REGIONE LIGURIA
AZIENDA SANITARIA LOCALE N. 3
"GENOVESE"

DELIBERAZIONE N. 827 DEL 27 DIC. 2016

OGGETTO: **Aggiornamento del Documento Programmatico sulla Sicurezza (DPS) dei dati trattati nell'ambito della A.S.L. 3 "Genovese".**

IL DIRETTORE GENERALE

Su conforme proposta del Direttore della Struttura Complessa Affari Generali;

Visti:

- l'art.4, comma 1, lett.d) del D.Lgs. 30 giugno 2003 n. 196 e s.m.i., che individua come "sensibili", tra gli altri, i dati personali idonei a rivelare lo stato di salute o la vita sessuale;
- il Titolo V "Trattamento di dati personali in ambito sanitario" del D.lgs.196/03 e s.m.i;
- gli artt. da 18 a 22 del D.Lgs 196/03 e s.m.i;
- le autorizzazioni generali dell'Autorità Garante per la protezione dei dati personali, ed in particolare la n.1/2014 "Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro" e la n. 2/2014 "Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale", disposte in data 11 dicembre 2014 ed aventi efficacia fino al 31 dicembre 2016;
- gli artt. 161-166 del D. Lgs. 196/03 e s.m.i. che sanzionano le relative violazioni amministrative;
- gli artt. 167-170 del D. Lgs 196/03 e s.m.i., che sanzionano penalmente la violazione delle prescrizioni in esso contenute;
- gli artt. 33-35 e l'allegato B del D.Lgs 196/03 e s.m.i., recanti norme sulle misure minime di sicurezza;
- la deliberazione n. 573 del 03 novembre 2015 "Aggiornamento del Documento Programmatico sulla Sicurezza (DPS) dei dati trattati nell'ambito della ASL 3 Genovese";
- la deliberazione n. 642 del 31 agosto 2016 "Designazione dei responsabili del trattamento dati ai sensi dell'art. 29 del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i."

Considerato che il Regolamento Europeo (General Data Protection Regulatione n. 2016/679) avrà totale applicazione nel nostro paese solo dal 25 maggio 2018, per cui nell'adozione del presente documento si tiene conto delle disposizioni di cui al D. Lgs. 196/2003 e s.m.i. e relative norme attuative;

Richiamato il punto 14 del citato documento programmatico, che prevede un aggiornamento annuale dello stesso entro il 31 dicembre di ciascun anno;

Considerata la necessità di aggiornare il Documento Programmatico sulla Sicurezza, quale strumento idoneo a rappresentare e definire il quadro di riferimento entro il quale ricondurre l'azione dell'Azienda in materia di protezione dei dati, ispirandosi al principio della massima riduzione del rischio previsto dall'art. 31 del D.Lgs 196/03 e s.m.i. e delineando l'insieme delle disposizioni e delle misure di sicurezza organizzative, fisiche e logiche da applicarsi per il trattamento dei dati da parte di questa Azienda Sanitaria;

Ritenuto, pertanto, di aggiornare il testo del Documento Programmatico sulla Sicurezza secondo lo schema elaborato dalle Strutture Complesse Sistemi Informativi Aziendali e Affari Generali, schema che, allegato al presente provvedimento, ne costituisce parte integrante e sostanziale (allegato A);

Su parere conforme del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

1. di approvare l'aggiornamento del Documento Programmatico sulla Sicurezza dei dati nell'ambito della A.S.L. n.3 "Genovese", secondo lo schema allegato A) al presente provvedimento, di cui costituisce parte integrante e sostanziale;

2. di provvedere alla sua pubblicazione sulla rete intranet aziendale;

3. di dare atto che il presente provvedimento non comporta oneri diretti;

4. di dare atto che la presente deliberazione è composta di n.2 pagine e da n.1 allegato (all. A di 61 pagine) e così in totale di n. 63 pagine.

IL DIRETTORE GENERALE
(Dott. Luigi Carlo BOTTARO)

IL DIRETTORE AMMINISTRATIVO
(Dott. Avv. Luigi BERTORELLO)

IL DIRETTORE SANITARIO
(Dott. Paolo CAVAGNARO)

IL DIRETTORE
S.C. AFFARI GENERALI
(Dott.ssa Avv. Giovanna DEPETRO)

Pubblicata all'Albo dalla data
- 7 DIC. 2016
del .....
Il Responsabile

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Premesso che nell'ambito della propria attività istituzionale l'Azienda Sanitaria Locale 3 "Genovese" effettua trattamento di dati personali, come di seguito elencati, con il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza organizzative, fisiche e logiche, previste per la tutela dei dati trattati, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati stessi, di accessi non autorizzati o di trattamenti non consentiti o non conformi alle finalità della raccolta.
Si forniscono, pertanto, idonee informazioni e prescrizioni riguardanti:

1. Elenco dei trattamenti dei dati personali:

1.1) Tipologie dei dati trattati

1.2) Aree, locali e strumenti con i quali si effettuano i trattamenti

1.3) Sistema di videosorveglianza

1.4) Mappa dei trattamenti effettuati

2. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

2.1) Amministratori di sistema

2.2) Incaricati del trattamento

2.3) Custode della parola chiave

2.4) Procedure applicative gestite dall'Area Sistema Informativo Aziendale

3. Analisi dei rischi a cui sono soggetti i dati

4. Misure adottate e da adottare atte a garantire l'integrità e la disponibilità dei dati

5. Criteri e modalità di ripristino dei dati a seguito di distruzione o danneggiamento

6. Formazione degli incaricati al trattamento dati

7. Misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno della struttura

8. **Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati inerenti lo stato di salute dagli altri dati personali dell'interessato**

9. **Consegna dei referti on line**

10. **Responsabili ed incaricati del trattamento nell'ambito delle sperimentazioni cliniche**

11. **Raccolta consenso al CUP regionale**

12. **Pubblicazioni provvedimenti sul sito Internet aziendale per finalità di trasparenza e per altre finalità**

12 a) Pubblicazioni per finalità di trasparenza

12 b) Pubblicazioni per altre finalità

13. **Trattamento dei dati tramite dossier sanitario elettronico**

14. **Aggiornamento periodico del Documento programmatico sulla Sicurezza**

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

1.1 Tipologie dei dati trattati

In seguito all'analisi compiuta, anche attraverso specifica richiesta alle singole strutture aziendali, sono stati individuati i seguenti trattamenti:

- Dati relativi al personale dipendente, sia di natura personale sia sensibili, conseguenti al rapporto di lavoro ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali o inerenti l'adesione ad organizzazioni sindacali
- Dati personali, sensibili e giudiziari relativi ai fornitori e terzi ricavati da albi ed elenchi pubblici o comunicati dagli stessi compresi dati sul patrimonio e sulla situazione economica o necessari ai fini fiscali o afferenti alla reperibilità e alla corrispondenza con gli stessi o all'espletamento delle procedure di gara
- Dati personali degli utenti dagli stessi forniti per l'espletamento dei fini e per l'esercizio delle attività istituzionali attinenti le funzioni del Servizio Sanitario Nazionale
- Dati sensibili degli utenti idonei a rivelare lo stato di salute degli stessi. Per l'identificazione delle diverse tipologie di dati inerenti lo stato di salute, dato il numero elevato degli stessi, si rinvia all'elenco del trattamento di dati notificati al Garante per la privacy in data 29 aprile 2004 e conservato presso la S.C. Affari Generali.

L'Azienda ha altresì preso atto con deliberazione n. 1082 del 17/10/2006 del Regolamento Regionale 16/05/2006 n.1 avente ad oggetto il Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20 e 21 del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i.

Tale Regolamento è stato successivamente abrogato e sostituito dal Regolamento Regionale 9 aprile 2014 n. 2 "Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi degli artt. 20 e 21 del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i."

Il Regolamento, pubblicato nella sezione della Intranet aziendale denominata normativa/privacy, è costituito da una serie di schede che identificano le rilevanti finalità di interesse pubblico, le tipologie di dati oggetto del trattamento e le operazioni su di essi eseguibili, e ognuna di esse è completata da una descrizione del trattamento effettuato.

Le Strutture aziendali interessate sono tenute a verificare che le procedure di trattamento in essere siano corrispondenti a quanto previsto nel Regolamento, attuando gli adeguamenti necessari ove si riscontrino eventuali difformità.

1.2 Aree, locali e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati avviene presso la sede dell'Azienda, e presso le singole strutture dislocate sul territorio di competenza della medesima, presso le sedi della società regionale d'informatica, Liguria Digitale S.c.p.a. e presso altri soggetti esterni debitamente designati responsabili esterni del trattamento dati.

Presso ogni struttura o ufficio aziendale in cui si effettua il trattamento di dati sono impartite apposite istruzioni affinché il medesimo avvenga in locali accessibili solo al personale incaricato del trattamento. I locali sono forniti di serratura a chiave.

Il trattamento dei dati avviene sia con strumenti elettronici sia con strumenti non elettronici (supporti cartacei tradizionali).

Per quanto concerne questi ultimi sono raccolti in schedari o fascicoli a loro volta custoditi in armadi o cassetti, anch'essi dotati di serratura.

Gli uffici che alla data del presente aggiornamento sono privi di appositi armadi o cassetti per la custodia dei supporti cartacei contenenti dati personali, devono comunque essere chiusi a chiave dal personale al termine dell'orario di ufficio.

Il trattamento effettuato con strumenti elettronici prevede l'utilizzo di personal computer non in rete (pc stand alone) ed in rete.

Gli strumenti informatici di cui dispone la Rete Aziendale sono costituiti, attualmente, da:

- N. 122 server
- N. 3345 personal computer in rete
- N. 33 personal computer non in rete

Con Rete Aziendale s'intende l'insieme delle apparecchiature informatiche (server, pc, hub, switch, router, stampanti) interconnesse su Lan e dotate di un indirizzo IP conforme al piano di indirizzamento interno dell'Azienda.

1.3 Sistema di videosorveglianza

Al fine di garantire il controllo degli accessi e la vigilanza a tutela della sicurezza dei pazienti, dei visitatori e dei lavoratori, la salvaguardia del patrimonio aziendale, degli assistiti, dei lavoratori, dei visitatori e la tutela della salute degli assistiti, viene effettuato un trattamento dei dati anche attraverso un sistema di videosorveglianza. Le immagini laddove registrate vengono conservate per 24 ore dalla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Decorso il termine il sistema provvede in modo automatico alla cancellazione delle immagini registrate.

Qualora una struttura aziendale intenda installare un sistema di videosorveglianza per una delle finalità sopra indicate deve inoltrare una richiesta alla S.C. Affari Generali. al Dipartimento delle Infrastrutture ed alla S.C. Servizio Amministrazione del Personale nella quale si devono indicare:

- le finalità perseguite, specificando le motivazioni che rendono proporzionale l'installazione di telecamere rispetto all'effettivo grado di rischio;

- il numero, la dislocazione e la tipologia delle video-camere;

- se le immagini devono essere solo rilevate od anche registrate

- le eventuali necessità di conservare le immagini per un periodo superiore alle 24 ore, specificandone le speciali esigenze,;

Inoltre ogni volta che viene attivato un sistema di videosorveglianza deve essere redatto dalla struttura aziendale presso cui viene installato tale sistema un apposito documento, con il quale vengono documentate le ragioni delle scelte che hanno determinato l'attivazione della videosorveglianza, ed una copia di tale documento deve essere trasmessa alla S.C. Affari Generali, che lo conserverà ai fini di eventuali esibizioni in occasione di visite ispettive disposte dall'Autorità Garante per la protezione dei dati personali, oppure ai fini di dare riscontro all'esercizio dei diritti dell'interessato o ancora in caso di contenzioso.
L'elenco delle strutture presso cui sono installati sistemi di videosorveglianza è detenuto dal Dipartimento delle Infrastrutture.
Per ogni altra prescrizione in materia si rimanda al regolamento aziendale sulla videosorveglianza approvato con deliberazione n. 640 del 11 novembre 2013.

1.4 Mappa dei trattamenti effettuati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delinea il seguente schema:

Tipologia trattamento	Cartaceo	PC non in rete	PC in rete pubblica	PC in rete privata
Dati comuni personale dipendente	X	X		X
Dati sensibili personale dipendente	X			X
Dati comuni fornitori e terzi	X			X
Dati comuni degli utenti	X	X		X
Dati utenti idonei a rivelare lo stato di salute degli utenti	X	X		X

2. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

L'Azienda Sanitaria Locale 3 "Genovese" titolare del trattamento dei dati provvede, ai sensi dell'art. 29 del Decreto Legislativo 196/2003 e s.m.i., a designare per esigenze organizzative i Responsabili del trattamento dei dati, individuandoli nei Direttori di Struttura Complessa, nei Direttori di Struttura Semplice Dipartimentale, nei Direttori di Distretto, nel Direttore del Presidio Unico Ospedaliero, nei Direttori degli Ospedali, nel Direttore Sanitario e nel Direttore Amministrativo, nell'ambito delle loro rispettive competenze e funzioni, così come indicato da ultimo con la Deliberazione n. 642 del 31/08/2016 "Designazioni dei Responsabili del trattamento dati ai sensi dell'art. 29 del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i."

Le designazioni dei Responsabili del Trattamento dati vengono effettuate dal Titolare Azienda Sanitaria Locale 3 "Genovese", nella persona del legale rappresentante pro-tempore, ed hanno efficacia fino a termine degli incarichi di direzione conferiti e/o alla modifica degli stessi.

