016.

Comunicazione a terzi

Ciascun Contitolare deve rispettare il divieto assoluto di diffusione, condivisione, comunicazione a terzi e di trasferimento dati a soggetti situati in paesi terzi (extra UE), con particolare attenzione a soggetti giuridici afferenti l'indotto delle prestazioni sanitarie e sociali ovvero la fornitura/ commercializzazione di beni e servizi ad essa afferenti.

Se il Contitolare intendesse comunque trasferire tutti o alcuni dati personali oggetto dell'Accordo verso un paese terzo o un'organizzazione internazionale, si impegna ad informare il Contitolare prima di procedere al trasferimento, fornendo indicazioni sulla base legale che legittima il trasferimento.

Ricorso a Responsabili esterni

Ciascun Contitolare può nominare responsabili esterni in relazione ai trattamenti di cui trattasi, nel rispetto delle previsioni di cui al regolamento europeo 679/2016 e norme di armonizzazione, mettendo a disposizione a richiesta del Contitolare i relativi dati di contatto.

Riservatezza dei dati trattati

Ciascun Contitolare ***si impegna a garantire e garantisce*** di mantenere la segretezza e riservatezza riguardo a dati e informazioni personali e non ai quali abbia avuto accesso in virtù del presente Accordo anche dopo il termine dello stesso.
Ciascun Contitolare ***si impegna a garantire e garantisce*** che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza od abbiano un adeguato obbligo legale di riservatezza.

Autorizzati al trattamento

Ciascun Contitolare ***si impegna a garantire e garantisce*** di:

- individuare tra i propri collaboratori, quelli che compiono operazioni di trattamento dati personali e categorie particolari di dati personali e nominarli quali persone autorizzate al trattamento;
- dare le istruzioni agli Autorizzati al trattamento circa gli obblighi previsti dalle vigenti disposizioni in materia di privacy;
- adoperarsi al fine di rendere effettive le suddette istruzioni, curando in particolare il profilo della riservatezza, della sicurezza di accesso e dell'integrità dei dati;

- stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli Autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persona fisiche.

Diritti dell'interessato

Ciascun Contitolare adotta misure tecniche e organizzative adeguate atte a dare seguito alle richieste di esercizio dei diritti da parte degli interessati/utenti di cui al capo III del Regolamento UE 679/2016 tra le altre:

- Diritti di accesso, rettifica, cancellazione e opposizione;
- Diritto alla limitazione del trattamento;
- Diritto alla portabilità dei dati;
- Diritto di opposizione ad un processo decisionale automatizzato relativo alle persone fisiche;
- Violazione dei dati personali.

Ciascun Contitolare si impegna ad informare l'interessato/utente sulle modalità utilizzate per conservare i dati in modo da consentire la sua identificazione per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e/o successivamente trattati, avendo cura di applicare, in caso di conservazione digitalizzata, le norme vigenti in materia.

L'interessato/utente può esercitare i propri diritti nei confronti di e contro ciascuno dei Contitolari.

Ciascun comunque ***si impegna a garantire e garantisce:***

- di comunicare, a richiesta dell'altro Contitolare, in caso di esercizio dei diritti di cui e agli artt. da 15 a 21 e 23 del Regolamento UE n. 679/2016, i dati inerenti i file di log di accesso in formato intellegibile al fine di consentire la loro esibizione, come previsto all'interno del sopraccitato Regolamento UE.

Su richiesta di un Contitolare o di un interessato/utente , l'altro Contitolare dà seguito direttamente e tempestivamente a dette richieste di esercizio dei diritti, dandone contestualmente comunicazione al Contitolare.

In caso di violazione, fuga o perdita di dati personali, Ciascun Contitolare del trattamento, contestualmente agli adempimenti previsti dal regolamento UE 679/2016 e norme di armonizzazione, informa l'altro Contitolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Nell'informare il Contitolare comunica le seguenti informazioni:

- Descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di dati personali oggetto della violazione;
- il nome ed i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere ulteriori informazioni;

- descrizione delle misure adottate per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi sui diritti e libertà delle persone fisiche;
- descrizione delle probabili conseguenze della violazione dei dati personali.

Valutazione d'impatto

Se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto del presente Accordo, i Contitolari si impegnano a collaborare nella redazione della Valutazione d'impatto sulla protezione dei dati e negli adempimenti conseguenti previsti dalla vigente normativa.

Consultazione preventiva

Se si rende necessaria la Consultazione preventiva dell'Autorità di Controllo, in merito alle attività di trattamento oggetto del presente Accordo, i Contitolari collaborano per la raccolta di tutte le informazioni necessarie e per la Redazione della Consultazione preventiva.

Responsabile della Protezione dei Dati

Ciascun Contitolare designa ai sensi dell'art. 37.1, un Responsabile della Protezione dei Dati (RPD) di cui al capo IV, Sezione 4, qualora rientrante nei casi previsti dall'art. 37.1 e, comunque, un referente Privacy e ne comunica i dati di contatto all'altro Contitolare.

Misure di sicurezza

Tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, ma anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, Ciascun Contitolare mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Ciascun Contitolare deve implementare misure che garantiscano:
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi in uso ai fini dello svolgimento delle Attività di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico;
- la verifica e valutazione periodica dell'efficacia delle misure tecniche e organizzative.

Nello specifico Ciascun Contitolare deve garantire comunque l'implementazione delle misure di sicurezza di carattere generale indicate nell'**Allegato B** "Misure di sicurezza".

Ciascun Contitolare comunque ***si impegna a garantire e garantisce:***

1. di osservare e applicare, anche per conto di eventuali terzi affidatari, le misure idonee alla sicurezza dei dati a norma del Regolamento UE n.679/2016 e relative norme di armonizzazione, con particolare riferimento all'applicazione del criterio di indispensabilità del dato nella cernita degli stessi;
2. di applicare, anche in caso di trattamento digitale dei dati, misure di sicurezza, volte ad eliminare o, comunque, a ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati personali e delle categorie particolari di dati personali trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle disposizioni contenute nel Regolamento U.E. 679/2016 e relative norme di armonizzazione;
3. di adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);
4. di comunicare per iscritto, in forma chiara, compiuta e specifica all'altro Contitolare entro e non oltre 60 giorni dal presente Accordo, le misure assunte a norma dello stesso, nonché, negli stessi termini e tempi, le modalità di conservazione dei dati, del loro ripristino, della gestione dei *data breach* e dei *file di log* relativi alla tracciabilità degli accessi;
5. di garantire il rispetto degli artt. da 32 a 36, con particolare riferimento all'art. 33 par. 2 del Regolamento UE n.679/2016 (*data breach*);
6. di comunicare per iscritto, in forma chiara, compiuta e specifica all'altro Contitolare le misure idonee alla sicurezza del dato, a norma del Regolamento UE n. 679/2016 e relative norme di armonizzazione;
7. di produrre acconcia documentazione scritta ovvero relazione circa il regolare adempimento di quanto sopra all'altro Contitolare e per esso al suo RPD.

Termine del rapporto

I termini di conservazione dei dati trattati sono definiti da ciascun Contitolare ai sensi della vigente normativa e ne viene data informativa all'interessato/utente nelle forme di legge in materia.

Ciò fatto salvo, la durata del presente Accordo segue il rapporto contrattuale/convenzionale sostanziale di cui in premessa a decorrere dall'effettiva attivazione dello stesso.
In caso di inadempimento di una delle parti agli obblighi derivanti dal presente Accordo, l'altra parte, previa formale diffida ad adempiere, in caso di persistente inadempienza nei termini as-

segnati, potrà procedere alla risoluzione-cessazione degli effetti del presente Accordo e del rapporto sostanziale sotteso, fatto salvo ed impregiudicato ogni diritto.

Obblighi del Titolare

Ciascun Contitolare fornisce ai propri autorizzati istruzioni precise sulle modalità di trattamento dei dati (come da presente Accordo e da **Allegato B**, sulle categorie di dati e sulla finalità per le quali vengono trattati.
Ciascun Contitolare garantisce che i dati siano stati raccolti in maniera lecita, per finalità determinate (indicate **nell'Allegato A**), e che i dati siano adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti.

Responsabilità

Ciascun Contitolare rimane responsabile delle attività di trattamento di cui al presente Accordo per le quali ha determinato finalità e mezzi del trattamento e manleva l'altro Contitolare da eventuali danni inerenti o derivanti dalla mancata osservanza delle presenti istruzioni e/o da comportamenti illeciti per fatto proprio o dei soggetti dei quali lo stesso si avvale.

Il presente Accordo potrà essere oggetto di revisione qualora successivamente alla sottoscrizione intervengano modifiche normative che comportino il suo adeguamento alla normativa nazionale e/o a quella europea.

Data e luogo _____

ASL 3

In persona del delegato del Legale Rappresentante

[********]

In persona del Legale Rappresentante

…….

Allegati

Allegato A: "Attività di trattamento"

[********]

Allegato B: "Misure di sicurezza" e "Istruzioni su mezzi e modalità trattamento" all'accordo relativo alle funzioni di Contitolare nel trattamento dei dati personali ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione:

INFORMAZIONI, MISURE DI SICUREZZA ED ISTRUZIONI OPERATIVE

Il Regolamento Europeo 679/2016 e norme di armonizzazione prevedono precisi obblighi per coloro che intendono procedere ad un trattamento di dati personali.

Tali obblighi si sostanziano in adempimenti dettagliati, omessi i quali scattano le sanzioni sia penali, sia amministrative, sia civili, poste a salvaguardia dei diritti tutelati.

La normativa in materia di protezione dei dati personali in oggetto individua tre figure fondamentali:

1. Il Titolare del trattamento;
2. Il Responsabile esterno del trattamento;
3. Gli autorizzati al trattamento
4. Il Responsabile per la Protezione dei Dati (R.P.D.).

Il **Titolare del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed 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 od i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.. E' Responsabile dell'attuazione dei precetti normativi previsti dalla Legge.

Il titolare del trattamento è la A.S.L. 3.

Il **Responsabile esterno del trattamento,** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. E'nominato dal titolare, nella persona del legale rappresentante pro-tempore anche tramite delega alla sottoscrizione e deve provvedere all'applicazione di tutti i compiti impartiti dal Titolare, nonché fornire, agli autorizzati al trattamento istruzioni in merito alle operazioni di raccolta e trattamento dei dati, nonché vigilare sulla corretta applicazione delle medesime.

L'**autorizzato al trattamento**, nominato dal Titolare o dal Responsabile esterno, anche tramite delega alla sottoscrizione, deve elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni impartite.

All'autorizzato del trattamento sono devoluti compiti volti a garantire una puntuale applicazione della vigente normativa in materia di protezione dei dati.