La Struttura Complessa Organizzazione e Sviluppo Risorse Umane, contestualmente alla sottoscrizione del contratto di conferimento di incarico di direzione delle suddette strutture, provvede a far sottoscrivere per presa visione anche la nomina a responsabile del trattamento dati, utilizzando il modello allegato al presente documento (**allegato A**), conservando agli atti della struttura copia della designazione e dandone comunicazione alla S.C. Affari Generali.

Analogamente, la Struttura Complessa Organizzazione e Sviluppo Risorse Umane provvederà a far sottoscrivere per presa visione la nomina a responsabile del trattamento dati per gli incarichi di direzione delle strutture aziendali sopra citate, che possano derivare da procedure di affidamento temporanee e/o ad interim, per i quali non interviene la sottoscrizione di specifico contratto di

riferimento, conservando anche in tale ipotesi copia della designazione, dandone comunicazione alla S.C. Affari Generali.

Ad ogni Responsabile all'atto della nomina, sono state fornite idonee e specifiche istruzioni scritte.

In particolare è compito del Responsabile del trattamento:

- Verificare che i dati personali oggetto del trattamento siano:

a) trattati in modo lecito e secondo correttezza
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi
c) esatti e se necessario aggiornati
d) pertinenti, completi e non eccedenti rispetto alle finalità per i quali sono raccolti o successivamente trattati
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati

- Evadere le eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati presentate su istanza dall'interessato ai sensi degli artt. 7 e 10 D. Lgs. 196/03 e s.m.i.
- Vigilare sul rispetto e sull'adozione delle misure di sicurezza predisposte dal Titolare del trattamento e riportate nel presente Documento Programmatico sulla Sicurezza e, comunque, assicurare la predisposizione e l'aggiornamento delle stesse in modo conforme alle misure minime previste nel D. Lgs. 196/03 e s.m.i.
- Procedere alla nomina dei soggetti incaricati del trattamento dei dati, impartendo loro specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, utilizzando i modelli allegati al presente documento **(allegati B, C e R)**, dandone comunicazione alla S.C. Affari Generali. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun incaricato, nonché vigilare che l'accesso ai dati da trattare da parte degli incaricati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni il nominato responsabile avrà anche il compito di verificare, almeno annualmente, la sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto di procedere alla revoca delle stesse. La nomina dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti assegnati alla struttura, che effettuano trattamento dei dati.

- Verificare che la fase di raccolta del consenso al trattamento dei dati sia preceduta da idonea informativa.
- Osservare le disposizioni e gli obblighi derivanti dal D. Lgs. 196/03 e s.m.i. in particolare per quelli inerenti la comunicazione e la diffusione dei dati.
- Osservare le istruzioni impartite dal Titolare del trattamento, anche quali risultanti dal Documento Programmatico aziendale sulla Sicurezza dei dati trattati.

L'eventuale redazione ed utilizzo di modulistica specifica in materia di trattamento dei dati personali (informative, modelli di acquisizione del consenso, liberatorie per l'utilizzo di immagini, ecc.), diversa rispetto alla modulistica allegata al presente documento, dovrà essere previamente concordato con la S.C. Affari Generali.

2.1 Amministratori di sistema

In ottemperanza a quanto prescritto dal provvedimento dell'Autorità Garante per la protezione dei dati del 27 novembre 2008, pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008 "misure e accorgimenti prescritti ai titolari di trattamento effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" e s.m.i, l'A.S.L.3 "Genovese" ha provveduto al conferimento di incarico di amministratore di sistema, da identificarsi nella figura professionale dedicata alla gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, ai seguenti dipendenti:

Sig. Vitale Cosolito Alessandro - Assistente Tecnico Informatico - funzioni attribuite per gli applicativi del settore diagnostica per immagini (RIS/PACS), laboratori analisi (LIS) su tutta la ASL 3, neurologia, CPR (Clinical patient record), medicina nucleare, ricetta elettronica, Dossier sanitario elettronico - Amministratore di rete –

Sig. Demaria Fabio - Assistente Tecnico Programmatore – funzioni attribuite per gli applicativi della specialistica convenzionata, recupero crediti, gestione dei trasporti sanitari, ricetta elettronica, fisica sanitaria, visite fiscali, portali informativi web , Dossier sanitario elettronico -,Amministratore di rete;

Sig. Laforgia Raffaele - Assistente Tecnico Programmatore – funzioni attribuite per gli applicativi del settore protocollo, gestione documentale e firma digitale, ricetta elettronica, Dossier sanitario elettronico - limitatamente all'Ospedale Villa Scassi le funzioni sono attribuite per il servizio di reperibilità per piattaforma Unit/Linux – Windows/VmWare – Amministratore di rete – Database Oracle – DBA Oracle – sistemista di RDBMS (piattaforme non Oracle), sistema di accesso regionale IAM;

Sig. Colangelo Pierluigi - Collaboratore Tecnico DS - funzioni attribuite per anagrafica ospedaliera – accettazione e dimissione ospedaliera – Pronto Soccorso – gestione dei reparti e ambulatori ospedalieri, Anatomia Patologica integrazione con i dipartimentali, sistemi di prenotazione, flussi informativi, amministratore di sistema, cedap, tutte relativamente all'Ospedale Villa Scassi, Dossier sanitario elettronico;

Sig.ra Cassano Maria - Collaboratore Tecnico – funzioni attribuite per gli applicativi di gestione del Personale relativamente alle competenze giuridico – matricolare – economico e per rilevazione presenze e assenze, Dossier sanitario elettronico , Amministratore di rete;

Sig. Filippone Francesco - Assistente Tecnico Programmatore – funzioni attribuite per anagrafica ospedaliera —Accettazione e dimissione ospedaliera – Pronto Soccorso - CUP — Dialisi – Cartella clinica, cedap –, tutte relativamente all'Ospedale Villa Scassi, portali informativi web. Farmaceutica – Fisica Sanitaria e Flussi Informativi , Dossier sanitario elettronico , Amministratore di rete;

Dott. Landa Paolo - Assistente Tecnico Programmatore – funzioni attribuite per anagrafica ospedaliera — accettazione e dimissione ospedaliera - Pronto Soccorso — Dialisi – Cartella Clinica – Anatomia Patologica –- Laboratori analisi, tutte relativamente all'Ospedale Villa Scassi; sono attribuite funzioni di amministratore di sistema anche per il sistema di reperibilità dell'Ospedale Villa Scassi per piattaforma UNIX/Linus – Windows/VmWare – Amministratore di rete – database Oracle - sistema RDBMS (piattaforme non Oracle); Rischio Clinico; Centro Trasfusionale, Dossier sanitario elettronico;

Sig. Medulla Maurizio - Assistente Tecnico Programmatore – funzioni attribuite per sistema di gestione ordini, contabilità e per la farmaceutica, Dossier sanitario elettronico, Amministratore di rete, gestione del sistema di Formazione a Distanza (FAD);

Sig. Landi Diego - Assistente Tecnico Programmatore – funzioni attribuite per infrastrutture/applicativi concernenti attività presso l'Ospedale Villa Scassi per piattaforma Windows/VmWare e amministratore di rete, limitatamente all'Ospedale Villa Scassi le funzioni sono attribuite per il servizio di reperibilità, Ricetta Elettronica, Dossier sanitario elettronico;

Sig. Rebora Massimo - Assistente Tecnico Programmatore – funzioni attribuite per infrastrutture/applicativi concernenti attività presso l'Ospedale Villa Scassi per piattaforma Windows/VmWare, anagrafica ospedaliera, accettazione e dimissione ospedaliera, Pronto Soccorso, gestione dei reparti e ambulatori ospedalieri, Anatomia Patologica integrazione con i dipartimentali, sistemi di prenotazione – relativamente all'Ospedale Villa Scassi, Sistema di accesso regionale IAM Ricetta Elettronica, Pronto Soccorso;

Dott.ssa Ravera Laura - Collaboratore Tecnico – funzioni attribuite per infrastrutture/applicativi per piattaforma Linux – Windows/VmWare – sistemi di RDBMS - amministratore sistemi applicativi, anagrafica ospedaliera, accettazione e dimissione ospedaliera, Pronto Soccorso –relativamente all'Ospedale Villa Scassi; portali informativi web, sistema di accesso regionale IAM, Dossier sanitario elettronico;

Sig. Galeno Luigi Marco - Collaboratore Tecnico – funzioni attribuite per infrastrutture/applicativi per piattaforma Linux – Windows/VmWare – sistemi di RDBMS – amministratore di applicativi – amministratore di rete, Database Oracle per il servizio di reperibilità presso l'Ospedale Villa Scassi, Ricetta Elettronica, centri trasfusionali, Laboratori di Analisi, Dossier sanitario elettronico;

Sig. Lorenzo Guzzinati – Assistente Tecnico Informatico – funzioni attribuite per Libera Professione, Intramoenia, Portali di accesso, applicativi di gestione del Personale relativamente alle competenze giuridico – matricolare – economico e per rilevazione presenze e assenze, ricetta elettronica, specialistica convenzionata, gestione dei trasporti sanitari. portali informativi web, Dossier sanitario elettronico , Amministratore di rete;

Sig. Marco Fantini – Assistente Tecnico Programmatore – funzioni attribuite per Medicina Legale (patenti, invalidi civili), convenzionati esterni, Dossier sanitario elettronico, anagrafica ospedaliera, accettazione e dimissione ospedaliera, Pronto Soccorso - relativamente all'Ospedale Villa Scassi;

Ing. Manuela Guerisoli – Collaboratore Tecnico Professionale Ingegnere Biomedico - funzioni attribuite per infrastrutture/applicativi concernenti attività presso l'Ospedale Villa Scassi per piattaforma Windows/VmWare, anagrafica ospedaliera, accettazione e dimissione ospedaliera, Pronto Soccorso – relativamente all'Ospedale Villa Scassi, Sistema di accesso regionale IAM Ricetta Elettronico, dati relativi al consenso al trattamento dei dati effettuati tramite Dossier Sanitario Elettronico, diagnostica per immagini (RIS/PACS), laboratori analisi (LIS) su tutta la ASL3, cardiologia, anatomia patologica, neurologia, , centri trasfusionali, CPR (clinical patient record), medicina nucleare, salute mentale, teleconsulto specialistico intra-interaziendale, screening oncologici, endoscopia, ricetta elettronica, Amministratore di rete;

Ing. Alessandra Spadafora – Coadiutore amministrativo esperto - funzioni attribuite per infrastrutture/applicativi concernenti attività presso l'Ospedale Villa Scassi per piattaforma Windows/VmWare, anagrafica ospedaliera, accettazione e dimissione ospedaliera, Pronto Soccorso – relativamente all'Ospedale Villa Scassi, Sistema di accesso regionale IAM Ricetta Elettronico, dati relativi al consenso al trattamento dei dati effettuati tramite Dossier Sanitario Elettronico, diagnostica per immagini (RIS/PACS), laboratori analisi (LIS) su tutta la ASL3, cardiologia, anatomia patologica, neurologia, , centri trasfusionali, CPR (clinical patient record), medicina

nucleare, salute mentale, teleconsulto specialistico intra-interaziendale, screening oncologici, endoscopia, ricetta elettronica, Amministratore di rete;

Dott.ssa Pareto Luisa - Dirigente Analista – funzioni attribuite per piattaforma Linux – Unix – Windows/VmWare – sistemi di RDBMS – amministratore di applicativi – amministratore di rete;

Sig.ra Patrizia Poli – funzioni di amministratore di sistema attribuite relativamente al consenso al trattamento dei dati effettuati tramite Dossier Sanitario;

Sig.ra Alba Maggiora - funzioni di amministratore di sistema attribuite relativamente al consenso al trattamento dei dati effettuati tramite Dossier Sanitario;

La Società Liguria Digitale S.c.p.a., con la quale A.S.L. 3 "Genovese" ha un contratto per la gestione in outsourcing dei sistemi e strumenti informatici, ha provveduto ad identificare ed incaricare gli amministratori di sistema, predisponendo la piattaforma per la raccolta e conservazione dei log di accesso.

L'elenco dei soggetti designati all'interno di Liguria Digitale S.c.p.a. a svolgere la funzione di amministratore di sistema per conto di ASL3 è conservato presso la S.C. Affari Generali.

Entro il 31 dicembre di ogni anno la S.C. Sistemi Informativi Aziendali verifica l'operato degli amministratori di sistema, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati personali, provvedendo altresì a confermare annualmente la designazione degli amministratori di sistema, ove non si siano modificati i relativi profili di autorizzazione e/o a nominare i nuovi amministratori di sistema ove necessario, trasmettendo contestualmente alla S.C. Affari Generali copia delle note di conferma o copia delle nuove designazioni.

La S.C. Sistemi Informativi Aziendali provvede, inoltre, a richiedere, sempre entro il 31 dicembre di ogni anno, alla Società Liguria Digitale S.c.p.a. – l'elenco aggiornato degli amministratori di sistema che svolgono dette funzioni per conto di ASL 3, nell'ambito del servizio in outsourcing per la gestione dei sistemi e strumenti informatici, comprensivo degli estremi identificativi di detti amministratori, trasmettendone copia alla S.C. Affari Generali.

2.2 Incaricati del trattamento

Il trattamento dei dati viene effettuato solo dal personale che ha ricevuto un formale incarico mediante designazione per iscritto, attraverso il modello di nomina allegato al presente documento e relative istruzioni operative (**allegati B, C e R**), con la quale si individua l'ambito del trattamento consentito (c.d. mansionario). Si considera tale anche la documentata preposizione del dipendente

ad una struttura per la quale è individuato per iscritto l'ambito del trattamento consentito ai dipendenti della medesima struttura.

Oltre alle istruzioni generali sulle modalità di trattamento dei dati personali, agli incaricati sono fornite esplicite istruzioni relativamente a:

- Procedure da seguire per la classificazione dei dati personali al fine di distinguere quelli di natura sensibile e giudiziaria, osservando le maggiori cautele che questa tipologia di dati richiedono;
- Modalità di reperimento dei documenti contenenti dati personali e modalità da osservare per la custodia ed archiviazione degli stessi;
- Modalità per elaborare e custodire le password necessarie per accedere agli strumenti elettronici ed ai dati in essi contenuti;
- Prescrizioni di non lasciare incustoditi ed accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro, né i documenti contenenti dati personali qualora si stia operando un trattamento con supporti di tipo cartaceo;
- Prescrizioni inerenti l'obbligo di assoluta riservatezza e di divieto di divulgazione delle password di accesso al sistema;
- Procedure per il salvataggio dei dati;
- Procedura in caso di assenza prolungata od impedimento dell'incaricato che renda indispensabile ed indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema;
- Modalità di utilizzo, custodia ed archiviazione dei supporti rimovibili contenenti dati personali;
- Aggiornamento continuo, utilizzando il materiale e gli strumenti forniti dal Titolare del trattamento, sulle misure di sicurezza;
- Modalità di utilizzo di posta elettronica ed internet (Regolamento di cui alla Deliberazione n. 228 del 22 febbraio 2010)
- Prescrizioni sulle modalità di informativa ai terzi (pazienti, utenti, etc.) in merito al trattamento dei loro dati ed all'acquisizione del relativo consenso, utilizzando i modelli generali allegati al presente documento (**allegati E, F, G, I, L, M, O, P e Q**) o specifici modelli definiti di concerto con la S.C. Affari Generali.

La Struttura Complessa Organizzazione e Sviluppo Risorse Umane comunica periodicamente e, comunque, almeno ogni 12 mesi alla Struttura Complessa Affari Generali l'elenco dei dipendenti neoassunti, al fine di consentire un monitoraggio costante dell'avvenuta nomina degli incaricati al trattamento dei dati.

Tale elenco deve contenere il nome e cognome del dipendente, la data di assunzione e la sede aggiornata di assegnazione.

La Struttura Complessa Servizio Amministrazione del Personale, contestualmente alla sottoscrizione del contratto di lavoro individuale con il dipendente, rende altresì allo stesso l'informativa di cui al modello allegato al presente documento **(allegato H)** , pubblicato anche sul sito intranet aziendale, nella sezione "*normativa/privacy*".

2.3) Custode delle parole chiave

Il punto 10 dell'Allegato B. "Disciplinare Tecnico" del Codice Privacy prevede l'individuazione di un soggetto preposto alla custodia delle parole chiave (password), il quale deve garantirne la segretezza e che, in caso di prolungata assenza o impedimento dell'incaricato, possa assicurare ai soggetti debitamente autorizzati la disponibilità dei dati o degli strumenti elettronici, per gli interventi indispensabili ed indifferibili che si dovessero rendere necessari per ragioni di operatività o di sicurezza del sistema.

Al fine di ottemperare a tale disposizione, l'Azienda aveva comunicato ai Responsabili del trattamento, con nota dell'U.O. S.I.A. del 15/10/2004, avente ad oggetto "Adempimenti D. Lgs. 196/03 e s.m.i. (codice privacy)", una procedura che prevedeva la consegna in busta chiusa della password da parte degli incaricati al trattamento al Responsabile, che di fatto assumeva la qualifica di custode della parola chiave.

Poiché la procedura utilizzata ha evidenziato alcune difficoltà operative, stante l'elevato numero di dipendenti incaricato del trattamento e la necessità di modificarle ogni tre mesi, con conseguente difficoltà nella gestione delle password, si è individuata una nuova procedura che persegua le finalità richieste dal D. Lgs. 196/03 e s.m.i., prescindendo dal dover richiedere ad ogni utente-incaricato di consegnare le proprie credenziali di autentificazione al responsabile-custode delle parole chiave.

Secondo questa procedura, la Struttura Complessa Sistemi Informativi Aziendali, attraverso i propri amministratori di sistema ed a seguito di richiesta scritta del Responsabile del trattamento, come sopra individuato, nel caso di documentata necessità di accedere ai dati gestiti da un incaricato, è in grado di rimuovere la password di quell'utente, generandone una nuova che viene consegnata al Responsabile del trattamento 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 Responsabile del trattamento che ha

richiesto la procedura di accesso straordinario è tenuto ad avvertire tempestivamente l'incaricato che è stata attivata la procedura di generazione di nuove credenziali d'accesso.
In ogni caso l'incaricato non potrà più utilizzare le precedenti credenziali e per accedere al sistema dovrà richiederne di nuove.

2.4 Procedure applicative gestite dall'Area Sistema Informativo Aziendale

Nell'ambito del Sistema Informativo di ASL 3 sono gestite applicazioni che comprendono dati personali e sensibili relativi alle seguenti competenze:

- Personale aziendale e rilevazione presenze
- Protocollo e gestione documentale
- Contabilità e gestione dei magazzini economali e farmaceutici
- Distribuzione e somministrazione dei farmaci
- Compilazione Piani Terapeutici
- Prescrizioni farmaceutiche territoriali
- Conferma delle prestazioni sanitarie specialistiche erogate
- Attività Consultoriale
- Protesi
- Disabili
- Registro Cause di Morte
- Dipartimento di Prevenzione e veterinaria
- Anagrafe Sanitaria e dei Contatti
- Medicina Legale e Invalidi Civili
- Ricettari
- Ricetta elettronica e dematerializzata
- Gestione Reclami
- Pazienti Celiaci
- Assistenza Domiciliare Integrata
- Attività Istituti Accreditati per la specialistica ambulatoriale
- Gestione RSA
- Gestione Sistema Informativo Ospedaliero
- Pronto Soccorso
- Censimento Dati Assistenza Parto – CEDAP
- Sistema Prevenzione e Sicurezza Ambienti di Lavoro
- Lesioni da Decubito
- Sportello distrettuale polifunzionale

- Trasporti sanitari
- Assistenza ospedaliera privata
- Vaccinazioni
- Sistema Trasfusionale
- Anatomia Patologica
- Gestione Pagamenti Esterni
- Calcolo Trattamento Pensionistico
- Registrazione Notizie di Reato
- Sistema di Gestione Informatizzata del Laboratorio di Analisi
- Sistema di Gestione Informatizzata Diagnostica per Immagini
- Cartella clinica neurologia
- Diabetologia
- Cardiologia
- Nefrologia e Dialisi
- Screening oncologici
- Rischio clinico
- Salute Mentale
- Sert
- Anagrafica utenti dell'Ospedale Villa Scassi
- Medicina Nucleare
- Sale Operatorie
- Convenzionati esterni
- Attività Ambulatoriali Intramoenia
- Gestione Richieste Interne
- Cartella clinica ambulatoriale e ricovero Ospedale Villa Scassi
- Riabilitazione
- Dietologia
- Lesioni Difficili
- Cruscotto Sanitario Epidemiologico
- Cruscotto Amministrativo
- Dossier Sanitario Aziendale
- Refertazione Ambulatoriale
- Portale per acquisizione consenso privacy e dossier aziendale
- Portale per la gestione delle richieste Dipartimento Infrastrutture

- Portale Informativo attività intramoenia
- Refertazione endoscopica
- Teleconsulto
- Refertazione remota ECG

3. ANALISI DEI RISCHI A CUI SONO SOGGETTI I DATI

In questa sezione del documento sono stati individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati, rilevando una gradazione del fattore di rischio (basso, medio o alto) ed i riferimenti circa le contromisure adottate.
Tale analisi viene riportata nella tabella seguente:

EVENTO	GRAVITA' STIMATA	CONTROMISURE
Furto credenziali autenticazione	BASSA	Disposizioni sulla custodia e segretezza delle credenziali
Disattenzione o incuria degli incaricati	BASSA	Istruzioni agli incaricati circa l'attenzione da porre durante un trattamento
Comportamenti sleali o fraudolenti	BASSA	Informazione agli incaricati del trattamento sulle responsabilità penali, civili e disciplinari
Azioni di virus informatici	MEDIA	Il sistemi server sono protetti da antivirus aggiornati quotidianamente. I personal computer connessi alla Rete Aziendale e facenti parte del dominio ASL 3 sono protetti da antivirus centralizzato aggiornato quotidianamente. I rimanenti pc acquisiscono l'aggiornamento dell'antivirus a richiesta dell'utente, attraverso il servizio di assistenza, e, comunque, almeno ogni tre

		mesi.
Spamming o altre tecniche di sabotaggio	BASSA	Utilizzo regolamentato dell'uso di Internet e della posta elettronica. Implementazione su server aziendali di programma anti-spam, che blocca la ricezione di e-mail indesiderate.
Malfunzionamento o degrado degli strumenti elettronici	BASSA	Aggiornamento programmato del parco macchine e installazione di patch per le applicazioni da parte del servizio di assistenza
Accessi esterni non autorizzati agli strumenti elettronici	BASSA	La Rete Aziendale si configura come una rete privata e l'accesso avviene attraverso credenziali di autenticazione personali.
Accessi non autorizzati a locali o reparti ad accesso ristretto	BASSA	Disposizioni sulle procedure di accesso e dispositivi di sicurezza fisici
Asportazione e furto di strumenti contenenti dati	MEDIA	Dispositivi di sicurezza fisica e sorveglianza
Eventi distruttivi, naturali o artificiali, dolosi, accidentali	BASSA	Adozione sistema antincendio e sorveglianza
Guasti ai sistemi complementari	BASSA	Gruppi di continuità e gruppo elettrogeno per il CED

4. MISURE ADOTTATE E DA ADOTTARE ATTE A GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

Alla luce dei fattori di rischio vengono descritte sinteticamente le misure adottate al fine di garantire la sicurezza dei dati, in termini di integrità e disponibilità. Per quanto concerne il trattamento dei dati effettuato **senza l'ausilio di strumenti elettronici:**

- Le operazioni di trattamento e di conservazione dei dati sono effettuate presso uffici, locali ed archivi accessibili solo al personale incaricato del trattamento, mediante l'utilizzo di apposite chiavi a disposizione dei soli addetti;
- Gli incaricati operano seguendo le procedure e le istruzioni fornite dai Responsabili del trattamento;
- L'accesso agli archivi è controllato e consentito al solo personale specificatamente autorizzato. Dopo l'orario di chiusura le persone ammesse a qualunque titolo sono identificate e registrate. Per gli archivi che non sono dotati di strumenti elettronici per il controllo degli accessi o privi comunque di personale incaricato della vigilanza, le persone che vi accedono sono preventivamente autorizzate dal Responsabile.
- Durante le operazioni di trattamento i documenti non devono essere lasciati incustoditi sia in caso di allontanamento temporaneo dalla stazione di lavoro sia al termine della giornata qualora il trattamento non sia ancora terminato.
- L'accesso agli edifici dell'Azienda è monitorato da personale di servizio, per cui non è permesso l'accesso ad estranei non autorizzati.
- Viene annualmente verificata l'individuazione dei profili di autorizzazione.

Per quanto concerne il trattamento dei dati effettuato **con strumenti elettronici:**

- Ciascun computer integrato nella Rete Aziendale accede alle risorse condivise, quali file server, applicazioni transattive e posta elettronica, attraverso credenziali di accesso a norma. L'accesso a tali risorse viene autorizzato dal Responsabile del trattamento, il quale ha il compito di comunicare ogni variazione delle competenze dell'incaricato che comportino differenze nell'accesso ai dati.
- Ogni applicazione transattiva di medio-alta complessità e gestita dalla Struttura Complessa Sistemi Informativi Aziendali (piattaforma Oracle, SQL Server, MySQL, etc.) dispone di un sistema di autenticazione specifico. Ulteriori applicazioni di bassa complessità sono realizzate con semplici database, come MS Access, File Maker e altri, sono gestiti direttamente dall'incaricato con il sistema di autenticazione del prodotto specifico. Altrettanto dicasi per dati gestiti con applicazioni come word processor e fogli di calcolo.

- Ogni incaricato, attraverso la designazione dei Responsabili dei trattamenti, è stato edotto che la password deve essere di almeno otto caratteri e cambiata almeno trimestralmente, e che deve essere tenuta assolutamente riservata. I sistemi informatici di autenticazione che lo consentono sono parametrati per la verifica dei requisiti di lunghezza e scadenza delle password. Tali sistemi non concedono l'accesso in deroga alla politica di sicurezza.
- Sui pc stand alone su cui è installato un sistema operativo quale Windows, 2000 o XP, è stata parametrata la configurazione che prevede l'utilizzo di una password a norma di legge. Agli incaricati è stato indicato come effettuare il backup dei dati.
- Sui pc stand alone che non dispongono di un sistema di autenticazione adeguato, è compito del Responsabile del Trattamento impartire disposizioni agli incaricati dei trattamenti al fine che non siano utilizzati per la memorizzazione di dati personali e sensibili.
- E' prevista la cessazione delle credenziali di autenticazione in caso di inutilizzo delle stesse per un periodo superiore ai sei mesi, e comunque in caso di modifica dei profili di autorizzazione che identificano gli incaricati del trattamento.
- E' compito della Struttura Complessa Servizio Amministrazione del Personale comunicare alla Struttura Complessa Sistemi Informativi Aziendali le variazioni nello stato dei dipendenti che possono comportare cambiamenti nella politica delle autorizzazioni, come a titolo di esempio cessazioni dal servizio e trasferimenti di struttura.
- La Rete Aziendale è una Rete Privata, dotata di sistema informatico di sicurezza perimetrale.
- L'accesso ad Internet è rilasciato su richiesta del Responsabile della Struttura a cui appartiene il dipendente.
- All'assegnazione della matricola viene generato un account di posta aziendale per il dipendente.
- E' stata data disposizione di non abbandonare il posto di lavoro durante una sessione in cui si trattino dati personali o sensibili. In questa eventualità l'incaricato ha l'obbligo di chiudere la sessione.
- L'Azienda Sanitaria Genovese ha deliberato un regolamento relativo all'uso appropriato delle risorse informatiche, dell'uso della posta elettronica aziendale, dell'accesso a Internet. Tale provvedimento è stato adottato con la Deliberazione n. 228 del 22/2/2010. Il personale dell'Azienda è stato informato per via gerarchica ed attraverso la Intranet Aziendale dei contenuti del regolamento.