Il Responsabile per la Protezione dei dati Personali R.P.D: è una figura, obbligatoria nei casi previsti dal Regolamento U.E. 679/2016 e norme di armonizzazione, che sovraintende a tutte le attività di protezione dei dati e che costituisce il soggetto di raccordo con l'autorità di controllo (Autorità garante per la Protezione dei dati) e con gli interessati/utenti.

Questa comunicazione è l'allegato dell'Accordo di Contitolarità nel trattamento dei dati personali nell'ambito dei rapporti che La legano all'A.S.L. 3 individuati nello stesso.

Si ricorda che per trattamento si intende " 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"

Si fa presente che, per quanto riguarda il trattamento dei dati personali, lo stesso si considera lecito se ricorre almeno una delle seguenti condizioni (art. 6 comma 1 Regolamento Europeo 679/2016 e norme di armonizzazione):

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità, salvi i casi in cui non è richiesto ai sensi della medesima normativa (tra gli altri art.9.2 Regolamento Europeo 679/2016) e disposizioni di armonizzazione;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il Regolamento Europeo 679/2016 e norme di armonizzazione che regolano il trattamento dei dati personali prevede il trattamento di dati personali *(qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale)* e di dati c.d. "particolari" (che il D. Lgs. 196/2003 e s.m.i definiva quali"dati sensibili" e richiamati dall'art.9 del Regolamento Europeo 2016/679), *cioè i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.*

Il Contitolare è tenuto in relazione a detti trattamenti dati*:*

a) Ad effettuarli in modo lecito, corretto e trasparente e nel rispetto dei principi sanciti dal Regolamento UE 679/2016 e norme di armonizzazione;
b) a raccoglierli e registrarli per finalità determinate, esplicite e legittime, e successivamente a trattarli in modo che non siano incompatibili con tali finalità;
c) a verificare, ove possibile, la loro esattezza e, se necessario, aggiornarli;
d) a verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati;
e) a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte. In ogni operazione di trattamento andrà garantita la massima riservatezza;
a) a osservare scrupolosamente tutte le misure di sicurezza predisposte ed idonee ai sensi della vigente normativa in materia.

Nell'espletamento dell'Accordo di cui trattasi ciascun Contitolare e ciascun autorizzato dallo stesso, dovrà, inoltre:

1. adempiere agli obblighi di cui all'Accordo stesso;

2. collaborare con il R.P.D. Aziendale e con l'altro Contitolare per l'attuazione delle prescrizioni in materia di privacy;
3. attuare le misure di sicurezza informatiche e non informatiche idonee a rispettare le indicazioni del Regolamento Europeo 679/2016 e norme di armonizzazione ;
4. garantire il rispetto degli artt. da 32 a 36, con particolare riferimento all'art. 33 par. 2 del Regolamento UE n.679/2016 (*data breach*);
5. accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;
6. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto dalla normativa vigente, nei confronti dell'interessato;
7. conservare gli atti e documenti, contenenti dati personali utilizzati per lo svolgimento dei compiti propri, in contenitori muniti di serratura (cassetti, armadi, ecc.) e restituirli al termine delle operazioni di competenza. Sulla base di quanto sopra, in caso di allontanamento, anche temporaneo, dalla postazione di lavoro dei suoi autorizzati al trattamento, il Contitolare dovrà verificare che non vi sia la possibilità da parte di terzi, anche dipendenti, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
8. testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative volte a garantire la sicurezza dei trattamenti espletati;
9. in caso di utilizzo di strumento elettronico, lo stesso non dovrà mai essere lasciato incustodito e accessibile durante una sessione di trattamento. In particolare si ricorda che anche in caso di abbandono temporaneo della postazione di lavoro, il personal computer con il quale si sta operando un'operazione di trattamento dei dati dovrà essere spento, dopo aver effettuato il salvataggio dei dati oppure dovrà essere attivato lo screensaver con inserimento di password personale al fine di evitare la riapertura a terzi della sezione di trattamento in corso;
10. Sempre in caso di utilizzo di strumento elettronico, nel caso di informazioni memorizzate sulle memorie locali dei personal computer e affidate esclusivamente agli utenti, effettuare il tempestivo salvataggio dei dati;
11. Qualora il trattamento dei dati, la formazione e la comunicazione di documenti ed atti, avvenga con strumenti elettronici dovranno essere accuratamente applicate, tra le altre, le seguenti misure di sicurezza:
    -dovranno essere predisposte tutte le cautele necessarie per assicurare la segretezza della componente riservata della credenziale di autenticazione (codice associato a parola chiave o dispositivo di autenticazione conosciuto o in possesso e uso esclusivo del responsabile esterno e dei soggetti dallo stesso autorizzati);
    -la password personale dovrà essere modificata periodicamente e ogni qualvolta l'autorizzato al trattamento abbia motivo di ritenere che non sia di sua esclusiva conoscenza;
    -i supporti rimovibili (floppy disk, cd rom, chiavette USB, ecc.) su cui sono memorizzati copie di dati dovranno essere custoditi in appositi contenitori muniti di serratura (armadi, cassetti, ecc.), al fine di evitare accessi non autorizzati e trattamenti non consentiti o comunque custoditi in locali ad accessi autorizzati e chiusi a chiave;
    -i supporti rimovibili contenenti dati sensibili, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri autorizzati solo

se le informazioni precedentemente in essi contenute non sono intelligibili e in nessun modo tecnicamente ricostruibili.

12. mantenere aggiornate costantemente e conservare le informazioni contenute nel Registro dei Trattamenti di cui all'art.30.2 del Regolamento UE 679/2016 e norme di armonizzazione, qualora previsto per legge;
13. adottare le cautele previste per legge (anonimato) nel trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati (a titolo esemplificativo e non esaustivo: Legge n. 66/1996 Norme contro la violenza sessuale; Legge n. 269/1998 Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori quali nuove forme di riduzione in schiavitù; Legge n. 38/2006 Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet; Legge n. 135/1990 Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS; D.P.R. n. 309/1990 Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza; Legge n. 194/1978 Norme per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza; D.M. n. 349/2001 Regolamento recante: "Modificazioni al certificato di assistenza al parto, per la rilevazione dei dati di sanità pubblica e statistici di base relativi agli eventi di nascita, alla nati-mortalità ed ai nati affetti da malformazioni"; Legge n. 405/1975 Istituzione dei consultori familiari);
14. Collaborare con il Contitolare nella redazione della Valutazione d'impatto sulla protezione dei dati e negli adempimenti conseguenti, se si rende necessaria una Valutazione d'impatto sulla protezione dei dati, in merito alle attività di trattamento oggetto dell'Accordo;
15. Collaborare con il Contitolare ed il R.P.D. per l'evasione di eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati ed ulteriori esercizi di diritti su istanza dall'interessato ai sensi del Regolamento UE 2016/679 e norme di armonizzazione.
16. comunicare, a richiesta del Contitolare, in caso di esercizio dei diritti di cui e agli artt. da 15 a 21 e 23 del Regolamento UE n. 679/2016, i dati inerenti i *file di log* di accesso in formato intellegibile al fine di consentire la loro esibizione, come previsto all'interno del sopraccitato Regolamento UE;
17. inviare, con cadenza annuale, al Contitolare l'elenco aggiornato degli Amministratori di Sistema e degli eventuali terzi affidatari, designati Responsabili del trattamento dei dati afferenti l'Accordo;
18. comunicare al Contitolare il luogo fisico di archiviazione dei dati sottoposto ad allocazione vincolante all'interno del territorio italiano, nonché le modalità di loro conservazione (backup e architetture di *Disaster Recovery*) ovvero, fermo restando quanto precede, le eventuali allocazioni su *cloud*, i relativi dati di sicurezza, declinando le generalità del provider/gestore designato preventivamente a responsabile esterno;
19. Procedere all'individuazione di eventuali soggetti sotto propria responsabilità da autorizzarsi al trattamento dei dati personali o di categorie particolari di dati personali

e procedere alla loro autorizzazione al trattamento, completa di specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun autorizzato, nonché ciascun Contitolare dovrà vigilare, che l'accesso ai dati da trattare da parte degli autorizzati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni ciascun Contitolare dovrà anche verificare la permanente sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto procedere alla revoca delle stesse. La nomina ad autorizzato dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti , che effettuano trattamento dei dati inerente l'Accordo di cui trattasi.

Per quanto concerne la gestione degli archivi cartacei dovranno essere adottate misure di sicurezza idonee e comunque:

1. Tutti i documenti dovranno essere accuratamente custoditi all'interno degli appositi locali o contenitori amovibili muniti di serratura;
2. L'accesso all'interno degli archivi dovrà essere rigorosamente limitato alle persone autorizzate dal Contitolare ed addette a tale attività;
3. Deve essere vietato allontanarsi dagli archivi, dalla segreteria e dagli uffici lasciando i locali incustoditi;
4. Gli atti ed i documenti contenenti dati personali, utilizzati per lo svolgimento dei compiti propri devono essere conservati accuratamente in contenitori e/o locali muniti di serratura e restituiti al termine delle operazioni affidate;
5. Nessun dato potrà essere comunicato a terzi o diffuso, al di fuori di quanto previsto nell'Accordo di cui trattasi;
6. E' comunque vietata la diffusione dei dati inerenti lo stato di salute e la vita sessuale degli interessati;
7. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica e/o cessazione del rapporto sotteso all'Accordo.

Data e luogo _____

ASL 3

In persona del delegato del Legale Rappresentante

[********] In persona del Legale Rappresentante

…….

ALLEGATO M: REQUISITI MINIMI DI SICUREZZA

Nello schema seguente sono state descritte le modalità di implementazione relativamente ai requisiti di livello M, ovvero quelli che rappresentano per lo più lo stato attuale dell'Azienda.