Sempre allo scopo di impedire intrusioni all'interno della Rete Aziendale è vietato a tutto il personale di utilizzare modem su elaboratori appartenente alla Rete stessa. Ogni apparecchiatura di

telecomunicazione installata abusivamente in tale configurazione verrà rimossa immediatamente dal personale coordinato dalla Struttura Complessa Sistemi Informativi Aziendali.
La Struttura Complessa Sistemi Informativi Aziendali sovrintende alle risorse del sistema operativo degli elaboratori e dei sistemi di base dati al fine di consentirne l'utilizzazione.
Le strutture tecniche aziendali, che comprendono gli amministratori di sistema, intervengono sul Sistema Informativo attraverso propri codici di accesso.
L'autenticazione degli utenti della Rete Aziendale, per l'utilizzo di risorse quali i documenti e la posta elettronica interna, avviene tramite il sistema operativo (Windows 2000, Me e XP, Window 7).
I criteri e le procedure informatiche per assicurare l'integrità e la disponibilità dei dati sono affidati alle applicazioni di gestione dei dati stessi, al RDBMS ed ai suoi meccanismi di backup e recovery.
I dati allocati all'interno dei file del RDBMS (Oracle/SQLServer) sono mascherati dal sistema di criptazione tipico del DB.
I Server dei dati sono ospitati nel CED presso la server farm Liguria Digitale e in parte presso il CED del P.O. Villa Scassi.
I backup dei dati residenti sui server di ASL3 ospitati nel CED presso la server farm Liguria Digitale, e presso il CED del P.O. Villa Scassi vengono eseguiti tutti i giorni della settimana; 6 sono di tipo "incrementale" (da lunedi' a sabato) più 1 di tipo "full" che viene effettuato nell'arco del week-end.

La "retention" dei backup è di 3 settimane.

Nel primo week-end di ogni mese il "backup full" eseguito presso il CED della server farm Liguria Digitale viene trasferito in altra sede e conservato per un anno in armadio di sicurezza.

I sistemi, le NAS e le librerie utilizzati per i backup sono ubicati in sala diversa da quella dove sono installati i sistemi ASL3 su cui risiedono i dati da salvare.

I dati salvati sono replicati su di un'altra NAS ubicata in una sede Liguria Digitale diversa dalla Server Farm.

Tutto le apparecchiature del Centro Elaborazione Dati sono oggetto di contratto di assistenza e manutenzione che garantisce la sostituzione della componentistica e la reinstallazione del software di base.
Tutte le operazioni di assistenza sono organizzate sulla base di Livelli di Servizio che governano i tempi di intervento.

5. CRITERI E MODALITA' DI RIPRISTINO DEI DATI A SEGUITO DI DISTRUZIONE O DANNEGGIAMENTO

Qualora, tra i sistemi gestititi dalla Struttura Complessa Sistemi Informativi Aziendali si dovessero verificare situazioni di emergenza derivanti dal danneggiamento di un supporto di memorizzazione (HD, CD, DVD, tape, etc) o dalla distruzione accidentale delle informazioni memorizzate, si descrive la procedura normalmente attuata:

- Individuazione del malfunzionamento da parte del personale del CED
- Attivazione dei servizi di assistenza e manutenzione
- Ripristino del sistema ed eventuale caricamento del backup.

Qualora si dovessero verificare situazioni di emergenza derivanti dal danneggiamento di un supporto di memorizzazione (HD, CD, DVD, tape, etc) o dalla distruzione accidentale delle informazioni memorizzate su un pc stand alone, si descrive la procedura normalmente attuata:

- L'utente che ha verificato l'impossibilità di accedere ai dati di cui è incaricato, comunica l'evento al Responsabile del trattamento in oggetto e contatta il servizio telefonico di assistenza informatica. Il servizio di assistenza opera all'interno di livelli di servizio definiti
- Il servizio di assistenza assegna a un tecnico l'intervento
- Attivazione dei servizi di assistenza e manutenzione
- Ripristino del sistema, ed eventuale caricamento del backup, messo a disposizione dall'incaricato del trattamento.

6. FORMAZIONE DEGLI INCARICATI AL TRATTAMENTO DATI

La formazione degli incaricati deve essere monitorata dal Responsabile del trattamento designato.
La formazione viene predisposta al momento di ingresso dell'incaricato al servizio e quando si proceda all'installazione di nuovi strumenti elettronici per il trattamento dei dati.

La formazione ha come obiettivo quello di sensibilizzare gli incaricati del trattamento sulle tematiche della sicurezza, analizzando i rischi e le responsabilità che tale operazione comporta, anche attraverso un'attenta analisi del vigente testo legislativo.

Inoltre essa tende alla compiuta spiegazione del concetto di quale sia la natura ed il contenuto dei dati sensibili e delle modalità per aggiornarsi sulle misure minime adottate dall'Azienda.

La Struttura Complessa Sistemi Informativi Aziendali svolge costantemente opera di informazione attraverso pubblicazioni sulla rete Intranet aziendale riguardanti le corrette modalità di utilizzo delle strutture tecnologiche ed applicative dell'Azienda.

Nel mese di febbraio 2005 la S.C. Affari Generali ha provveduto ad organizzare, in collaborazione con la S.C. Aggiornamento e Formazione, il primo corso di formazione per i Direttori delle Strutture Complesse Amministrative e Sanitarie.

Per quanto concerne la formazione degli incaricati, fermo restando che la stessa deve essere monitorata da ogni singolo Responsabile per le relative competenze, dato l'elevato numero degli stessi, la S.C. Affari Generali, di concerto con la S.C. Aggiornamento e Formazione, ha organizzato un corso di formazione on-line.

Il corso di formazione sia per i Responsabili, sia per gli Incaricati ha come finalità quella di far conoscere i rischi che possono incombere sui dati; le misure a disposizione per poter prevenire eventi dannosi; le disposizioni in materia di trattamento e protezione dei dati personali, le responsabilità che ne derivano e le modalità per aggiornarsi sulle misure minime adottate dal Titolare.

Il corso on line per i dipendenti dell'Azienda ha avuto inizio nel settembre 2005, prima in via sperimentale e poi, compatibilmente con le piattaforme informatiche disponibili, allargandolo a tutto il personale amministrativo e sanitario.

Nel febbraio del 2008 il corso sulla privacy è stato accreditato presso la Commissione Regionale ECM per tutte le figure professionali del ruolo sanitario.

7. MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

L'Azienda Sanitaria Locale 3 "Genovese" attraverso incarichi formali (a titolo meramente esemplificativo convenzione, contratto, ecc.) si avvale di soggetti esterni per lo svolgimento di attività e servizi, correlate alle finalità istituzionali dell'Azienda. Tali soggetti operano, pertanto, di norma, quali Responsabili esterni dell'Azienda.

La designazione del Responsabile esterno è effettuata dal Titolare, previa istruttoria dei responsabili interni. A tale scopo ogni struttura aziendale che proceda ad affidare un'attività od un servizio all'esterno della ASL 3 "Genovese" è tenuta a predisporre la nomina del soggetto affidatario Responsabile esterno del trattamento, utilizzando il modello di nomina allegato al presente documento (**allegato D**) ed allegandolo quale parte integrante e sostanziale al provvedimento di affidamento dell'attività o del servizio.

La S.C. Affari Generali collabora con le strutture aziendali qualora si renda necessario integrare il modello di nomina in relazione allo specifico trattamento di dati affidato all'esterno.

Nell'ambito degli incarichi affidati, i soggetti esterni assumono l'obbligo di operare secondo quanto previsto dalle vigenti disposizioni in materia di protezione dei dati personali, nonché secondo le istruzioni generali impartite dal Titolare e di fornire al medesimo tutte le informazioni necessarie per consentire l'attuazione di adeguate verifiche periodiche.

In particolare i citati soggetti curano i seguenti adempimenti:

- nominano gli incaricati del trattamento, all'interno delle rispettive strutture, ed impartiscono dettagliate istruzioni operative. Le relative nomine e nominativi devono essere messi a disposizione dell'ASL 3 Genovese a richiesta della stessa;
- verificano almeno annualmente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati agli incaricati del trattamento;
- assicurano e garantiscono la predisposizione e l'aggiornamento di un sistema di sicurezza dei dati conforme alle misure minime prescritte dal Decreto Legislativo 196/03 e s.m.i.;
- assicurano e verificano che i dati oggetto del trattamento siano trattati in modo lecito e secondo correttezza;
- osservano il divieto di comunicazione di dati a terzi, se non espressamente autorizzati dal Titolare, e il divieto di diffusione degli stessi;
- comunicano al Titolare ogni eventuale reclamo o istanza degli interessati, nonché ogni eventuale istanza dell'Autorità Garante per la protezione dei dati personali.

Ogni struttura deve tenere un elenco dei soggetti nominati Responsabili esterni del trattamento, conservando altresì copia dell'avvenuta nomina, che dovrà essere comunicato periodicamente e, comunque, almeno una volta all'anno entro il 31 dicembre alla S.C. Affari Generali.

8. INDIVIDUAZIONE DEI CRITERI DA ADOTTARE PER LA CIFRATURA O PER LA SEPARAZIONE DEI DATI INERENTI LO STATO DI SALUTE DAGLI ALTRI DATI PERSONALI DELL'INTERESSATO

I dati contenuti nei database dei server gestiti dalla S.C. Sistemi Informativi Aziendali sono gestiti dalla tecnologia Oracle e SQL SERVER. Tali RDBMS memorizzano i dati e le strutture all'interno di file che non sono leggibili al di fuori dell'architettura stessa, a meno che non siano stati esportati con le procedure previste.

9. CONSEGNA DEI REFERTI ON LINE

La ASL 3 Genovese ha messo a disposizione della propria utenza il servizio di consegna on line dei referti relativi agli esami di laboratorio, che consente di accedere e di stampare i propri referti via internet.

Nel rispetto della normativa in materia di riservatezza dei dati sono esclusi dalla consultazione on line i referti relativi a:

- esami per HIV;
- esami colturali;
- esami che ricomprendono analisi genetiche.

Gli incaricati del trattamento che svolgono l'attività di accettazione dovranno consegnare all'utenza l'informativa sul trattamento dei dati e acquisire di volta in volta lo specifico consenso da parte del richiedente il servizio, utilizzando i modelli di cui agli **allegati I (informativa) ed L (raccolta consenso)** al presente documento e pubblicati nell'apposita sezione del sito Internet aziendale denominata "Il referto a portata di click".

10. RESPONSABILI ED INCARICATI DEL TRATTAMENTO NELL'AMBITO DELLE SPERIMENTAZIONI CLINICHE

L'Azienda tramite le Sue strutture cliniche ospedaliere e tramite il proprio personale sanitario è coinvolta nell'ambito delle sperimentazioni cliniche in qualità di centro sperimentatore.

In relazione ai trattamenti di dati effettuato nell'ambito delle sperimentazioni citate l'Autorità garante per la protezione dei dati personali ha adottato con la Deliberazione n. 52 del 24 luglio 2008 le "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali", nelle quali sono individuate le disposizioni cui devono attenersi tanto i soggetti promotori delle sperimentazioni quanto i centri individuati per la sperimentazione medesima.

In particolare occorre precisare che tutti i dipendenti coinvolti, a vario titolo, in una sperimentazione devono essere autorizzati ad utilizzare i dati dei pazienti arruolati attraverso una designazione in qualità di responsabili od incaricati del trattamento, effettuata ai sensi degli artt. 29 e 30 del Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i.

Quindi, si prevede che le nomine dei Responsabili e degli incaricati del trattamento, effettuate secondo i modelli di nomina di cui agli allegati A e B al presente documento, siano valide anche come designazioni per il trattamento di dati personali e sensibili effettuate nell'ambito delle sperimentazioni cliniche.

11. RACCOLTA CONSENSO AL CUP REGIONALE

A partire dal 1/06/2014 è stato implementato sulle postazioni informatiche degli sportelli CUP/Anagrafe sanitaria/Sportelli Unici Distrettuali un programma per la raccolta, gestione ed archiviazione informatizzata dei consensi al trattamento dei dati personali rilasciati dai cittadini/utenti dell'Azienda.

Tale applicativo consente la gestione informatizzata dei consensi non solo a livello aziendale ma anche a livello regionale, sulla base della nuova informativa che viene resa all'utenza ai sensi dell'articolo 13 del D. Lgs. 196/2003 e s.m.i, condivisa da tutte le aziende sanitarie ed ospedaliere regionali, ad eccezione, alla data del presente aggiornamento, dell'Istituto Giannina Gaslini, e allegata al presente documento (**allegato M**). Pertanto il consenso prestato dall'interessato presso qualsiasi azienda sanitaria e ospedaliera regionale, ha valore non solo per i successivi accessi presso la medesima struttura sanitaria che ha raccolto il consenso, ma anche presso le altre strutture sanitarie ed ospedaliere regionali.