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI: Sono stati analizzati solo i Requisiti Minimi

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Compliant Il blocco della connessione per i dispositivi non autorizzati è normato dal regolamento Aziendale Attualmente la ASL 3 dispone di inventari realizzati con sw differenti in base alle diverse categorie di dispositivi. Le postazioni di lavoro sono inventariate non automaticamente sulla piattaforma HP Service Manager che ne permette la gestione remota e il controllo delle postazioni e dei dispositivi (stampanti) connessi. Tale applicazione mantiene anche la correlazione tra pc/portatili e utenti ai quali sono assegnate le risorse. La console centralizzata dell'antivirus Symantec Endpoint Protection permette di visualizzare la lista di tutti i server e client con relativo	Aggiornare Il Regolamento Aziendale sull'utilizzo delle dotazioni informatiche per regolamentare oltre all' utilizzo dei dispositivi aziendali anche gli extraziendali eventuali e stabilendo le tipologie di dispositivi autorizzati esterni all'azienda (dispositivi connessi tramite VPN, dispositivi mobili connessi tramite wifi) Impedire l'accesso alla rete aziendale e VPN ai dispositivi che non sono inventariati e/o successivamente autorizzati. Attivare un servizio di autenticazione con utenza di Dominio

					indirizzo IP sulle quali tale sw è installato. L'inventario di tutti i sistemi server fisici e virtuali in gestione a Liguria Digitale viene mantenuto all'interno di un CMDB che contiene anche le informazioni di configurazione e del sw installato. L'inventario dei cellulari, smartphone e tablet aziendali è mantenuto in un elenco aggiornato manualmente: Esiste un inventario su foglio Excel degli apparati di rete installati e viene aggiornato manualmente. L'elenco degli elettromedicali attivi è contenuto all'interno di un censimento costantemente aggiornato in cui però non viene evidenziato la connessione in rete o stand-alone. Non è ammesso da Regolamento Aziendale sull'utilizzo delle dotazioni informatiche l'utilizzo in rete Aziendale l'utilizzo di dispositivi personali .	che separi la rete per i dispositivi aziendali da quella per i dispositivi personali, limitando questi ultimi alla sola navigazione Internet. Tracciare sul censimento delle apparecchiature elettromedicali l'eventuale collegamento in rete.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Compliant con le limitazioni di cui al punto 1.1.1 Il collegamento alla rete di ASL3 dei dispostivi autorizzati avviene dopo una procedura di inserimento manuale sulla piattaforma HP service Manager che ne garantisce la gestione cen-	Aggiornamento del preesistente regolamento relativo all'utilizzo delle attrezzature informatiche aziendali. Attivare un servizio di autenticazione con utenza di Dominio

					tralizzata. L'inventario contenuto nel CMBD viene aggiornato ogni qual volta si connette un nuovo server alla rete. L'aggiornamento dei nuovi apparati di rete connessi avviene manualmente	che separi la rete per i dispositivi aziendali da quella per i dispositivi personali, limitando questi ultimi alla sola navigazione Internet. In tal modo associando i dispositivi autorizzati a ciascun utente di dominio viene regolamentato l'accesso di dispositivi alla intranet anche via wifi.
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Compliant Su un foglio di calcolo è tenuta traccia di tutti gli ip statici in uso e relative macchine . Tale corrispondenza è confermata dalla Console Antivirus e su HP Service Manager dove applicabile.	Verifica e aggiornamento inventario. Per i dispositivi BYOD, tablet e smartphone vedi ABSC_ID 1.1.1. e 1.3.1.

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di	Compliant Esiste un elenco del software applicativi formalmente autorizzato.	Aggiornare l'elenco dei sw autorizzati ed inserirlo nel Regolamento Aziendale da aggiornare annualmente.

				software non compreso nell'elenco.	Le postazioni di lavoro sono configurate dagli amministratori di sistema e, poiché gli utenti non hanno diritti amministrativi, non è loro consentito installare software in autonomia. Il CMDB mantiene un catalogo delle applicazioni implementate e del software installati sui sistemi server.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Compliant relativamente al contesto autorizzativo: Attualmente non vengono eseguite scansioni temporizzate per verificare il software installato in quanto, non essendo gli utenti amministratori non possono installare nulla sulle postazioni di lavoro(vedi Regolamenti Aziendale utilizzo dotazioni informatiche) Sui server sono installati solamente i software strettamente necessari al funzionamento dei relativi servizi.	E' comunque in fase di test il modulo symantec per la verifica dei sw autorizzati su macchine MS e Linux (server e client). Non appena validato può essere attivato.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Compliant Sia le postazioni di lavoro che i server vengono installati con configurazioni standard tali da garantire un livello di sicurezza adeguato, prevedendo ad esempio un numero minimo di porte di rete aperte e disponibili. Quando rite-	Formalizzare e/o aggiornare la procedura di configurazione dei sistemi client e server. Pianificare la dismissione dei si-

					nuto necessario i sistemi vengono ulteriormente hardenizzati. Non è prevista una configurazione standard per quanto riguarda i dispositivi mobili.	stemi obsoleti che non permettono l'applicazione di configurazioni sicure (es. Windows XP).
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Compliant Esiste documento configurazioni standard	Ref. Action proposed ABSC 3.1.1 (Vedi Azione proposta ABSC 3.1.1.)
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Compliant I sistemi compromessi vengono ripristinati come da procedura a partire da immagini di backup integre.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Compliant Esistono copie offline delle immagini di installazione dei sistemi che possono essere utilizzate per effettuare verifiche di integrità.	Formalizzare in procedura la conservazione e manutenzione offline di immagini di installazione costantemente aggiornate ed implementare il livello S (3.3.2).
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Compliant Solo gli utenti autorizzati possono accedere alle immagini conservate su una macchina de-	

					dicata in rete con storage ridondato.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Compliant /partially compliant per apparati di rete. Tutti i sistemi sono amministrati attraverso connessioni protette e ritenute sicure (SSH, RDP, HTTPS). Rimangono in uso alcuni apparati di rete obsoleti nei quali l'amministrazione remota tramite canali crittografati non è supportata E' in fase di predisposizione una configurazione di un sistema ACS (Access Contro System) su server Radius per la gestione degli apparati di rete	Pianificare la dismissione degli apparati obsoleti (che non supportano l'amministrazione remota tramite canali crittografati). Attivare il sistema ACS attualmente in fase di predisposizione.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Compliant sono a disposizione strumenti automatici gestiti da Liguria Digitale in grado di rilevare eventuali vulnerabilità su tutti i sistemi. Tali ricerche e relativi report sono eseguiti a seguito di segnalazione di nuove vulnerabilità o di significative mo-	Nell'ambito del contratto di Gestione in outsourcing con Liguria Digitale, definire procedure formali di scansione sistematica della rete per l'implementazione del livello Standard di cui al punto 4.1.2.

					difiche della configurazione dei sistemi, su target critici in modo da non gravare significativamente sulle prestazioni della rete.	
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.		
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Compliant Gli strumenti di scansione delle vulnerabilità sono aggiornati in modo automatico.	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Compliant Nei sistemi Microsoft, WSUS gestisce la verifica e l'installazione automatica degli aggiornamenti critici e delle patch di sicurezza del sistema operativo e delle applicazioni Microsoft. La gestione delle patch sui sistemi server è semiautomatica al fine di garantire la continuità dei servizi attivi. Attualmente non esiste una gestione centralizzata delle patch relative alle applicazioni non Microsoft. Al fine di garantire la continuità dei servizi in ambito ospedaliero, gli aggiornamenti che possono rivelar-	Valutare eventuale pianificazione di aggiornamenti sistematici centralizzati per sistemi Linux

					si critici per applicazioni non interrompibili non sono installati automaticamente ma pianificati a seguito di esito positivo di test .	
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono presenti sistemi isolati dalla rete poiché non ne sussistono le necessità	Verificare la presenza e necessità di sistemi air-gapped nella'rea elettromedicale
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Compliant Il personale adibito alla gestione della sicurezza di Liguria Digitale informa il personale IT delle principali vulnerabilità e minacce e, in accordo con esso, pianifica e verifica l'esecuzione delle relative contromisure. Il documento programmatico sulla sicurezza aggiornato contiene l'analisi dei rischi dei dati trattati dall'Ente.	Aggiornare periodicamente l'analisi dei rischi contenuta nel DPS.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Ad oggi non è disponibile un'analisi dei rischi relativi alla cyber security.	Inserire nel DPS l'analisi del rischi
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Compliant Per i sistemi client e server la procedura automatica prevede l'applicazione di tutte le patch relative ai	Prevedere aggiornamenti sistematici delle patch di sicurezza anche direttamente sugli apparati elettromedicali in

					rischi di sicurezza e di quelle ritenute critiche.	rete.
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Compliant Sulle applicazioni critiche le patch vengono preventivamente testate per valutarne gli impatti (4.5.1)	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Compliant Le utenze di amministrazione sono assegnate solo a personale idoneo e competente. Gli utenti non possiedono privilegi amministrativi nemmeno sulle macchine a loro assegnate	
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Partially Compliant Gli amministratori di sistema di Liguria Digitale utilizzano utenze amministrative sui sistemi di ASL3 unicamente per lo svolgimento di attività di gestione. Gli amministratori di sistema dipendenti di ASL3 possiedono utenze amministrative per lo	

					svolgimento dell'intera attività lavorativa. I log degli accessi degli amministratori sono comunque raccolti da un sistema gestito da Liguria Digitale dai quali si possono tracciare gli accessi	
5	1	3	S	Partially Compliant Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Partially Compliant A livello di server esistono privilegi differenziati per ciascuna utenza amministrativa. Per quanto riguarda i privilegi di amministratore dei client è possibile assegnare i privilegi di amministratore su diversi gruppi di macchine a gruppi di utenze di amministratore diverse.	Valutare l'impatto di definizione di policy più granulari su tutti i client.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Compliant L'inventario delle utenze amministrative è aggiornato ad ogni nuova assegnazione e formalmente autorizzata . Esiste lettera di incarico per gli amministratori di sistema di Liguria Digitale che specifica la responsabilità verso i sistemi client e verso gli amministratori di sistema dipendenti di	

					ASL 3.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Compliant Prima di collegare alla rete un nuovo dispositivo le credenziali di amministratore predefinite vengono modificate secondo le policy delle password previste.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Compliant la lunghezza minima delle password degli amministratori attualmente non è impostata a 14 caratteri.	Formalizzare e impostare la lunghezza delle password di Amministratore a 14 caratteri con criteri di elevata robustezza. Verificare l'applicazione delle policy di robustezza delle password per i sistemi non gestiti centralmente.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Compliant Le policy MS impongono la modifica delle password almeno ogni 90 giorni, come prescritto dal Garante per la protezione dei dati personali.	Policy robustezza password vedi azioni proposte ABSC 5.7.1.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Compliant Le policy impediscono il riutilizzo delle ultime 4 password utilizza-	Policy robustezza password vedi azioni proposte ABSC 5.7.1.