La raccolta informatizzata del consenso al trattamento dei dati è stata avviata in forma sperimentale nelle sole postazioni della ASL 3 sopra citate. Come avveniva in precedenza, la raccolta dei consensi proseguirà anche in forma cartacea presso le strutture sanitarie territoriali e presso gli ospedali dell'Azienda, fino a quando il sistema di raccolta informatizzata non verrà diffuso, reso operativo e condiviso presso tutte le restanti strutture aziendali e presso le restanti strutture sanitarie ed ospedaliere regionali.

Le Direzioni Distrettuali devono provvedere almeno trimestralmente a verificare il numero di consensi privacy raccolti tramite gli sportelli CUP/Anagrafe sanitaria/Sportelli Unici Distrettuali, comunicando contestualmente alla S.C. Affari Generali tali rilevazioni.

La Direzioni Distrettuali dovranno altresì rappresentare alla S.C. Affari Generali ogni eventuale problematica o criticità relativa alla raccolta informatizzata del consenso. Laddove tali criticità

dovessero essere di natura tecnica, afferenti pertanto l'applicativo in uso presso le suddette postazioni, le stesse dovranno essere rappresentate anche alla S.C. Sistemi Informativi Aziendali.
Sulla base delle eventuali criticità riscontrate e dei risultati della citata reportistica, le Direzioni Distrettuali, di concerto con la S.C. Affari Generali e la S.C. Sistemi Informativi Aziendali, elaboreranno semestralmente un'eventuale pianificazione operativa di implementazione del numero di consensi acquisiti.

12. PUBBLICAZIONE PROVVEDIMENTI SUL SITO INTERNET AZIENDALE PER FINALITA' DI TRASPARENZA E PER ALTRE FINALITA'

L'azienda, in virtù delle recenti disposizioni in materia di trasparenza contenute nel Decreto Legislativo 14 marzo 2013 n. 33, così come modificato dal Decreto Legislativo 25 maggio 2016 n. 97, ha l'obbligo di pubblicare una serie di provvedimenti che possono contenere anche dati personali e sensibili dei soggetti destinatari dei provvedimenti o di soggetti terzi.
A questi obblighi di pubblicazione continuano ad affiancarsi altri obblighi di pubblicità c.d. "on line" di provvedimenti contenuti in diverse disposizioni di settore, diverse da quelle in materia di trasparenza, tra cui quelli atti a garantire la pubblicità legale degli atti amministrativi, determinando anch'essi una possibile diffusione di dati personali.
Pertanto, al fine di contemperare le esigenze di pubblicità e trasparenza con i diritti alla riservatezza dei dati e delle informazioni ricompresi nei suddetti provvedimenti, l'Autorità garante per la protezione dei dati personali, con il provvedimento n. 243 del 15 maggio 2014 ha emanato le "Linee guida in materia di trattamento di dati personali, contenuti in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati".
Le suddette linee guida, contengono una serie di indicazioni a cui attenersi nel momento in cui vengono redatti gli atti che saranno oggetto di pubblicazione nel rispetto delle normative citate.
Di seguito vengono riportati i principali accorgimenti da seguire nella redazione e nella pubblicazione dei provvedimenti in argomento.

12 a) Pubblicazioni per finalità di trasparenza

Il Decreto Legislativo 14 marzo 2013 n. 33 e s.m.i. ha disciplinato in maniera organica i casi di pubblicità per finalità di trasparenza mediante inserzione di dati, informazioni, atti e documenti sui siti web istituzionali dei soggetti obbligati, precisando che "oggetto del decreto" è l'individuazione

degli obblighi di trasparenza "concernenti l'organizzazione e l'attività delle pubbliche amministrazioni".

Il riferimento è, pertanto, limitato agli "obblighi di pubblicazione concernenti l'organizzazione e l'attività delle pubbliche amministrazioni" contenuti, oltre che nel d.lgs. n. 33/2013 e s.m.i, anche in altre disposizioni normative aventi analoga finalità di trasparenza, con esclusione degli obblighi di pubblicazione aventi finalità diverse, quali ad esempio gli obblighi di pubblicazione a fini di pubblicità legale. I principi e la disciplina di protezione dei dati personali devono essere rispettati anche nell'attività di pubblicazione di dati sul web per finalità di trasparenza.

Pertanto, prima di mettere a disposizione sul sito web istituzionale informazioni, atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, occorre verificare che la normativa in materia di trasparenza preveda tale obbligo. Laddove si riscontri l'esistenza di un obbligo normativo che impone la pubblicazione dell'atto o del documento è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni. È, quindi, consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti da pubblicare sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto, nel rispetto del cd. "principio di pertinenza e non eccedenza" di cui al Decreto Legislativo 30 giugno 2003 n. 196 e s.m.i.

È, invece, sempre vietata la diffusione di dati idonei a rivelare lo "stato di salute". In particolare è vietata la pubblicazione di qualsiasi informazione da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Il procedimento di selezione dei dati personali che possono essere resi conoscibili online deve essere, inoltre, particolarmente accurato nei casi in cui tali informazioni siano relative ad altri dati sensibili o a dati giudiziari. A titolo di esempio si citano quelli idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, l'adesione a partiti e a sindacati ("dati sensibili"), oppure quelli idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonché la qualità di imputato o di indagato ("dati giudiziari").

Le suddette informazioni possono, quindi, non essere riportate nel testo dei provvedimenti da pubblicare sul sito Internet aziendale (ad esempio nell'oggetto, nel contenuto, etc.), ma citate solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento). Altro utile accorgimento può essere quello di indicare delicate situazioni di disagio personale (ad esempio

sociale, economico o legale) solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici.

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo "procedendo alla c.d. anonimizzazione dei dati personali eventualmente presenti. In proposito, si evidenzia che sostituire il nome e cognome con le iniziali del soggetto interessato dal provvedimento potrebbe non essere sufficiente ad anonimizzare i dati personali, laddove accanto alle iniziali del nome e cognome permangano ulteriori informazioni di contesto che rendono, comunque, identificabile l'interessato (quali ad esempio la residenza, il domicilio, il luogo di lavoro, il numero di telefono, la data di nascita oppure la complessiva vicenda oggetto di pubblicazione sufficiente a individuare univocamente la persona cui le stesse si riferiscono).

Con riferimento ad alcuni specifici obblighi di pubblicazione le linee guida del Garante forniscono tra le altre le seguenti indicazioni:

- *curricula professionali*

l'obbligo di pubblicazione del curriculum comporta di dover operare un'attenta selezione dei dati in essi contenuti, se del caso predisponendo modelli omogenei ed impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio curriculum in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad esempio, gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato). Non devono formare invece oggetto di pubblicazione dati eccedenti, quali, ad esempio, i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità.

- *corrispettivi e compensi*

l'entità di corrispettivi e compensi percepiti da alcune tipologie di soggetti è oggetto di pubblicazione secondo le modalità previste dal D. Lgs. n. 33/2013 e s.m.i. Tra questi ultimi sono annoverati, ad esempio, i titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza, nonché i dipendenti pubblici cui siano stati conferiti o autorizzati incarichi

Ai fini dell'adempimento degli obblighi di pubblicazione, risulta proporzionato indicare il compenso complessivo percepito dai singoli soggetti interessati, determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione. Non appare, invece,giustificato riprodurre sul web la versione integrale di documenti contabili, i dati di dettaglio risultanti dalle dichiarazioni

fiscali oppure dai cedolini dello stipendio di ciascun dipendente, come pure l'indicazione di altri dati eccedenti riferiti a percettori di somme quali, ad esempio, i recapiti individuali e le coordinate bancarie utilizzate per effettuare i pagamenti).

Non risulta inoltre giustificata la pubblicazione di informazioni relative alle dichiarazioni dei redditi dei dipendenti e dei loro familiari, ipotesi questa che la legge impone esclusivamente nei confronti dei componenti degli organi di indirizzo politico.

- *provvedimenti amministrativi*

con riferimento ai provvedimenti adottati dall'Azienda verranno pubblicati, al di fuori dei termini di legge per la pubblicità degli stessi e degli obblighi di pubblicazione integrale specificamente previsti da disposizioni di legge, solo gli elementi di sintesi quali il contenuto, l'oggetto, l'eventuale spesa prevista e gli estremi dei principali documenti contenuti nel fascicolo del procedimento, utilizzando il modello di tabella allegata al presente documento **(allegato N)**. Detta indicazione viene ancora mantenuta in vigore alla data di aggiornamento del presente documento, in attesa di specifiche ed eventuali indicazioni da parte dell'Autorità Nazionale Anticorruzione e/o dell'Autorità garante per la protezione dei dati personali, in conseguenza delle recenti modifiche apportate al D. Lgs. 33/2013. Viene pertanto altresì mantenuta la previsione dell'integrazione del suddetto modello all'interno della procedura di gestione dell'iter di adozione dei provvedimenti amministrativi, in corso di rielaborazione ed informatizzazione.

- *atti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici di importo superiore ai mille euro ed elenco dei soggetti beneficiari*

per le predette pubblicazioni è prevista l'indicazione delle seguenti informazioni: a) il nome dell'impresa o dell'ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario; b) l'importo del vantaggio economico corrisposto; c) la norma o il titolo a base dell'attribuzione; d)l'ufficio e il funzionario o dirigente responsabile del relativo procedimento amministrativo; e) la modalità seguita per l'individuazione del beneficiario; f) il link al progetto selezionato ed al curriculum del soggetto incaricato.

Non possono, invece, essere pubblicati i dati identificativi delle persone fisiche destinatarie dei provvedimenti di concessione di sovvenzioni, contributi, sussidi e attribuzione di vantaggi economici, nonché gli elenchi dei relativi destinatari:

a) di importo complessivo inferiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario;

b) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario, qualora da tali dati sia possibile ricavare informazioni relative allo stato di salute (ad esempio indicazioni quale "erogazione ai sensi della legge 104/1992");

c) di importo superiore a mille euro nel corso dell'anno solare a favore del medesimo beneficiario, qualora da tali dati sia possibile ricavare informazioni relative alla situazione di disagio economico-sociale.

Non risulta inoltre giustificato diffondere dati quali, ad esempio, l'indirizzo di abitazione o la residenza, il codice fiscale di persone fisiche, le coordinate bancarie dove sono accreditati i contributi od i benefici economici (codici IBAN), la ripartizione degli assegnatari secondo le fasce dell'Indicatore della situazione economica equivalente-Isee, l'indicazione di analitiche situazioni reddituali, di condizioni di bisogno o di peculiari situazioni abitative, etc.

12 b) Pubblicazioni per altre finalità

Anche per quanto attiene alle pubblicazioni "on line" per altre finalità, prima di mettere a disposizione sul sito internet aziendale atti e documenti amministrativi (in forma integrale o per estratto, ivi compresi gli allegati) contenenti dati personali, occorre verificare se la normativa di settore preveda espressamente tale obbligo e la relativa durata e laddove si riscontri l'esistenza di tale obbligo normativo è necessario selezionare i dati personali da inserire in tali atti e documenti, verificando, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni soprattutto ove si riscontri la presenza di dati sensibili e giudiziari.

Di seguito si riportano alcune fattispecie esplicative.

- *Pubblicazioni all'albo pretorio on line*

I provvedimenti aziendali (deliberazioni e determinazioni dirigenziali, bandi, atti dispositivi e altre tipologie di atti) sono pubblicati in forma integrale per un periodo di 15 giorni consecutivi dalla data di approvazione del medesimo o per un periodo di tempo superiore se espressamente previsto da una specifica norma di settore, a meno che non sia esclusa la pubblicazione all'albo on line per ragioni di riservatezza. In questo caso il provvedimento dovrà riportare l'indicazione *"ai sensi del D. Lgs. 30/06/2003 n. 196 e s.m.i. il presente provvedimento non verrà pubblicato"*.

Inoltre, anche alle pubblicazioni nell'albo pretorio online si applicano tutti i limiti già indicati per le pubblicazioni per finalità di trasparenza (divieto di diffusione di dati idonei a rivelare lo stato di salute e cautele per gli altri dati sensibili e giudiziari; nonché divieto di diffondere dati personali non necessari, non pertinenti o eccedenti).

Una volta trascorso il periodo temporale previsto dalle singole discipline per la pubblicazione nell'albo pretorio, i documenti e gli atti non sono più visionabili integralmente, rimanendo pubblicato all'albo aziendale on line soltanto l'oggetto.

Ciò, salvo che gli stessi atti e documenti non debbano essere pubblicati in ottemperanza agli obblighi in materia di trasparenza, in apposita sezione del sito denominata "Amministrazione

Trasparente", nella quale saranno ancora alla data di aggiornamento del presente documento pubblicate anche le tabelle riassuntive dei provvedimenti adottati infra citate (**allegato N**).

- *Graduatorie*

Con riguardo alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali – nonché, nei casi (e con le modalità) previsti, dei risultati di prove intermedie – di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati. Non possono, quindi, formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (utenze di telefonia fissa o mobile, l'indirizzo di residenza o di posta elettronica, il codice fiscale, l'indicatore Isee, il numero di figli disabili, i risultati di test psicoattitudinali, né quelli concernenti le condizioni di salute degli interessati, ivi compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Per ogni altra disposizione in materia di pubblicazione di provvedimenti aziendali sul sito internet dell'Azienda si rimanda alle linee guida dell'Autorità garante per la protezione dei dati personali, pubblicato sulla rete Intranet aziendale, nella sezione normativa/privacy.

13. TRATTAMENTO DEI DATI TRAMITE DOSSIER SANITARIO ELETTRONICO

L'Autorità garante per la protezione dei dati personali, con il provvedimento n. 331 del 4 giugno 2015 ha emanato le "Linee guida in materia di dossier sanitario", delineando un quadro di riferimento unitario per disciplinare i trattamenti di dati tramite l'utilizzo dei dossier sanitari.