					te.	
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non compliant Non viene applicato il controllo temporale per problemi gestionali (password smarrite, reset..)	Applicare la policy temporale a tutti gli utenti tranne che per gli amministratori di dominio ai quali è concessa la modifica delle password degli utenti per ripristini, reser etc.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Partially compliant (cedi 5.7.6) Non viene assicurato un tempo preciso ma viene impedito il restore delle ultime 3 password utilizzate	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Compliant Le utenze amministrative sono destinate esclusivamente ai gestori dei sistemi informativi e completamente distinte dalle utenze che non svolgono tali attività.	Vedi azioni proposte ABSC 5.1.2.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Compliant Sia le utenze standard che quelle amministrative sono personali . (All. B DLG 146/2003)	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di	Compliant Di norma le utenze amministrative "root" e "Administrator" sono	Formalizzare la procedura per l'utilizzo di utenze amministrative anonime in caso di emergenza che comprenda la custo-

				chi ne fa uso.	utilizzate solo in caso di emergenza.	dia delle password, la registrazione degli utilizzatori e la sostituzione della password.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Compliant Le credenziali amministrative sono conservate in busta chiusa accessibile ai soli amministratori di sistema in caso di necessità.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Compliant Attualmente non è prevista l'autenticazione mediante l'utilizzo di certificati digitali. In caso di necessità è tuttavia a disposizione presso Liguria Digitale un sistema di gestione delle chiavi crittografiche.	Valutare l'implementazione di una Public Key Infrastructure (PKI) aziendale.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Compliant Tutti i sistemi gestiti centralmente e collegati alla rete locale sono dotati di sistemi antivirus la cui configurazione e aggiornamento è gestita in maniera centralizzata tramite la console di Symantec Endpoint Protection.	Inserire sempre nei requisiti di gestione degli elettromedicali la dotazione e la gestione degli antivirus analogamnete a quanto avviene per gli altri dispositivi informatici connessi in rete
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Compliant I firewall locali sono attivi su sistemi di recente installazione nei quali tale protezione è attiva di default. Il software antivirus in uso è dotato di un modulo con funzionalità di IPS.	Verificare che antivirus e firewall locali siano attivi su tutti i sistemi.
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Partially compliant Gli antivirus sono gestiti centralmente e monitorati per tutti i dispositivi in dominiio MS. Agli utenti, non essendo amministratori delle macchine , non è possibile altercarne la configurazione.	Monitorare la gestione degli antivirus anche su altri dispositivi (elettromedicali) per i quali non è possibile la gestione centralizzata
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Compliant Di norma l'utilizzo di dispositivi esterni non necessari per le attività lavorative è limitato. ed è normato dal Regolamento Aziendale	Aggiornare il "Documento programmatico sulla sicurezza" includendo una procedura per la verifica del rispetto della policy di utilizzo dei dispositivi esterni.
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano		

				una cattiva reputazione.		
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Compliant L'esecuzione automatica dei contenuti dei dispositivi removibili è disabilitata per tutti i sistemi Microsoft Windows client/server più recenti.	Aggiornare il Regolamento Aziendale definendo comunque norme di comportamento e policy per tutti gli utenti per la disattivazione dell'esecuzione automatica dei contenuti dinamici (unica cautela possibile per quei casi in cui non è possibile impedirlo tecnicamente).
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Compliant In tutti i sistemi Microsoft Windows client/server e nelle applicazioni più recenti è richiesta all'utente l'autorizzazione all'esecuzione di contenuti dinamici.	Vedi azioni proposte ABSC 8.7.1
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Compliant I client di posta in gestione a Liguria Digitale di norma impediscono l'apertura automatica dei messaggi come impostazione di default.	
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Not Compliant Al momento l'anteprima automatica dei contenuti dei file non è disabilitata poiché non ritenuta particolarmente significativa ai fini della sicurezza	Valutare l'impatto sugli utenti e le implicazioni di sicurezza di una policy che disattivi l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Partially Compliant La scansione avviene ad oggi prima dell'utilizzo del-	

					la risorsa.	
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Compliant Requisito rispettato attraverso il servizio Antispam (Sophos) gestito da Liguria Digitale	
8	9	2	M	Filtrare il contenuto del traffico web.	Compliant Tutto il traffico web diASL 3 è filtrato da sistemi avanzati di content filtering (Fortinet)	
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Compliant Fare riferimento al gestore del servizio Antispam e Web Filtering (Sophos + Fortinet) gestito da Liguria Digitale	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Compliant I backup delle informazioni necessarie al ripristino dei sistemi server critici e dei sistemi virtuali sono schedulati settimanalmente (vedi allegato tecnico PTE Liguria Digitale e gestione sistemi LIS e PACS)	Inserire nel Regolamento Aziendale una policy che vieti di mantenere informazioni critiche sul disco locale non sottoposte ad attività di backup.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Partially compliant : Il ripristino di prova viene effettuato solo per immagini particolarmente critiche	Regolamentare il ripristino di prova per tutte le copie

10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Compliant : I supporti fisici di conservazione dei backup sono adeguatamente protetti in locali chiusi accessibili al solo personale autorizzato e archiviati in cassaforte. Non viene effettuata attività di cifratura.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Compliant : I backup full di lungo periodo sono mantenuti offline su nastri magnetici.	

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Azioni migliorative
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Partially compliant Non è prevista una attività sistematica di analisi e classificazione delle informazioni gestite dall'ente salvo nell'ambito di alcuni progetti. Un'analisi circa la riservatezza di diverse tipologie di dati è contenuta all'interno del DPS. Non vengono applicate protezioni crittografiche.	Analizzare la possibilità di applicazione di protezione crittografiche per le categorie più critiche; Raffinare l'analisi all'interno del DPS.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Compliant Tutto il traffico internet è filtrato da sistemi avanzati di content filtering in grado di bloccare i flussi	

					da e verso URL non autorizzate (Fortinet).	

ALLEGATO N: NFORMAZIONI SUL TRATTAMENTO DATI TRAMITE DOSSIER SANITARIO

ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione

Gentile Sig./Sig.ra di seguito la ASL 3 le fornisce le informazioni previste dalle norme in materia di protezione dei dati utili a comprendere quali siano le finalità e le modalità del trattamento dei suoi dati sanitari effettuati tramite il Dossier sanitario Elettronico (nel proseguo DSE)

- **Che cos'è un Dossier Sanitario Elettronico e a che cosa serve ?**

Al fine di migliorare i processi di prevenzione, diagnosi, cura e riabilitazione che La riguardano, l'Azienda Socio Sanitaria Ligure 3 ha la possibilità di costituire il Suo DSE, uno strumento che raccoglie in formato digitale i dati e i documenti clinici relativi alle prestazioni sanitarie che Le vengono erogate, e archiviati elettronicamente da ASL 3, allo scopo di documentarne la Sua storia clinico-sanitaria. IL DSE è disciplinato dalle Linee Guida del 16/07/2009 e 4/6/2015 emanate dall'Autorità Garante per la protezione dei dati personali e disponibili sul sito dell'Autorità (www.garanteprivacy.it).

- **Perché occorre il Suo consenso?**

La costituzione del DSE è facoltativa e libera: pertanto qualora ritenesse di voler attivare il suo Dossier, è necessario che rilasci uno specifico consenso.

In caso di minori il consenso deve essere rilasciato da chi ne esercita la legale rappresentanza e resterà valido fino al compimento del 18° anno di età.

Dal momento in cui verrà rilasciato il consenso alla costituzione il DSE sarà alimentato dalle informazioni di salute che La riguardano, generate presso l'Azienda Socio Sanitaria Ligure 3.

Per permettere ai professionisti sanitari che La prenderanno in cura di avere un più completo quadro clinico inerente il suo stato di salute, Lei potrà inoltre esprimere un ulteriore specifico consenso, affinché il Suo DSE venga alimentato anche dai dati clinico-sanitari già in possesso di questa ASL.

Qualora invece non intenda rilasciare il consenso per la costituzione del Dossier Sanitario Elettronico ed usufruire dei benefici legati al suo utilizzo, potrà comunque accedere alle prestazioni sanitarie e cure di cui ha bisogno.

- **Una volta rilasciato il consenso chi accede ai dati del DSE?**

Tale strumento, può essere consultato, integrato o modificato, e pertanto reso accessibile, da/a tutti i professionisti sanitari che di volta in volta La prenderanno in cura all'interno dell'Azienda Socio Sanitaria Ligure 3, limitatamente al periodo di tempo in cui si articola il percorso di cura stesso, per valutare nel modo più completo possibile il suo stato di salute, anche attraverso l'accesso alle informazioni relative alle prestazioni sanitarie effettuate in passato, c.d. eventi clinici pregressi, al fine di erogare tempestivamente le cure migliori. L'accesso ai dati clinici, reso possibile tramite il DSE, è consentito solo durante il percorso di cura e nel caso di urgenza/emergenza. E' altresì prevista l'eventualità che il Dossier Sanitario possa essere consultato anche da parte dei professionisti sanitari che operano in regime di libera professione intramuraria (*c.d. intramoenia*). La consultazione del Dossier Sanitario potrebbe, inoltre, essere consentita, anche senza il suo consenso, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività, in caso di emergenza e tutela della salute ed incolumità fisica, nel rispetto della vigente normativa.

Per finalità di difesa e di prevenzione, accertamento o repressione di reati, le "categorie particolari di dati" o i risultati degli esami clinici (facenti parte o meno nel DSE) potranno essere comunicati anche senza il suo consenso a: forze di polizia, autorità giudiziaria, organismi di informazione e di sicurezza.

I dati contenuti nel DSE possono essere ulteriormente trattati ai fini di archiviazione nel pubblico interesse di ricerca scientifica nei limiti di quanto previsto dall'art. 89 par. 1 del Regolamento UE 679/2016 e norme di armonizzazione.

- **Che cos'è il c.d. "Diritto di oscuramento"?**

Una volta manifestato il consenso, Lei può sempre decidere di non rendere disponibili sul Dossier Sanitario Elettronico i dati clinico – sanitari relativi a singoli eventi di cura (ad es. un referto di laboratorio o di diagnostica per immagini, una prestazione specialistica, ecc.), manifestando il *c.d. diritto all'oscuramento,* compilando un apposito modello di richiesta, disponibile sul sito internet della ASL 3 (www.asl3.liguria.it), anche successivamente all'avvenuta produzione della documentazione clinico-sanitaria. L'Azienda Socio Sanitaria Ligure 3 Le ricorda comunque che la decisone di procedere all'oscuramento di un evento o di una informazione sanitaria dovrebbe avvenire previa condivisione della scelta con il Suo medico di riferimento circa le possibili conseguenze della stessa.

Il Dossier Sanitario Elettronico non verrà comunque alimentato da alcuni documenti clinico – sanitari correlati a prestazioni per le quali la vigenti disposizioni normative prevedono la tutela dell'anonimato della persona, tra cui quelle a tutela delle vittime di violenza sessuale e pedofilia, delle persone sieropositive, di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che si sottopongono all'interruzione volontaria della gravidanza o che decidono di partorire in anonimato o con riferimento ai servizi offerti dai consultori familiari.

Lei può, con espresso consenso, autorizzare l'Azienda ad inserirli nel DSE, rendendoli visibili a tutti gli operatori che hanno accesso al DSE o de-oscurare gli stessi dati in precedenza oscurati.

- **Il consenso dato può essere revocato?**

Il consenso rilasciato per la costituzione del Dossier Sanitario Elettronico, può essere revocato in qualsiasi momento. Sia in caso di revoca che di diniego al rilascio del consenso, sia anche in caso di richiesta di oscuramento dell'evento clinico i Suoi dati rimarranno comunque accessibili ai soli professionisti sanitari che li hanno generati e prodotti durante il percorso di cura ed in conservazione per eventuali obblighi di legge.

- **Come vengono trattati i dati del DSE?**

Relativamente al DSE La informiamo, inoltre, che lo specifico trattamento dei dati personali, verrà effettuato in modalità anche automatizzata, esclusivamente da parte del personale espressamente autorizzato e da parte di soggetti aventi la qualifica ed individuazione di Amministratore di Sistema, e comunque sempre limitatamente ai dati pertinenti, necessari ed indispensabili per il periodo di tempo in cui si articola il percorso di cura. Ogni operazione di trattamento avviene con un livello di sicurezza elevato ed adeguato. L'accesso ai dati del DSE è organizzato in modo che il personale autorizzato acceda alle informazioni in ragione del profilo professionale e dell'area organizzativa a cui appartiene. I dati contenuti nel DSE vengono conservati tenendo conto di specifici termini di conservazione stabiliti per legge, o conformemente ai criteri di conservazione stabiliti nel prontuario di scarto della documentazione sanitaria e amministrativa di cui alla deliberazione di questa azienda n. 405 del 29/06/2016 e sue successive modifiche (pubblicata sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) o ancora sulla base del principio della necessità del trattamento in relazione alle finalità istituzionali perseguite dalla A.S.L.3 ed, in particolare per il DSE, a quelle per le quali è stato costituito (e quindi comunque non oltre la vita del paziente).

- **Quali sono i miei diritti in tema di DSE?**

In ogni momento potranno essere esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento UE 679/2016 e norme attuative, che riconoscono, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne la rettifica ovvero l'integrazione, la cancellazione ("diritto all'oblio"), salvo i casi previsti all'art. 17 comma 3 del Regolamento UE 679/2016 e norme di armonizzazione, la limitazione del trattamento, se ricorra-

no le ipotesi di cui all'art. 18 del Regolamento UE 679/2016 e norme di armonizzazione **("Diritto di limitazione di trattamento")**, l'opposizione al loro trattamento ai sensi dell'art. 21 del regolamento UE 679/2016 e norme di armonizzazione **("Diritto di opposizione").**

Qualora sia manifestato il consenso alla costituzione del DSE, è riconosciuto all'utente il diritto di poter richiedere all'Azienda quali siano stati gli accessi allo stesso.

Inoltre ha diritto di proporre reclamo all'autorità di controllo (Autorità Garante per la protezione dei dati personali- secondo le modalità previste sul sito internet dello stesso www.garanteprivacy.it) nei casi previsti dalle disposizioni in materia di protezione dei dati di cui al Regolamento UE 679/2016 e norme di armonizzazione.

- **A chi posso rivolgermi per esercitare i miei diritti?**

Il Titolare del trattamento è l'Azienda Socio Sanitaria Ligure 3 con sede in Via Bertani 4 – 16125 Genova (**indirizzo PEC**: protocollo@pec.asl3.liguria.it)

Il R.P.D. è contattabile ai seguenti indirizzi di posta: Via Bertani 4 – 16125 Genova ed alla **PEC aziendale**: protocollo@pec.asl3.liguria.it.

I dati di contatto dello stesso sono pubblicati anche sul sito aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy.

ALLEGATO O: MODELLO CONSENSO COSTITUZIONE DOSSIER SANITARIO

RACCOLTA CONSENSO AL TRATTAMENTO DEI DATI EFFETTUATI TRAMITE DOSSIER SANITARIO ELETTRONICO

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i(1)

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno,) (2)

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa al trattamento dei dati effettuati tramite Dossier Sanitario Elettronico ed **esprimo il consenso** alla costituzione del Dossier Sanitario Elettronico ed all'inserimento nel medesimo dei dati clinico – sanitari generati da oggi in poi

SI ☐ NO ☐

esprimo inoltre il consenso all'inserimento nel Dossier Sanitario Elettronico dei dati clinico – sanitari pregressi, già nella disponibilità dell'Azienda Socio Sanitaria Ligure 3 ——

SI ☐ NO ☐

Il sottoscritto è inoltre consapevole che in occasione di ogni singolo evento clinico potrà esercitare il c. d. diritto all'oscuramento, mediante la compilazione e sottoscrizione di apposito modello reperibile sul sito internet della ASL 3 (www.asl3.liguria.it)

Genova, ___/___/___ Firma dell'interessato

…….

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I. /Pat…….....n……

Rilasciata da ……..il……

Firma dell'operatore incaricato

[1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: "Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera."

Art. 76, D.P.R. n. 445/2000 e s.m.i.: "Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L'esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[2] Precisare la qualità ed allegare documentazione.

ALLEGATO P: MODELLO RICHIESTA OSCURAMENTO EVENTO CLINICO

RICHIESTA DI OSCURAMENTO DI EVENTO CLINICO SUL DOSSIER SANITARIO ELETTRONICO

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i[1]

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno, altro -precisare) [2]

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

CHIEDE

che l'evento clinico effettuato in data _____qui di sotto meglio individuato

_____

_____

NON SIA RESO VISIBILE SUL DOSSIER SANITARIO ELETTRONICO

Il/La sottoscritto/a è comunque consapevole che in ogni momento potrà revocare la richiesta di oscuramento dell'evento clinico, consentendo ai professionisti sanitari dell'Azienda Socio Sanitaria Ligure 3 di poterlo visionare per una migliore cura.

Genova, ___/___/___ Firma dell'interessato

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat……..n……

Rilasciata da ……..……il……

Firma dell'operatore incaricato

[1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: "Fermo restando quanto previsto dall'articolo 76, qualora dal controllo di cui all'art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera."

Art. 76, D.P.R. n. 445/2000 e s.m.i.: "Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L'esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte".

[2] Precisare la qualità ed allegare documentazione.

ALLEGATO Q: MODELLO REVOCA CONSENSO ALIMENTAZIONE DOSSIER SANITARIO

MODELLO REVOCA CONSENSO ALIMENTAZIONE DOSSIER SANITARIO

Il/La sottoscritto/a_____

nato/a_____prov. di_____

il_____C.F._____

consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i[(1)]

☐ in nome proprio

☐ esercitando la rappresentanza legale sull'assistito in qualità di (specificare se genitore, tutore, amministratore di sostegno, altro -precisare) [(2)]

_____

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____Via/ Piazza_____

Avendo prestato il consenso alla costituzione del Dossier Sanitario Elettronico in nome proprio, in qualità di Interessato al trattamento dei dati o di rappresentante legale per la persona sopra indicata e consapevole delle sanzioni penali, nel caso di dichiarazioni non veritiere e falsità negli atti, richiamate dall'art. 76 del D.P.R. 445 del 28/12/2000 e s.m.i.

CHIEDO

che venga revocato il consenso ad alimentare ulteriormente il Dossier sanitario elettronico con nuovi esami o con nuovi referti

Genova, ___/___/___ Firma dell'interessato

……

_____

A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat……n……

Rilasciata da ……..il……

Firma dell'operatore incaricato

[1] Art. 75, D.P.R. n. 445/2000 e s.m.i.: “Fermo restando quanto previsto dall’articolo 76, qualora dal controllo di cui all’art. 71 emerga la non veridicità del contenuto della dichiarazione, il dichiarante decade dai benefici eventualmente conseguiti al provvedimento emanato sulla base della dichiarazione non veritiera.”

Art. 76, D.P.R. n. 445/2000 e s.m.i.: “Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico e punito ai sensi del codice penale e delle leggi speciali in materia. L’esibizione di un atto contenente dati non rispondenti a verità equivale ad uso di atto falso.

Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell’art. 4, comma 2, sono considerate come fatte a pubblico ufficiale. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l’autorizzazione all’esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l’interdizione temporanea dai pubblici uffici o dalla professione e arte”.

[2] Precisare la qualità ed allegare documentazione comprovante la qualità.

ALLEGATO R: NOMINA AUTORIZZATO TRATTAMENTO DATI TRAMITE DOSSIER SANITARIO

Struttura ……..

Direttore……..

Genova, ……

Prot.n. /

Al Sig.

NOMINA AD AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI EFFETTUATI TRAMITE DOSSIER SANITARIO ELETTRONICO

ai sensi del Regolamento Europeo n. 679/2016 e norme di armonizzazione ~~e~~ delle Linee guida in materia di dossier sanitario (allegato A alla deliberazione del Garante del 04/06/2015 fatta propria dal Titolare quale policy aziendale in quanto compatibile con detta normativa)

ASL 3 quale Titolare, in persona del legale rappresentante pro tempore Dott. ……, Direttore Generale/in persona del Referente, Dott. ……..Direttore ……., delegato alla firma dal Titolare , legale rappresentante pro tempore, con il presente atto **designa la S.V. Dott.……, in qualità di Dirigente responsabile della Struttura……..(oppure DIPENDENTE -ruolo – eventuale P.O.), "autorizzato al trattamento dei dati personali"**, con riferimento ai trattamenti effettuati tramite Dossier Sanitario Elettronico, svolti per finalità di prevenzione, diagnosi, cura e riabilitazione degli interessati, nell'ambitodelle funzioni e competenze cui è preposto e/o assegnato, per la relativa durata di preposizione-assegnazione, compresi, i trattamenti effettuati nell'ambito di servizi di supporto, servizi di guardia, reperibilità, pronta disponibilità, consulenza e/o attività sostitutiva, di attività libero professionale, anche in convenzione, o di attività di sperimentazione autorizzate, nonché nell'ambito delle **specifiche funzioni e competenze** del sistema Privacy, come da D.P.S. aziendale.