In considerazione di tale provvedimento l'Azienda ha intrapreso un percorso al fine di allineare le proprie procedure alle recenti linee guida in argomento, che ha determinato in questa fase iniziale la predisposizione di una informativa specifica in materia di trattamento dei dati tramite dossier sanitario **(allegato O),** del modello di acquisizione del consenso per la costituzione del dossier **(allegato P)**, del modello per la richiesta di oscuramento dell'evento clinico **(allegato Q),** nonché la predisposizione di un portale aziendale per la raccolta e gestione del consenso informatizzato, sia per le finalità di cura ai sensi dell'art. 76 del D. Lgs. 196/2003 e s.m.i. sia per l'ulteriore finalità di cura tramite l'utilizzo del Dossier Sanitario Elettronico, che è stato implementato a partire dal mese di ottobre 2016. In parallelo sono iniziati i corsi di formazione per il personale dipendente autorizzato all'utilizzo del dossier sanitario elettronico, corsi che prevedono una parte di Formazione A Distanza (FAD) ed una parte informatico – operativa in aula. I dipendenti che accederanno al dossier sanitario elettronico dovranno essere individuati quali incaricati al

trattamento dei dati ai sensi dell'art. 30 del D.Lgs. 196/2003 e s.m.i., utilizzando il modello di nomina allegato al presente documento **(allegato R).**

14. AGGIORNAMENTO PERIODICO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente Documento Programmatico sulla Sicurezza è sottoposto ad aggiornamento annuale, entro la scadenza del 31 dicembre di ciascun anno.

ALLEGATO A: NOMINA RESPONSABILE DEL TRATTAMENTO DATI

NOMINA DEL RESPONSABILE PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 29 DEL DECRETO LEGISLATIVO 196/03 e s.m.i.

L'Azienda Sanitaria Locale 3 "Genovese", titolare del trattamento dei dati, con sede in Via Bertani 4, Genova, nella persona del Commissario Straordinario Dott.....

NOMINA

Il Dott..... in qualità di responsabile della Struttura....., **Responsabile del trattamento** dei dati personali, nell'ambito delle funzioni e competenze cui è preposto, in quanto, per esperienza, capacità ed affidabilità, fornisce idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

A tal fine vengono fornite specifiche informazioni ed istruzioni al Responsabile del trattamento dei dati, di seguito riportate.

E' compito del Responsabile del trattamento:

- Verificare che i dati personali oggetto del trattamento siano
f) trattati in modo lecito e secondo correttezza
g) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi
h) esatti e se necessario aggiornati
i) pertinenti, completi e non eccedenti rispetto alle finalità per i quali sono raccolti o successivamente trattati
j) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati
- Evadere le eventuali domande di accesso, di aggiornamento, di rettifica, di integrazione, di cancellazione, di trasformazione in forma anonima e di blocco dei dati presentate su istanza dall'interessato ai sensi degli artt. 7 e 10 D. Lgs. 196/03 e s.m.i.

- Vigilare sul rispetto e sull'adozione delle misure di sicurezza predisposte dal Titolare del trattamento e riportate nel Documento Programmatico sulla Sicurezza e comunque assicurare la predisposizione e l'aggiornamento delle stesse in modo conforme alle misure minime previste nel D. Lgs. 196/03 e s.m.i.
- Procedere alla nomina dei soggetti incaricati del trattamento dei dati, compresi eventualmente quelli inseriti nei dossier sanitari (con incarico specifico), impartendo loro specifiche istruzioni circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza, dandone comunicazione alla S.C. Affari Generali. Nell'ambito delle istruzioni così impartite dovranno essere rilasciati i profili di autorizzazione al trattamento dei dati a ciascun incaricato, nonché vigilare che l'accesso ai dati da trattare da parte degli incaricati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate. In merito al mantenimento delle predette autorizzazioni il nominato responsabile avrà anche il compito di verificare almeno annualmente la sussistenza delle condizioni che hanno determinato la loro emanazione ed in difetto di procedere alla revoca delle stesse. La nomina dovrà essere effettuata sistematicamente nei confronti di tutti i neoassunti assegnati alla struttura che effettuano trattamento dei dati;
- Verificare che la fase di raccolta del consenso al trattamento dei dati sia preceduta da idonea informativa
- Osservare le disposizioni e gli obblighi derivanti dal D. Lgs. 196/03 e s.m.i. in particolare per quelli inerenti la comunicazione e la diffusione dei dati
- Osservare le istruzioni impartite dal Titolare del trattamento, anche quali risultanti dal Documento Programmatico aziendale sulla Sicurezza dei dati trattati.

  (1)

  Per ogni altra misura ed istruzione qui non prevista si rinvia alle disposizioni di cui al Decreto Legislativo 196/03 e s.m.i. (e relativi allegati), e al Documento Programmatico sulla Sicurezza pubblicato sulla rete intranet aziendale nella sezione normativa/privacy.

Genova, lì.....

Il Commissario Straordinario

Dott.....

IL Direttore della Struttura.....

Dott.....

(1) In caso di trattamento di dati tramite dossier sanitari inserire:

La S.V. è altresì nominata responsabile del "trattamento dei dati personali", ai sensi del decreto legislativo 196/03 e s.m.i., con riferimento ai trattamenti effettuati tramite Dossier Sanitario Elettronico, svolti per finalità di prevenzione, diagnosi, cura e riabilitazione degli interessati, nell'ambito delle funzioni e competenze cui è preposta.

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
- inserimento dati
- modifica, aggiornamento dei dati
- stampa documenti
- altro _____

  (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 incaricata di trattare i dati personali e sensibili strettamente necessari allo svolgimento delle mansioni assegnate e a rispettare e le misure di sicurezza predisposte dal titolare del trattamento dei dati e alla puntuale adozione delle istruzioni impartite dal sottoscritto 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 decreto, alle linee guida dell'autorità garante per la protezione dei dati personali in materia di dossier sanitario e al Documento Programmatico sulla Sicurezza (entrambi pubblicati sulla rete Intranet Aziendale nella sezione normativa/privacy) nonché alle istruzioni operative fornite.

ALLEGATO B: NOMINA INCARICATI TRATTAMENTO DATI

Struttura .....

Direttore.....
Tel. 010 .....
Fax 010 .....
e-mail.....

Genova, ...

Prot.n. /

Al Sig.

NOMINA AD INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 30 Del Decreto Legislativo N° 196 del 30/06/2003 e s.m.i.

"Codice In Materia Di Protezione Dei Dati Personali"

Il sottoscritto Dott. ..... Direttore della Struttura..... Responsabile del trattamento dei dati personali ai sensi dell'art. 29 del decreto legislativo 196/03 e s.m.i., con il presente atto **nomina la S.V. "incaricato del trattamento dei dati personali"**, ai sensi del decreto legislativo 196/03 e s.m.i., con riferimento ai trattamenti svolti nell'ambito delle funzioni e competenze cui è preposto.

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 ottemperanza al decreto legislativo 196/03 e s.m.i. che regola il trattamento dei dati personali, laddove costituisce trattamento "*qualunque operazione o complesso di operazioni effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati, anche se non registrati in una banca dati*", ed in relazione al presente atto di nomina, la S.V. è incaricata di trattare i dati personali (qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso il numero di identificazione personale, ad es. i dati anagrafici, i recapiti telefonici, il numero di matricola, ecc.) strettamente necessari allo svolgimento delle mansioni proprie assegnate:

- in modo lecito e secondo correttezza;
- a raccoglierli e registrarli per gli scopi determinati, espliciti e legittimi inerenti l'attività svolta da ciascuno ed utilizzati in altre operazioni del trattamento in termini compatibili con gli stessi scopi;
- a verificare la loro esattezza e, se necessario, aggiornarli;
- 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 sottoscritto o dal titolare del trattamento dei dati;
- a conservarli, in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi 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;
- a rispettare e adottare le misure di sicurezza predisposte dal titolare del trattamento dei dati e riportate sul Documento programmatico sulla sicurezza nonché alla puntuale adozione delle istruzioni impartite dal sottoscritto circa la corretta gestione e tutela dei dati personali anche ai fini della loro integrità e sicurezza;
- a fornire l'idonea informativa nei casi di raccolta del consenso al trattamento dei dati;
- osservare le disposizioni e gli obblighi derivanti dal D.Lgs 196/2003 e s.m.i., in particolare per quelli inerenti la comunicazione e la diffusione dei dati.

Per ogni altra misura si rinvia alle disposizioni di cui al succitato decreto e al Documento Programmatico sulla Sicurezza (entrambi pubblicati 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'incaricato 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/o del Responsabile.

Il Responsabile del Trattamento
Dott.....
Direttore Struttura.....

Allegato: istruzioni ed informazioni operative

ALLEGATO C: ISTRUZIONI OPERATIVE INCARICATI

Struttura.....
Direttore
Tel.
Fax
e-mail

Allegato alla nomina a incaricato del trattamento dei dati personali ai sensi dell'art. 30 del Decreto Legislativo N° 196 del 30/06/2003 e s.m.i. "Codice in Materia di Protezione dei Dati Personali": INFORMAZIONI, MISURE MINIME DI SICUREZZA ED ISTRUZIONI OPERATIVE **(nota prot. n. ..... del .....)**

Il Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. "codice in materia di protezione dei dati personali" prevede 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 legge in oggetto individua tre figure fondamentali:

1. Il Titolare del trattamento;
2. Il Responsabile del trattamento;
3. Gli Incaricati del trattamento.

Il **Titolare del trattamento** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza. E' Responsabile dell'attuazione dei precetti normativi previsti dalla Legge.

Il titolare del trattamento ai sensi dell'art.4 del D.L.vo 196/2003 e s.m.i. è la A.S.L. 3 Genovese.

Il **Responsabile del trattamento,** nominato dal titolare, deve provvedere all'applicazione di tutti i compiti impartiti dal Titolare, nonché fornire, ai sensi dell'art. 30, agli incaricati del trattamento istruzioni in merito alle operazioni di raccolta e trattamento dei dati, nonché vigilare sulla corretta applicazione delle medesime.

L'**Incaricato del trattamento**, nominato dal Titolare e/o dal Responsabile, deve elaborare i dati personali ai quali ha accesso attenendosi alle istruzioni del titolare o del Responsabile.

Al Responsabile ed all'Incaricato del trattamento sono devoluti compiti volti a garantire una puntuale applicazione della Legge sulla Privacy.

Sulla base di quanto sopra, dopo che con note formali il Titolare del Trattamento dei dati ha provveduto alla nomina dei Responsabili del trattamento, attribuendogli il compito di provvedere alla nomina degli incaricati, nonché di impartire loro specifiche istruzioni circa la corretta gestione e tutela dei dati personali, anche ai fini della loro integrità e sicurezza, si rende necessario provvedere alla individuazione dei soggetti incaricati del trattamento, onde garantire la puntuale ed ottimale applicazione del D.L.vo 196/2003 e s.m.i..

Gli incaricati del 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 e/o dal Responsabile.

Dell'espletamento di tali funzioni rispondono direttamente e personalmente al Responsabile del trattamento ed al Titolare.

Questa comunicazione è l'allegato dell'atto formale di nomina della S.V. ad incaricato del trattamento dei dati personali nell'ambito del servizio proprio.

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 "*qualunque operazione o complesso di operazioni effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distribuzione dei dati, anche se non registrati in una banca dati*".

Si fa presente che, per quanto riguarda il trattamento dei dati personali da parte di soggetti pubblici, l'art.18 del D.L.vo 196/2003 e s.m.i., stabilisce che "*qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali*".

L'art. 4 definisce alcuni dati particolari "dati sensibili" e li individua nei dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati idonei a rivelare lo stato di salute e la vita sessuale.

In assenza di specifiche disposizioni di legge nella quale siano specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (art. 20 comma 1), gli stessi possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del garante (art. 26 comma 1).

Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, trattano i dati personali idonei a rivelare lo stato di salute (art 75):

-con il consenso dell'interessato e anche senza l'autorizzazione del garante, se il trattamento riguarda dati ed operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

-anche senza il consenso dell'interessato e previa autorizzazione del garante se la finalità di cui sopra riguarda un terzo o la collettività.

Per quanto riguarda la comunicazione all'interessato (art. 84), i dati idonei a rivelare il suo stato di salute possono essergli resi noti solo per il tramite di un medico da lui stesso designato ovvero designato dal titolare.

In ottemperanza al D.L.vo 196/2003 e s.m.i. che regola il trattamento dei dati personali ed in relazione al presente atto di nomina, la S.V. è incaricata di trattare i dati personali (qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso il numero di identificazione personale, ad es. i dati anagrafici, i recapiti telefonici, il numero di matricola, ecc.):

- in modo lecito e secondo correttezza;
- a raccoglierli e registrarli per gli scopi inerenti l'attività svolta da ciascuno;
- a verificare, ove possibile, la loro esattezza e, se necessario, aggiornarli;
- 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 o dal Responsabile;
- a conservarli, osservando scrupolosamente tutte le misure di sicurezza predisposte in Azienda, o che verranno comunicate in seguito dal Titolare o dal Responsabile. In ogni operazione di trattamento andrà garantita la massima riservatezza.