In ottemperanza al Regolamento Europeo n. 2016/679 e norme di armonizzazione, che regolano il trattamento dei dati personali, laddove costituisce trattamento " *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione,*

l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione", ed in relazione alla presente designazione, la S.V. è autorizzata a trattare i dati personali (*qualsiasi informazione riguardante una persona fisica identificata o identificabile «interessato»; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale)* strettamente necessari allo svolgimento delle mansioni proprie assegnate, ed in particolare:

a. A trattarli in modo lecito, corretto e trasparente ed, in generale in conformità ai principi del Regolamento UE 679/2016 (con particolare riguardo agli artt.5-6) e norme di armonizzazione;
b. a raccoglierli e registrarli per finalità determinate, esplicite e legittime, e successivamente a trattarli in modo che non siano incompatibili con tali finalità;
c. a verificare la loro esattezza e, se necessario, aggiornarli;
d. a verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare del trattamento dei dati, anche per il tramite del Dirigente/Direttore responsabile della struttura-area di afferenza;
e. a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario alle finalità per i quali sono stati raccolti o successivamente trattati, rispettando le misure di sicurezza predisposte in Azienda. In ogni operazione di trattamento andrà garantita la massima riservatezza;
f. ad implementare e/o aggiornare costantemente e tempestivamente i contenuti del "registro dei trattamenti" ed i format afferenti le banche dati, la valutazione del rischio di violazione privacy e le misure di sicurezza, nonché il monitoraggio periodico di queste ultime, per la parte di competenza della struttura-area di afferenza, provvedendo alla relativa conservazione, pubblicazione e comunicazione al R.P.D. ed alla S.C. Affari Generali, il tutto nell'ambito delle funzioni privacy specifiche del ruolo ricoperto, con le modalità previste dal D.P.S. aziendale (che mantiene i relativi adempimenti di responsabilità del Dirigente/Direttore responsabile della struttura di diretta afferenza) e dalla vigente normativa. Pertanto dette attività rimangono sotto esclusiva responsabilità (compresa redazione, aggiornamento, conservazione e pubblicità) dei Dirigenti/Direttori responsabili delle singole strutture aziendali , per gli ambiti di rispettiva competenza) e del Titolare, tenendo il R.P.D. solo in copia informatizzata quanto da detti Dirigenti/Direttori trasmessogli;
g. a rispettare ed adottare le misure di sicurezza predisposte (nel rispetto in particolare dei principi di cui all'art.32 del Regolamento UE 679/2016 e norme di armonizzazione) dal Titolare del trattamento dei dati e riportate nel Registro dei trattamenti e relative sche-

de allegate, nonché nel Documento Programmatico sulla Sicurezza aziendale, entrambi pubblicati sulla intranet aziendale nella sezione “Normativa/Privacy”;

h. a fornire l’idonea informativa agli interessati ed acquisirne il relativo consenso, laddove necessario ai sensi della vigente normativa, nei casi di raccolta del consenso al trattamento dei dati;
i. a collaborare con il Responsabile per la Protezione dei Dati (R.P.D.) aziendale ed il Titolare per ogni eventuale istruttoria o chiarimento dovesse essere disposta in materia di protezione dei dati personali;
j. ad osservare le disposizioni e/o indicazioni del R.P.D. Aziendale e del Titolare (fornite anche per il tramite del Dirigente/Direttore responsabile della struttura-area di afferenza) in materia di protezione dei dati personali;
k. ad osservare le disposizioni e gli obblighi derivanti dal Regolamento Europeo 679/2016 e norme di armonizzazione, in particolare per quelli inerenti la comunicazione e la diffusione dei dati.
l. ad attenersi alla puntuale adozione delle istruzioni impartite dal Titolare direttamente o tramite delegato alla firma ed anche per il tramite dei Dirigenti/Direttori responsabili della struttura-area di afferenza circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza.

Tale nomina è in relazione alle operazioni di trattamento dei dati personali ai quali la S.V. ha accesso nell’espletamento delle funzioni proprie, e presuppone la conoscenza degli obblighi di legge e delle disposizioni aziendali in materia e l’impegno a trattare i dati personali nel pieno rispetto di tali obblighi e delle istruzioni impartite.

In particolare l’ambito di trattamento dei dati consentito tramite l’accesso al Dossier Sanitario Elettronico è relativo alle seguenti tipologie di operazioni:

visualizzazione dei dati per consultazione	SI ☐	NO ☐
inserimento dati	SI ☐	NO ☐
modifica, aggiornamento dei dati	SI ☐	NO ☐
stampa documenti	SI ☐	NO ☐
altro _____	SI ☐	NO ☐

(specificare operazione di trattamento)

L’accesso al Dossier Sanitario Elettronico ed il relativo trattamento dei dati è consentito soltanto durante il percorso di cura del paziente o in caso di urgenza/emergenza e per il tempo in cui si articola il processo di cura medesimo.
In relazione al presente atto di nomina, la S.V. è altresì autorizzata a trattare i dati personali ed i dati particolari strettamente necessari allo svolgimento delle mansioni assegnate rispettando le misure di sicurezza e le istruzioni impartite dal Titolare, anche per il tramite dei dirigenti/direttori responsabili della struttura di afferenza, circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza.

Nessun dato potrà essere comunicato a terzi senza la specifica autorizzazione del Titolare.

Per ogni altra misura si rinvia alle disposizioni di cui al succitato Regolamento Europeo e normativa attuativa~~,~~ alle linee guida dell'autorità garante per la protezione dei dati personali in materia di dossier sanitario (fatte proprie dal Titolare quali policy aziendali in quanto compatibili con detta normativa) ed al Documento Programmatico sulla Sicurezza aziendale (entrambi pubblicati sulla rete Intranet Aziendale nella sezione "Normativa/Privacy") nonché alle istruzioni operative fornite.

Il Titolare/Il delegato alla firma del Titolare
Dott……..

MODELLO S

CHECK LIST DEGLI ADEMPIMENTI DEL SISTEMA PRIVACY AZIENDALE

GESTIONE DEL RISCHIO PRIVACY

N.	Quesito/requisito	Si	No	Note
1	Indicare il nominativo e il numero telefonico del coordinatore Dipartimentale per la prevenzione privacy			
2	I dirigenti Responsabili delle singole strutture hanno effettuato l'aggiornamento della gestione del rischio privacy trasmettendo a voi, al R.D.P. ed alla S.C. Affari Generali i relativi dati con le modalità previste dal D.P.S.? Indicare eventuali inadempienze di singole Strutture (nella col. Note)			
3	I dirigenti Responsabili delle singole strutture hanno compilato e trasmesso i format sul monitoraggio del trattamento del rischio privacy con le modalità previste dal D.P.S.? Indicare la data di trasmissione di ogni singola Struttura (nella col. Note)			

4	I dirigenti Responsabili delle singole strutture hanno rivisto l'analisi del rischio, migliorando la qualità nell'analisi (individuando rischi e predisponendo misure concrete? (obiettivo previsto nel D.P.S. 2018-2019)			
5	La revisione del processo del rischio effettuato dalle singole strutture (individuazione dei rischi e delle misure di prevenzione) è stato condotto con l'ausilio dei gruppi di lavoro secondo le indicazioni del D.P.S.2018-2019?			
6	Ci sono stati gli incontri dei gruppi di lavoro dedicati al processo della gestione del rischio privacy previsti dal D.P.S. 2018-2019 (Indicare nella col. Note il numero degli incontri suddivisi per singole strutture e/o le motivazioni della mancata effettuazione)			
7	Le singole strutture hanno indicato misure di prevenzione del rischio privacy secondo i criteri previsti dal D.P.S. (misure concrete e verificabili)? (Indicare nella col. Note eventuali criticità riscontrate per singole strutture e/o le motivazioni della mancata effettuazione)			

8	Indicare il nominativo e il n. telefonico dei coordinatori della prevenzione delle strutture afferenti al Dipartimento			
9	Indicare il nominativo ed i riferimenti telefonici dei dipendenti che hanno fatto parte dei gruppi di lavoro per l'analisi della gestione del rischio di ogni struttura appartenente al Dipartimento			

FORMAZIONE

10	E’ stato svolto dai dipendenti di afferenza individuati il corso FAD in materia di privacy obbligatorio (Indicare nella col. Note eventualmente il numero dei dipendenti -suddivisi in base alle strutture di appartenenza- che devono ancora svolgere il corso FAD obbligatorio)			
11	E' stato chiesto ai dirigenti di afferenza di sollecitare i loro dipendenti alla frequentazione del corso? (Indicare nella col. Note eventuali criticità)			
12	Gli incontri periodicamente svolti con			

	i Dirigenti delle Struttura afferenti al Dipartimento sono stati riservati anche ad analizzare le problematiche sulla prevenzione privacy e le criticità riscontrate?			
13	Sono state predisposte procedure per ricevere con puntualità le informazioni da parte dei Dirigenti di afferenza ? (Indicare le eventuali procedure predisposte nella col. Note)			

ALTRE INIZIATIVE ATTUATE O DA ATTUARE IN RELAZIONE AL D.P.S.

14	Sono pervenute delle denunce-segnalazioni di fatti illeciti-violazioni privacy?			
15	In caso di risposta affermativa indicare il numero e la struttura e trattamento-i interessati			
16	In caso di risposta affermativa indicare se il segnalante è un dipendente ovvero un soggetto esterno			
17	In caso di risposta affermativa indicare per ogni segnalazione le azioni intraprese secondo la procedura indica-			

	ta nel D.P.S. evidenziando eventuali criticità rilevate			
18	Sono pervenute delle denunce o delle segnalazioni anonime di fatti illeciti?			
19	Se sì indicare il numero e per ogni segnalazione la struttura-trattamento coinvolti e le risultanze delle verifiche effettuate			

MONITORAGGIO DEI TRATTAMENTI - REGISTRO dei TRATTAMENTI

N.	Quesito/requisito	Si	No	Note
20	Le singole strutture afferenti al Dipartimento hanno trasmesso ed aggiornato con le modalità previste dal D.P.S. il format relativo al registro dei trattamenti di competenza ai fini della pubblicazione nella sotto sezione relativa dell'intranet aziendale (sezione "Normativa-Privacy")?			
21	E' stato verificato che i dati ivi contenuti di tutte le strutture siano aggiornati e completi e siano stati comunicati al R.D.P. ed alla S.C. Affari Generali?			

22	Contiene il registro il nome e i dati di contatto del titolare del trattamento?			
23	Sono indicati il nome e i dati di contratto, ove sussistenti: ...del contitolare del trattamento? ...del rappresentante del titolare del trattamento? ...del responsabile della protezione dei dati (R.D.P.)?			
24	Sono esplicitate le finalità dei trattamenti effettuati?			
25	Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?			
26	Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati: • dati che rivelano l'origine razziale o etnica (art. 9)? • dati che rivelano le opinioni politiche (art. 9)? • dati che rivelano le convinzioni religiose o filosofiche (art. 9)? • dati che rivelano l'appartenenza			

	sindacale (art. 9)? • dati genetici (artt. 4, par. 1, n. 13 e 9)? • dati biometrici (artt. 4, par . 1, n. 14 e 9)? • dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)? • dati relativi alla vita/orientamento sessuale (art. 9)? • dati relativi a condanne penali e reati (art. 10)?			
27	Per ciascun trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?			
28	Vi sono trattamenti in cui i dati sono comunicati a destinatari di Paesi terzi ovvero di organizzazioni internazionali?			
29	Contiene il registro l'indicazione dei trattamenti che includono i trasferimenti di dati personali verso un paese Terzo o un'organizzazione internazionale?			
30	In caso di risposta affermativa al quesito n. 29), il registro include l'identificazione del paese terzo o dell'organizzazione internazionale?			