Nell'espletamento del proprio incarico la S.V. dovrà, inoltre, attenersi alle seguenti istruzioni:

1. collaborare 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;
2. attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti dell'interessato;
3. comunicare al Responsabile ogni necessità di predisporre la notificazione al Garante e le eventuali successive variazioni in caso di nuova tipologia di trattamento di dati sensibili o di cessazione di trattamento, verificando l'esattezza e la completezza dei dati contenuti;
4. presentare al Responsabile ogni richiesta di autorizzazione preventiva al trattamento dei dati sensibili (quando necessaria) da inviare al Garante;

5. collaborare con il Responsabile per l'attuazione delle prescrizioni del Garante;
6. attuare i dispositivi di sicurezza idonei a rispettare le indicazioni del D.Lgs. 196/2003 e s.m.i.;
7. comunicare al Responsabile ogni difficoltà o irregolarità delle procedure di applicazione;
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.) ed a restituirli al termine delle operazioni affidate; sulla base di quanto sopra, in caso di allontanamento, anche temporaneo, dal posto di lavoro, l'incaricato 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. 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:
11. 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;
12. Qualora il trattamento dei dati, la formazione e la comunicazione di documenti ed atti, avvenga con strumenti elettronici dovranno essere accuratamente applicate le indicazioni previste dall'allegato B del D.Lgs. 196/2003 e s.m.i. "disciplinare tecnico in materia di misure minime di sicurezza".
    In particolare:
    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'incaricato);
    b) la password personale dovrà essere modificata ogni tre mesi e ogni qualvolta il responsabile del trattamento abbia motivo di ritenere che non sia di sua esclusiva conoscenza;
    c) i supporti rimovibili (floppy disk, cd rom, 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;
    d) i supporti rimovibili contenenti dati sensibili, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati solo se le informazioni precedentemente in essi contenute non sono intelligibili e in nessun modo tecnicamente ricostruibili.

13. Sempre allo scopo di conformarsi alle disposizioni in materia di privacy e a quanto contenuto nel Documento Programmatico sulla Sicurezza, si indica la procedura che viene utilizzata per consentire operazioni di trattamento dei dati in caso di prolungata assenza o di impedimento dell'incaricato 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, dietro richiesta scritta del Responsabile del trattamento, nel caso di documentata necessità di accedere ai dati gestiti da un incaricato, è in grado di rimuovere la password di quell'utente e generarne una nuova che viene consegnata al Responsabile del trattamento esclusivamente per effettuare l'accesso straordinario. In ogni caso, gli amministratori di sistema non possono entrare in conoscenza della password originale dell'utente e utilizzarla 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. Il Responsabile del trattamento che ha richiesto la procedura di accesso straordinario è tenuto ad avvertire tempestivamente l'incaricato che è stata attivata la procedura di generazione di nuove credenziali d'accesso. In ogni caso l'incaricato non potrà più utilizzare le precedenti credenziali e per accedere al sistema dovrà richiederne di nuove.

La S.C. Sistemi Informativi Aziendali esegue le incombenze di cui al punto 11 (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 Unità Operative e ai Dipartimenti.

Per quanto concerne la gestione degli archivi cartacei (archivio clinico, protocollo, ecc) 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. Nessun dato potrà essere comunicato a terzi o diffuso senza la specifica autorizzazione del Titolare e/o del Responsabile.
6. 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 o del Responsabile del trattamento.

Nel formalizzarle l'assegnazione del ruolo di incaricato del trattamento dei dati è fondamentale precisare l'importanza e la responsabilità che tale ruolo comporta all'interno dell'applicazione del D.L.vo 196/2003 e s.m.i.. Infatti Le ricordo che tale legge prevede gravi sanzioni in caso di illecito trattamento dei dati, variabili, secondo tipologia e gravità, dalla reclusione da 6 mesi fino a 3 anni, al pagamento di sanzioni amministrative. Per ogni difficoltà o per qualsiasi chiarimento la S.V. potrà rivolgersi alla scrivente che è disponibile per ogni eventuale ulteriore delucidazione in merito.

Il Responsabile del Trattamento
DIRETTORE S.C.....

Allegato alla nomina ad incaricato del trattamento dei dati ai sensi dell'art.30 del D.L.vo 196/2003 e s.m.i.

ALLEGATO D: NOMINA RESPONSABILE ESTERNO TRATTAMENTO DATI

NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DATI

Ai sensi del D. Lgs. 196/03 e s.m.i., "Codice in materia di protezione dei dati personali", l'Azienda Sanitaria Locale 3 "Genovese", Titolare del trattamento, **nomina** con il presente atto la **Società/Ditta/Cooperativa/Sig.....**, con sede in....., in relazione alle attività di cui al Contratto/Convenzione/Deliberazione....., **Responsabile esterno del trattamento dati** a tutti gli effetti legali, secondo i criteri, le modalità e le istruzioni di seguito specificate.

I trattamenti di dati personali e sensibili, cui la Società/Ditta/Cooperativa/Sig..... è nominata Responsabile, consistono in particolare nei trattamenti necessari alle attività di.... (inserire oggetto del rapporto derivante dal contratto, convenzione o deliberazione). Tali operazioni di trattamento possono riguardare i dati personali e sensibili (indicare tipologia di dati principali oggetto di trattamento).

La ASL 3 "Genovese" affida pertanto alla **Società/Ditta/Cooperativa/Sig** .....ogni incombenza connessa all'esecuzione dell'incarico in questione necessaria e opportuna per l'esercizio dei compiti affidati.

Quanto sopra fermo restando l'obbligo a carico della **Società/Ditta/Cooperativa/Sig** .....di operare secondo quanto previsto dalle vigenti norme di legge in materia di protezione dei dati personali, di cui al D. Lgs. 30/6/2003 n. 196 e successive modificazioni ed integrazioni, nonché secondo le istruzioni generali impartite dal Titolare e di fornire al medesimo tutte le informazioni necessarie per consentire l'attuazione di adeguate verifiche periodiche.

In base alla presente nomina a Responsabile del trattamento, la **Società/Ditta/Cooperativa/Sig** .....dovrà in particolare curare i seguenti adempimenti:

- **nominare gli incaricati del trattamento all'interno della struttura della Società/Ditta/Cooperativa/Sig.....e fornire loro dettagliate istruzioni operative. Le relative nomine e nominativi devono essere messi a disposizione dell'ASL 3 Genovese a richiesta della stessa;**
- **verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione assegnati agli incaricati del trattamento;**

- **assicurare la predisposizione e aggiornamento di un sistema di sicurezza dei dati conforme alle misure minime prescritte nel D. Lgs. 196/2003 e s.m.i.;**
- **assicurare e verificare che i dati oggetto del trattamento siano trattati in modo lecito e secondo correttezza, e comunque nel rispetto delle disposizioni di cui al D. Lgs. 196/03 e s.m.i.;**
- **osservare il divieto di comunicazione e di diffusione a terzi dei dati trattati;**
- **comunicare tempestivamente alla ASL 3 Genovese ogni eventuale reclamo o istanza dovesse ricevere dagli interessati, nonché ogni eventuale istanza o richiesta di chiarimenti dell'Autorità Garante per la protezione dei dati personali.**

La presente nomina ha durata corrispondente alla esecuzione del contratto/convenzione/deliberazione in corso tra la ASL 3 "Genovese" e la **Società/Ditta/Cooperativa/Sig** e si intenderà revocata alla cessazione del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.

Data.....

Il Titolare del trattamento
Commissario Straordinario
Dott.....

Per accettazione
Società/Ditta/Cooperativa/Sig

_____

ALLEGATO E: Informativa ex art.13 Dlgs 30.06.2003 n.196 e s.m.i.

Egr. Sig./Sig.ra

Il D. lgs. 196/2003 e s.m.i. riconosce e disciplina il diritto alla protezione dei dati personali. La ASL 3 "Genovese", in attuazione della legge e nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale, La informa con la presente informativa su come vengono trattati i Suoi dati presso questa azienda sanitaria.

La presente informativa viene fornita per l'insieme dei trattamenti di dati personali e sensibili effettuati nel complesso delle strutture facenti capo alla A.S.L. 3 "Genovese", anche in regime libero professionale intramoenia per:

- tutelare la Sua salute o la Sua incolumità fisica;
- tutelare la salute o la incolumità fisica di altre persone o della collettività, per fini di sanità e igiene pubblica;
- svolgere attività di formazione e didattiche;
- finalità di ricerca scientifico-statistica e/o di prevenzione;
- prescrivere farmaci ed esami sanitari;
- accertare e certificare il Suo stato di salute e provvedere a tutti gli altri adempimenti, anche amministrativi e contabili, occorrenti per l'espletamento delle attività istituzionali.

L'azienda sanitaria, per le attività amministrative, anche se strumentali alle attività di prevenzione, diagnosi, cura e riabilitazione, tratta i dati sensibili in base al regolamento Regionale 16 maggio 2006 n. 1 "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".

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

Quando Lei accede ad una delle strutture dell'azienda per una prestazione sanitaria, sia in regime ambulatoriale che di ricovero, Le vengono chiesti da parte degli operatori i dati personali (nome, cognome, codice fiscale, tipo di esenzione, etc.) necessari ed obbligatori per provvedere ad erogarLe e/o prenotarLe la prestazione richiesta (ad esempio assegnazione del medico di base, prenotazione della visita, etc.)

L'azienda sanitaria necessita per legge di un Suo specifico consenso per poter trattare i dati riguardanti il Suo stato di salute. Il rilascio del suddetto consenso è necessario per consentire alla struttura presso cui effettuerà la prestazione di trattare i Suoi dati di salute per curarLa in modo appropriato; l'eventuale rifiuto a prestare il consenso comporta l'impossibilità di erogare la prestazione richiesta, che Le verrà erogata solo in caso di urgenza o se disposta dalla Pubblica Autorità ed i Suoi dati verranno conservati solo per il tempo previsto dalla legge.

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, che verrà utilizzato, fino a Sua diversa indicazione, per confermarLe o ricordarLe il giorno della prenotazione o per avvisarLa 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 suoi dati anagrafici e il reparto di degenza in cui Lei è ricoverato/a saranno disponibili per agevolare l'accesso ai reparti di degenza da parte dei visitatori; nel caso in cui Lei non intenda renderli disponibili, può in occasione di ogni ricovero, manifestare l'eventuale specifico dissenso.

Al fine di evitare ripetute richieste del "consenso privacy" da parte di ogni singola struttura della A.S.L. 3 "Genovese"ed in conformità a quanto legislativamente previsto potrà manifestare il Suo consenso con un'unica dichiarazione. Si evidenzia che tale consenso sarà valido ed efficace fino a revoca dello stesso.

I dati da Lei rilasciati alla ASL 3 "Genovese" potranno essere utilizzati sia in modo manuale che informatizzato dal personale debitamente autorizzato al trattamento dei dati, in qualità di responsabile o di incaricato del 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 di cui sopra.

I Suoi dati potranno inoltre essere comunicati, quando ciò risulti necessario in relazione all'erogazione della prestazione o allo svolgimento dei compiti istituzionali attribuiti all'Azienda a medici convenzionati, strutture convenzionate, altre Aziende Sanitarie ed Ospedaliere, farmacie convenzionate, altri soggetti pubblici e privati, nei casi consentiti dalla normativa vigente oppure su Sua specifica richiesta o indicazione.

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

In ogni momento potranno essere esercitati i diritti di cui all'art. 7 del D. Lgs. 196/2003 e s.m.i. che riconosce tra gli altri il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne l'aggiornamento, la rettifica ovvero l'integrazione, la cancellazione-trasformazione in forma anonima ed il blocco dei dati se trattati in violazione di legge.

Il titolare del trattamento è l'Azienda Sanitaria Locale 3 "Genovese", con sede in Via Bertani 4 – 16125 Genova.

ALLEGATO F: RACCOLTA CONSENSO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI
ai sensi del Decreto Legislativo n. 196 del 30/6/2003 e s.m.i.

Il/La sottoscritto/a_____

nato/a a _____prov. di _____

il_____C.F._____

in nome proprio

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

_____

parente (familiare o congiunto da compilare solo in caso di incapacità fisica, giuridica o incapacità di intendere e volere dell'interessato ai sensi art. 82 comma 2 lettera a) del D. Lgs. 196/2003 e s.m.i.)

convivente da compilare solo in caso di incapacità fisica, giuridica o incapacità di intendere e volere dell'interessato ai sensi art. 82 comma 2 lettera a) del D. Lgs. 196/2003 e s.m.i.)

del/della Sig / Sig ra / minore _____

nato/a_____il_____

residente a _____ Via/ Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa di cui all'art. 13 del D. Lgs. 196/03 e s.m.i. in materia di protezione dei dati personali ed **esprimo il consenso** al trattamento dei dati personali e sensibili, 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 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 dell'interessato

_____

_____

1 A cura dell'operatore incaricato:

Identificato l'interessato a mezzo C.I./Pat.....n.....
Rilasciata da .....il.....

Firma dell'operatore incaricato

ALLEGATO G: RACCOLTA CONSENSO OSPEDALIERO AL TRATTAMENTO DEI DATI PERSONALI E SENSIBILI

ai sensi del Decreto Legislativo n. 196 del 30/6/2003

Il/La sottoscritto/a[1] _____

nato/a a _____ _____ _____ _____(_____)

il_____ __, C.F._____ _____ _____ _____ _____

in nome proprio

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

_____ _____ _____ _____ _____ _____

parente (familiare o congiunto da compilare solo in caso di incapacità fisica, giuridica o incapacità di intendere e volere dell'interessato ai sensi art. 82 comma 2 lettera a) del D. Lgs. 196/2003 e s.m.i.)

convivente (da compilare solo in caso di incapacità fisica, giuridica o incapacità di intendere e volere dell'interessato ai sensi art. 82 comma 2 lettera a) del D. Lgs. 196/2003 e s.m.i.)

del/della Sig / Sig ra / minore

_____ _____ _____ _____ _____ _____

nato/a_____ _____ _____ _____ _____il_____ _____ _____

residente a _____ _____ _____ _____Via/ Piazza_____ _____ _____

dichiaro di aver ricevuto, letto e compreso l'informativa di cui all'art. 13 del D. Lgs. 196/03 e s.m.i. in materia di protezione dei dati personali ed **esprimo il consenso** al trattamento dei dati personali e sensibili, 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 "Genovese" 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 ai seguenti familiari/conviventi/persone di fiducia: SI NO

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

_ _____ _____ _____ _____ _____ _____ _____ _____ _____ _

I A cura dell'operatore incaricato:

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

Rilasciata da.....il..... Firma dell'operatore incaricato

ALLEGATO H: Informativa ex art. 13 D.lgs. 30.06.2003, n. 196 e s.m.i. per il trattamento dei dati personali e sensibili dei dipendenti

Il D.lgs. 196/2003 e s.m.i. riconosce e disciplina il diritto alla protezione dei dati personali. Nell'osservanza della legge, il trattamento dei dati si svolgerà nel rispetto dei diritti e delle libertà fondamentali degli individui, nonché della loro dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali e sensibili.