31	In caso di risposta affermativa al quesito n. 28), per i trasferimenti di cui al secondo comma dell'articolo 49, il registro documenta le prescritte garanzie adeguate (per l'art. 49, comma 2, “Il trasferimento di cui al paragrafo 1, primo comma, lettera g) [che sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse], non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari?)			
32	E' stata individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?			
33	Detta base giuridica consente, per ciascun trattamento, di definire un tempo massimo di gestio-			

	ne/conservazione dei dati?			
34	Sono indicati i termini ultimi previsti per la cancellazione delle diverse categorie di dati?			
35	Sono descritte le misure di sicurezza tecniche e quelle organizzative di cui all'articolo 32, par. 1, tra cui, a titolo di esempio: • la pseudonimizzazione e la cifratura dei dati personali? • la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? • la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico? • una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?			
36	Dette misure garantiscono un livello di sicurezza adeguato al rischio?			

37	Ha il titolare aderito ad un codice di condotta (art. 40) o ad un sistema di certificazione (art. 42)?			
38	In caso risposta positiva alla domanda 37, in quale misura detto codice di condotta/sistema di certificazione include adempimenti in materia di misure di sicurezza dei trattamenti?			
39	In caso risposta positiva alla domanda 37, il registro contiene l'informazione circa l'adesione del titolare al codice di condotta/sistema di certificazione?			
40	In caso risposta positiva alla domanda 37, esplicita il registro le misure tecniche ed organizzative implementate e riconducibili al codice di condotta e/o al sistema di certificazione?			
41	Reca il registro la data del suo aggiornamento?			
42	E' specificato se si tratta di prima emissione o di successiva revisione?			
43	Il registro proviene dalla funzione che in base al sistema di procure e deleghe dell'organizzazione è deputata a farlo?			

44	Sono rispettate le modalità di conservazione e distribuzione interna del registro previste dal D.P.S.?			
45	E' individuata la funzione responsabile della conservazione e distribuzione interna del registro?			
46	E’ stato pianificato un check di verifica semestrale sullo stato di revisione del registro?			

OBIETTIVI PERFORMANCE

47	I direttori di Struttura hanno illustrato ai propri dipendenti gli obiettivi organizzativi relativi alla prevenzione privacy?			
48	I singoli Direttori di Struttura hanno stabilito obiettivi individuali, nell’ambito della scheda di valutazione 2019, da assegnare ai propri dipendenti (comparto/dirigenza), coinvolti nelle attività della prevenzione privacy, in ottemperanza a quanto previsto nel D.P.S.?			

ADEMPIMENTI PREVISTI PER I REFERENTI

49	I dati trasmessi, afferenti alle Strutture del Dipartimento, sono aperti, aggiornati, integri, completi, tempestivi di semplice consultazione?			
50	Se non lo sono, o lo sono solo in parte spiegare le difficoltà o i problemi riscontrati			
51	E' stata monitorata l'attività di prevenzione privacy svolta dai dirigenti di afferenza?			
52	In particolare, è stato verificato che i dirigenti del Dipartimento abbiano promosso ed accertato la conoscenza del D.P.S. e del "sistema privacy" aziendale (comprese le previsioni del codice di comportamento aziendale) da parte del proprio personale? (ad esempio attraverso opportuni incontri formativi?)			
53	Ai fini della valutazione individuale il Referente e i dirigenti afferenti hanno tenuto conto delle violazioni privacy?			

PROPOSTE E PROBLEMATICHE

54	

Scheda di accompagnamento al REGISTRO DEI TRATTAMENTI DEL _CODICE STRUTTURA

format TAB_CODICE STRUTTURA_01 REGISTRO DEI TRATTAMENTI

format TAB_CODICE STRUTTURA_02 REGISTRO DELLE BANCHE DATI

format TAB_CODICE STRUTTURA_03 SCHEDA ANALISI E VALUTAZIONE RISCHI POTENZIALI

format TAB_CODICE STRUTTURA_04 SCHEDA MONITORAGGIO RISCHI POTENZIALI

Scheda di accompagnamento al REGISTRO DEI TRATTAMENTI DEL _CODICE STRUTTURA

DENOMINAZIONE STRUTTURA:

CDC STRUTTURA*:

Direttore:

UBICAZIONE**:

DESCRIZIONE ATTIVITA' ISTITUZIONALI***:

DESCRIZIONE TRATTAMENTI****:

L'azienda socio sanitaria 3, per le attività amministrative, anche se strumentali alle attività di prevenzione, diagnosi, cura e riabilitazione, tratta le categorie particolari di dati personali , come individuati dal Regolamento Regionale 9 aprile 2013 n. 2 "Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione". In detto Regolamento (pubblicato sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) ed, in particolare, nelle relative schede dei trattamenti sono indicate le normative di riferimento che costituiscono la base normativa dei trattamenti effettuati da detta ASL e per essa dalla scrivente struttura-servizio, da intendersi parte integrante del registro dei trattamenti.

Detto Regolamento è, allo stato, mantenuto e fatto proprio dal Titolare ASL 3 quale elenco di trattamenti, tipologie di dati, finalità di trattamento (nel rispetto, tra l'altro, in particolare, delle previsioni degli artt.9 e 10 del Regolamento UE 679/2016 e norme di armonizzazione) , riferimenti normativi che legittimano i trattamenti e destinatari di comunicazioni afferenti i dati trattati dall'Azienda e dalla scrivente struttura-servizio , nelle aree di afferenza ed a miglior dettaglio del registro dei trattamenti agli atti in formato elettronico dell'Azienda, in quanto compatibili con la normativa europea e con le disposizioni attuative della stessa, a livello nazionale e/o regionale.

A titolo esemplificativo e non esaustivo di seguito si riportano le più importanti: l'art. 32 Cost., la legge 833/78 e s.m.i. Istituzione del SSN, il D.Lgs 502/92 e s.m.i.gs 229/99 Riordino della disciplina in materia sanitaria, di quella Regionale: la L.R. 41 del 7.12.2006 e s.m.i. Riordino del SSR, L.R. n.17 del 29.07.2016 e s.m.i. Istituzione dell'azienda ligure sanitaria della regione Liguria (A.Li.Sa.) ed indirizzi per il riordino delle disposizioni regionali in materia sanitaria e sociosanitaria, i vigenti piano sanitario nazionale e regionale.

I dati trattati non vengono trasferiti verso un paese terzo od un'organizzazione internazionale né extra Unione Europea dal Titolare. Qualora ciò avvenga per il tramite di responsabili esterni designati dal Titolare ci si assicurerà che tale trasferimento avvenga con un grado di protezione

adeguata e sia debitamente coperto in conformità alle Leggi sulla Protezione dei Dati applicabili, quali le Clausole Contrattuali Standard dell'UE o altre garanzie adeguate in conformità alle Leggi sulla Protezione dei Dati applicabili e che ne sia informato l'interessato.

I dati trattati potranno essere utilizzati sia in modo manuale che informatizzato dal personale debitamente autorizzato al trattamento dei dati, in qualità di autorizzato al trattamento, e saranno conservati in luogo idoneo ed appropriato, tutelandone la riservatezza, nel rispetto del segreto professionale e d'ufficio.

Potranno inoltre essere trattati da terzi, incaricati di svolgere specifiche operazioni necessarie per garantire i servizi dell'Azienda, nei limiti strettamente pertinenti alle finalità indicate nel registro.

Agli atti della struttura-servizio è conservata la documentazione relativa alla designazione di eventuali responsabili esterni dei trattamenti indicati nel registro, effettuata dal Titolare ai sensi della vigente normativa e del D.P.S. aziendale, nonché le designazioni ricevute per i medesimi trattamenti ed eventuali accordi di contitolarità di competenza.

I dati trattati potranno inoltre essere comunicati, quando ciò risulti necessario in relazione all'erogazione della prestazione o allo svolgimento dei compiti istituzionali attribuiti alla struttura-servizio alle seguenti categorie di soggetti: altre Amministrazioni pubbliche, quali, tra le altre, il Ministero della Salute, il Ministero dell'Economia e delle Finanze, la Regione Liguria, l'Azienda Ligure Sanitaria della Regione Liguria (A.Li.Sa.), altre Aziende Socio Sanitarie ed Ospedaliere, i Soggetti erogatori pubblici o equiparati, i Comuni, medici convenzionati, strutture convenzionate, farmacie convenzionate, consulenti, broker, compagnie di assicurazione, loss adjuster regionale, altri soggetti pubblici e privati nei casi consentiti dalla normativa vigente oppure su specifica richiesta o indicazione dell'interessato.

I dati trattati saranno conservati tenendo conto di specifici termini di conservazione stabiliti per legge, o conformemente ai criteri di conservazione stabiliti nel prontuario di scarto della documentazione sanitaria e amministrativa di cui alla deliberazione di ASL3 n. 405 del 29/06/2016 e sue successive modifiche (pubblicata sul sito internet aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy) o ancora sulla base del principio della necessità del trattamento in relazione alle finalità istituzionali perseguite dalla A.S.L.3.

Le misure tecnico-organizzative adottate dal Titolare ai sensi dell'art.32 del Regolamento UE 679/2016 e norme di armonizzazione sono descritte nelle tabelle allegate ed individuate a seguito dell'analisi ivi riportata e nel rispetto delle policy aziendali eventualmente presenti in materia (TAB_CODICE STRUTTURA_03 e TAB_CODICE STRUTTURA_04). Ogni misura è collegata al rischio che si vuole ridurre.

Il Titolare dei trattamenti è l'Azienda Socio Sanitaria Ligure 3 con sede in Via Bertani 4 – 16125 Genova (**indirizzo PEC:** protocollo@pec.asl3.liguria.it)

Il R.P.D. è contattabile ai seguenti **indirizzi di posta:** Via Bertani 4 – 16125 Genova ed alla **PEC**

aziendale protocollo@pec.asl3.liguria.it.

I dati di contatto dello stesso sono pubblicati anche sul sito aziendale www.asl3.liguria.it/siti tematici/Politiche della Privacy.

Per il rimanente si rinvia alla vigente normativa di settore ed all'ultimo D.P.S. aziendale e sue disposizioni attuative , che rappresentano il documento fondamentale per la definizione della strategia di prevenzione del rischio privacy in ASL 3.

ELENCO TRATTAMENTI: VEDI REGISTRO DEI TRATTAMENTI (**TAB_CDC_01) ***

STRUMENTI UTILIZZATI: VEDI REGISTRO DELLE BANCHE DATI (**TAB_CDC_02) ***

ANALISI DEI RISCHI POTENZIALI E RELATIVE MISURE DI SICUREZZA: VEDI SCHEDE ANALISI RISCHI POTENZIALI (**TAB_CDC_03) *** E SCHEDA VALUTAZIONE RISCHI POTENZIALI (**TAB_CDC_03) *** E SCHEDA MONITORAGGIO RISCHI POTENZIALI (**TAB_CDC_04) ***

LEGENDA:

*CDC: indica la codifica della struttura compilante
**Ubicazione: indica gli indirizzi delle sedi della struttura compilante nelle quali si svolgono i trattamenti descritti
*** Descrizione attività istituzionali: indica una sintetica descrizione delle attività istituzionali della struttura compilante
****Descrizione dei trattamenti: è l'elenco dei trattamenti che verranno inseriti dalla struttura compilante nel registro dei trattamenti (TAB_CDC_01)

REGISTRO DEI TRATTAMENTI TAB_CDC_01

DENOMINAZIONE E CODICE DIPARTIMENTO	
CENTRO DI COSTO DIPARTIMENTO	
DENOMINAZIONE E CODICE STRUTTURA	
CENTRO DI COSTO STRUTTURA	
DATA	

CODICE IDENTIFICATIVO DEL TRATTAMENTO		**TITOLARE DEL TRATTAMENTO E DATI DI CONTATTO**	**FINALITÀ**	**CATEGORIE DI INTERESSATI**	**TIPO-CATEGORIA DI DATO**	**DATO TRATTATO**	**SOGGETTI DESTINATARI DEI DATI**

REGISTRO BANCHE DATI TRATTAMENTI TAB_CDC_02

DENOMINAZIONE E CODICE DIPARTIMENTO	
CENTRO DI COSTO DIPARTIMENTO	
DENOMINAZIONE E CODICE STRUTTURA	
CENTRO DI COSTO STRUTTURA	
DATA:	

CODICE IDENTIFICATIVO DEL TRATTAMENTO	MODALITA' TRATTAMENTO	BANCA DATI	UBICAZIONE	DESCRIZIONE UBICAZIONE (*)*Se campo UBICAZIONE è SEDE ALTRO CENTRO DI COSTO (PRECISARE)*	PROCEDURA UTILIZZATA	INTERCONNESSIONE	PROCEDURE DI SALVATAGGIO DATI	LUOGO CUSTODIA COPIE DATI	INCARICATO SALVATAGGIO DATI	TEMPISTICA RIPRISTINO

SCHEDA ANALISI E VALUTAZIONE RISCHI POTENZIALI TAB_CDC_DS																			
DENOMINAZIONE E CODICE DIPARTIMENTO :																			
CENTRO DI COSTO DIPARTIMENTO																			
DENOMINAZIONE E CODICE STRUTTURA :																			
CENTRO DI COSTO DI STRUTTURA																			
DATA:																			
CODICE IDENTIFICATIVO DEL TRATTAMENTO	RISCHI POTENZIALI		SI	NO	IMPATTO SULLA SICUREZZA DEI DATI E GRAVITA' STIMATA			MISURE DI SICUREZZA ADOTTATE		MISURE DI SICUREZZA PROPOSTE				GRADO % DI INCIDENZA SULLE CAUSE DEL RISCHIO	STRUTTURA-SERVIZIO-UFFICIO RESPONSABILE				TEMPI E MODALITA' DI MONITORAGGIO INTERNO (PRECISARE SE SONO STATI EFFETTUATI CONTROLLI SULLA EFFETTIVA APPLICAZIONE DELLE MISURE; SE NON SI SONO VERIFICATI INDICARE LE MOTIVAZIONI DEL LORO MANCATO SVOLGIMENTO)
	AREA DI RISCHIO	TIPOLOGIA DI RISCHIO			ALTA	MEDIA	BASSA	INFORMATICHE	NON INFORMATICHE	INFORMATICHE	TEMPI ATTUAZIONE	NON INFORMATICHE	TEMPI ATTUAZIONE						
	COMPORTAMENTI DEGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE																	
	COMPORTAMENTI DEGLI OPERATORI	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA																	
	COMPORTAMENTI DEGLI OPERATORI	COMPORTAMENTI SLEALI O FRAUDOLENTI																	
	COMPORTAMENTI DEGLI OPERATORI	ERRORE MATERIALE																	
	COMPORTAMENTI DEGLI OPERATORI	ALTRO (SPECIFICARE)																	
	EVENTI RELATIVI AGLI STRUMENTI	AZIONE DI VIRUS INFORMATICI O PROGRAMMI IN GRADO DI VIOLARE IN SISTEMA																	
	EVENTI RELATIVI AGLI STRUMENTI	SPAMMING O TECNICHE DI SABOTAGGIO																	
	EVENTI RELATIVI AGLI STRUMENTI	MALFUNZIONAMENTO, OBSOLESCENZA OD INDISPONIBILITA' DEGLI STRUMENTI																	
	EVENTI RELATIVI AGLI STRUMENTI	ACCESSI ESTERNI NON AUTORIZZATI																	
	EVENTI RELATIVI AGLI STRUMENTI	INTERCETTAZIONI DI INFORMAZIONI IN RETE																	
	EVENTI RELATIVI AGLI STRUMENTI	ALTRO (SPECIFICARE)																	
	ALTRO EVENTO	ACCESSI NON AUTORIZZATI AD AREE AD ACCESSO RISTRETTO																	
	ALTRO EVENTO	ESPORTAZIONI - FURTO DI STRUMENTI CONTENENTI DATI																	
	ALTRO EVENTO	DISTRUZIONE CONSEGUENTE AD EVENTI NATURALI OD ARTIFICIALI (DOLOSI, ACCIDENTALI O DOVUTI AD INCURIA)																	
	ALTRO EVENTO	GUASTO AI SISTEMI DI SUPPORTO (IMPIANTI ELETTRICI, CLIMATIZZAZIONE, ETC)																	
	ALTRO EVENTO	ERRORI UMANI NELLA GESTIONE OPERATIVA DELLA SICUREZZA																	
	ALTRO EVENTO	ALTRO (SPECIFICARE)																	

LEGENDA STANDARD DI CODIFICA TRATTAMENTO :
CDC struttura_DS.....

SCHEDA MONITORAGGIO RISCHI POTENZIALI TAB_CDC_04

DENOMINAZIONE E CODICE DIPARTIMENTO E CENTRO DI COSTO:	
DENOMINAZIONE E CODICE STRUTTURA E CENTRO DI COSTO:	

CODICE IDENTIFICATIVO DEL TRATTAMENTO	RISCHI POTENZIALI		SI	NO	IMPATTO SULLA SICUREZZA DEI DATI E GRAVITA' STIMATA			MISURE DI SICUREZZA ADOTTATE		MISURE DI SICUREZZA PROPOSTE				GRADO % DI INCIDENZA SULLE CAUSE DEL RISCHIO	STRUTTURA-UFFICIO-UFFICIO RESPONSABILE	TEMPI E MODALITA' DI MONITORAGGIO INTERNO (PERIODICO ED ATTI EFFETTUATI CENTRALI SULLA EFFETTIVA APPLICAZIONE DELLE MISURE- SE NON SI SONO VERIFICATI INDICARE LE MOTIVAZIONI DEL LORO MANCATO SVOLGIMENTO)	PRECAUZIONI SULL'APPLICAZIONE DELLE MISURE (DIFFICOLTA' INCONTRATE NELL'APPLICAZIONE, MODALITA' DI COINVOLGIMENTO DEI DIRIPR DI LAVORO, TEMPI E MODALITA')
	AREA DI RISCHIO	TIPOLOGIA DI RISCHIO			ALTA	MEDIA	BASSA	INFORMATICHE	NON INFORMATICHE	INFORMATICHE	TEMPI ATTUAZIONE	NON INFORMATICHE	TEMPI ATTUAZIONE			
	COMPORTAMENTI DEGLI OPERATORI	SOTTRAZIONE DI CREDENZIALI DI AUTENTICAZIONE														
	COMPORTAMENTI DEGLI OPERATORI	CARENZA DI FORMAZIONE, DISATTENZIONE, INCURIA														
	COMPORTAMENTI DEGLI OPERATORI	COMPORTAMENTI SLEALI O FRAUDOLENTI														
	COMPORTAMENTI DEGLI OPERATORI	ERRORE MATERIALE														
	COMPORTAMENTI DEGLI OPERATORI	ALTRO (SPECIFICARE)														
	EVENTI RELATIVI AGLI STRUMENTI	AZIONE DI VIRUS INFORMATICI O PROGRAMMI IN GRADO DI VIOLARE IL SISTEMA														
	EVENTI RELATIVI AGLI STRUMENTI	SPAMMING O TECNICHE DI SABOTAGGIO														
	EVENTI RELATIVI AGLI STRUMENTI	MALFUNZIONAMENTO, OBSOLESCENZA DEI MALFUNZIONAMENTO, OBSOLESCENZA DEI STRUMENTI														
	EVENTI RELATIVI AGLI STRUMENTI	ACCESSI ESTERNI NON AUTORIZZATI														
	EVENTI RELATIVI AGLI STRUMENTI	INTERCETTAZIONE DI INFORMAZIONI IN RETE														
	EVENTI RELATIVI AGLI STRUMENTI	ALTRO (SPECIFICARE)														
		ACCESSI NON AUTORIZZATI AD AREE AD														
	ALTRI EVENTI	ACCESSI INDEBITI														
	ALTRI EVENTI	ASPORTAZIONE - FURTO DI STRUMENTI CONTENTI DATI														
	ALTRI EVENTI	DISTRUZIONI CONSEGUENTI AD EVENTI NATURALI DO ARTIFICIALI (DOLOSI, ACCIDENTALI O DOVUTI A INCURIA)														
	ALTRI EVENTI	GUASTO AI SISTEMI DI SUPPORTO (IMPIANTI ELETTRICI, CLIMATIZZAZIONE, ETC)														
	ALTRI EVENTI	ERRORE UMANO NELLA GESTIONE														
	ALTRI EVENTI	CONTATTO DELLA CUTE/CUTE														
	ALTRI EVENTI	ALTRO (SPECIFICARE)														

A SEGUITO DELLE RISULTANZE DEL MONITORAGGIO, SI ATTESTA CHE SONO STATE INDIVIDUATE ULTERIORI MISURE DI PREVENZIONE E/O CONFERMATE E/O MODIFICATE LE PRESISTENTI AL FINE DI PREVENIRE EPISODI DI VIOLAZIONE PRIVACY

DICHIARAZIONE

FIRMA DEL RESPONSABILE
DATA

LEGENDA STANDARD DI CODIFICA TRATTAMENTO:
CdC Direttore_G.I.....