Ai sensi dell'articolo 13 del D.lgs. 196/2003 e s.m.i. 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, si informano pertanto i dipendenti che:

a) I dati personali e sensibili direttamente forniti dal dipendente o raccolti presso terzi o attraverso altre fonti nel rispetto della normativa vigente, sono trattati 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 sensibili, 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 ASL 3 Genovese.
b) In particolare Il trattamento ha come oggetto ogni attività e operazione concernenti 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.
c) Il conferimento dei dati è necessario per l'esecuzione degli obblighi derivanti dal rapporto di lavoro. Il conferimento dei dati relativi ai propri familiari è obbligatorio considerato che, in caso di domande o 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.
d) I dati personali e sensibili sono trattati in modo lecito e corretto, raccolti esclusivamente per le finalità di cui ai punti a) e b), costantemente aggiornati e conservati per un periodo non superiore a quello necessario agli scopi per cui i dati vengono raccolti;
e) Il trattamento è effettuato mediante supporto cartaceo e/o mediante strumenti automatizzati e l'accesso ai dati ed il relativo trattamento è consentito al personale debitamente individuato come incaricato del trattamento dei dati e con l'adozione delle misure minime di sicurezza prescritte dal Codice in materia di protezione dei dati personali;
f) 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", 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 dei dipendenti. L'elenco degli amministratori di sistema è consultabile nel Documento Programmatico sulla Sicurezza, pubblicato sulla rete Intranet aziendale nella sezione " *Normativa/privacy*";
g) I dati personali necessari alla predisposizione dei cedolini paga e del CUD sono inoltre 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
h) I dati dei dipendenti possono inoltre essere comunicati 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;
i) Il titolare del trattamento è l'Azienda Sanitaria Locale 3 "Genovese" con sede legale in Via Bertani 4 – 16125 Genova
j) Il Responsabile del trattamento dati il Direttore della S.C. Servizio Amministrazione del Personale.
k) In ogni momento ogni dipendente può esercitare nei confronti del Titolare del trattamento, i diritti di cui all'art. 7 del D. Lgs. 196/2003 e s.m.i., che per comodità si riproduce integralmente.

Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

ALLEGATO I: INFORMATIVASERVIZIO CONSEGNA REFERTI ON LINE

CONSEGNA REFERTI ON LINE

Informativa ai sensi del D. Lgs. n. 196 del 30/6/2003 e s.m.i.

Egr. Sig./Sig.ra

La ASL 3 "Genovese", in attuazione della legge e con particolare riferimento al D.Lgs. 196/2003 e s.m.i. ed alle Linee Guida in tema di referti on line del 19/11/2009 dell'Autorità Garante per la protezione dei dati personali, nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale, La informa 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.

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 autorizzato al trattamento dei dati, in qualità di responsabile o di incaricato del trattamento, 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 minime di sicurezza di cui al D.Lgs. 196/2003 e s.m.i., 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 all'art. 7 del D. Lgs. 196/2003 e s.m.i., che riconosce, tra gli altri, il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne l'aggiornamento, la rettifica ovvero l'integrazione, la cancellazione-trasformazione in forma anonima ed il blocco dei dati se trattati in violazione di legge.

Il titolare del trattamento è l'Azienda Sanitaria Locale 3 "Genovese", con sede in Via Bertani 4 - 16125 Genova.

ALLEGATO L: MODELLO RACCOLTA CONSENSO SERVIZIO CONSEGNA REFERTI ON LINE

RACCOLTA CONSENSO PER CONSEGNA REFERTI ON-LINE

ai sensi del Decreto Legislativo n. 196 del 30/6/2003 e s.m.i.

Il/La sottoscritto/a [1] _____

nato/a a_____(_____)

il_____ _C.F._____

in nome proprio

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

del/della Sig / Sig ra / minore _____

nato/a _____il_____

residente a_____Via/Piazza_____

dichiaro di aver ricevuto, letto e compreso l'informativa relativa alla consegna dei referti on-line, di cui all'art. 13 del D. Lgs. 196/03 e s.m.i. in materia di protezione dei dati personali ed **esprimo il consenso** alla consegna del mio referto di laboratorio on line

☐ SI ☐ NO

Esprimo inoltre il consenso al fine di utilizzare il seguente numero di cellulare.....per avvisarmi che il referto è pronto ed accessibile on line e per comunicarmi i valori di INR attraverso SMS

☐ SI ☐ NO

Genova, __/___/_ _

Firma dell'interessato

.....

1 A cura dell'operatore incaricato:

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

Rilasciata da .....il.....

Firma dell'operatore incaricato

ALLEGATO M: INFORMATIVA UNIFICATA REGIONALE

Egr. Sig./Sig.ra

Il D. lgs. 196/2003 e s.m.i. riconosce e disciplina il diritto alla protezione dei dati personali. In attuazione della legge e nel rispetto dei Suoi diritti e libertà fondamentali e della Sua dignità personale, la presente informativa viene fornita per l'insieme dei trattamenti dei dati personali e sensibili effettuati, anche in regime di libero professionale intramoenia, nel complesso delle strutture facenti capo alle A.S.L.Liguri, all'Ente Ospedaliero Ospedali Galliera, all'IRCSS Azienda Ospedaliera Universitaria San Martino-IST e all'Ospedale Evangelico Internazionale per:

- tutelare la Sua salute o la Sua incolumità fisica;
- tutelare la salute o la incolumità fisica di altre persone o della collettività, per fini di sanità e igiene pubblica;
- svolgere attività di formazione e didattiche;
- finalità di ricerca scientifico-statistica e/o di prevenzione;
- prescrivere farmaci ed esami sanitari;
- accertare e certificare il Suo stato di salute e provvedere a tutti gli altri adempimenti, anche amministrativi e contabili, occorrenti per l'espletamento delle attività istituzionali.

Le A.S.L.Liguri, l'Ente Ospedaliero Ospedali Galliera, l'IRCSS Azienda Ospedaliera Universitaria San Martino-IST e l'Ospedale Evangelico Internazionale (di seguito Aziende/Enti), al fine di garantire una miglior integrazione della propria offerta sanitaria ed un crescente livello qualitativo dei servizi offerti ai cittadini, hanno deciso di uniformare le proprie procedure di raccolta e registrazione della presente informativa, anche al fine di consentire l'interscambio di dati fra le suddette Aziende/Enti, nei limiti e secondo le modalità di seguito riportate.

INFORMAZIONI DI CARATTERE GENERALE

Le Aziende/Enti, per le attività amministrative, anche se strumentali alle attività di prevenzione, diagnosi, cura e riabilitazione, trattano, ciascuno con propri sistemi e procedure, i dati sensibili in base al regolamento Regionale 9 aprile 2013 n. 2 "Regolamento per il trattamento dei dati personali sensibili e giudiziari ai sensi degli articoli 20 e 21 del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) e s.m.i. ed accolgono le indicazioni del Gruppo dei Garanti Europeo sul trattamento elettronico dei dati effettuato con la cartella clinica elettronica ed il dossier sanitario.

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

Quando Lei accede ad una delle strutture dell'Azienda/Ente per una prestazione sanitaria, sia in regime ambulatoriale che di ricovero, Le vengono chiesti da parte degli operatori i dati personali (nome, cognome, codice fiscale, tipo di esenzione, etc.) necessari ed obbligatori per provvedere ad erogarLe e/o prenotarLe la prestazione richiesta (ad esempio assegnazione del medico di base, prenotazione della visita, etc.)

L'Azienda/Ente necessita per legge di un Suo specifico consenso per poter trattare i dati riguardanti il Suo stato di salute. Il rilascio del suddetto consenso è necessario per consentire alla struttura presso cui effettuerà la prestazione di trattare i Suoi dati di salute per curarLa in modo appropriato; l'eventuale rifiuto a prestare il consenso comporta l'impossibilità di erogare la prestazione richiesta,

che verrà effettuata solo in caso di urgenza o se disposta dalla Pubblica Autorità ed i Suoi dati verranno conservati solo per il tempo previsto dalla legge.

In caso di prenotazione di visita attraverso il sistema CUP o di altra occasione di contatto con le suddette Aziende/Enti, oltre ai sopra citati dati personali, Le potrà essere richiesto anche un numero di telefono personale, fisso o cellulare, ed un indirizzo e-mail che potranno essere utilizzati, fino a Sua diversa indicazione, per confermarLe o ricordarLe il giorno della prenotazione o per avvisarLa in caso di annullamento della visita o per finalità di prevenzione e di tutela di sanità collettiva e igiene pubblica. 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.

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

Al fine di evitare ripetute richieste del "consenso privacy" per ogni singola prestazione sanitaria ed in conformità a quanto legislativamente previsto, potrà manifestare il Suo consenso con un'unica dichiarazione. Si evidenzia che tale consenso sarà valido ed efficace fino a revoca dello stesso e, per i minorenni, fino al compimento del 18° anno. La revoca del consenso può avvenire in qualsiasi momento, compilando il relativo modulo e consegnandolo ad 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 di persona sotto tutela possono prestare il consenso o revocarlo solo i soggetti che esercitano la potestà legale.

I dati da Lei rilasciati all'Azienda/Ente potranno essere utilizzati sia in modo manuale che informatizzato dal personale debitamente autorizzato al trattamento dei dati, in qualità di responsabile o di incaricato del 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 di cui sopra.

I Suoi dati, inclusi quelli relativi alla Sua storia clinica, potranno inoltre essere comunicati, quando ciò risulti utile in relazione all'erogazione della prestazione o allo svolgimento dei compiti istituzionali attribuiti all'Azienda a medici convenzionati, strutture convenzionate, altre Aziende Sanitarie ed Ospedaliere, farmacie convenzionate, altri soggetti pubblici e privati, nei casi consentiti dalla normativa vigente oppure su Sua specifica richiesta o indicazione.

I suoi dati trattati con strumenti elettronici sono trasmessi ai soggetti di cui al paragrafo precedente attraverso reti telematiche e sistemi informatizzati. Ogni operazione su tali dati avviene con un livello di sicurezza elevato. In particolare, sono adottate tutte le misure di protezione indicate nella normativa sulla protezione dei dati personali. L'accesso viene garantito per moduli di dati in modo da selezionare le informazioni accessibili in funzione del settore di specializzazione e del livello di consenso singolarmente prestato.

Lee aziende/Enti si riservano, inoltre, di effettuare le necessarie comunicazioni di detti dati agli enti competenti, ai sensi di legge o di regolamento.

In ogni momento potranno essere esercitati i diritti di cui all'art. 7 del D. Lgs. 196/2003 e s.m.i. che riconosce tra gli altri il diritto al soggetto interessato di poter accedere ai propri dati personali, di

chiederne l'aggiornamento, la rettifica ovvero l'integrazione, la cancellazione-trasformazione in forma anonima ed il blocco dei dati se trattati in violazione di legge.

Il titolare del trattamento sono i seguenti:

- A.S.L. 1 "Imperiese", con sede in Via Aurelia Ponente, 97 – 18038 Bussana di Sanremo (IM);
- A.S.L. 2 "Savonese", con sede in Via Manzoni, 14 – 17100 Savona (SV);
- A.S.L. 3 "Genovese", con sede in Via Bertani, 4 – 16125 Genova (GE);
- A.S.L.4 "Chiavarese" con sede in Via G.B. Ghio, 9 – 16143 Chiavari (GE);
- A.S.L.5 "Spezzino" con sede in Via XXIV Maggio, 139 – 19124 La Spezia (SP);
- IRCCS AOU San Martino-IST, con sede in Largo R. Benzi 10 – 16132 Genova;
- 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).

ALLEGATO N: Scheda riassuntiva deliberazioni – determinazioni – atti dispositivi

SCHEDA RIASSUNTIVA DELIBERAZIONI-DETERMINAZIONI-ATTI DISPOSITIVI
○ **DELIBERAZIONE** ○ **DETERMINAZIONE DIRIGENZIALE** ○ **ATTO DISPOSITIVO DEL COMMISSARIO LIQUIDATORE**
NUMERO
DATA
STRUTTURA:
TIPOLOGIA:
OGGETTO:
SPESA: €..... Per il periodo
NOTE

Allegato O: informativa trattamento dati tramite dossier sanitario

Egr. Sig./Sig.ra

al fine di migliorare i processi di prevenzione, diagnosi, cura e riabilitazione che La riguardano, l'Azienda Sanitaria Locale 3 Genovese ha la possibilità di costituire il Suo Dossier Sanitario Elettronico, uno strumento che raccoglie in formato digitale i dati e i documenti clinici relativi alle prestazioni sanitarie che Le vengono erogate, allo scopo di documentarne la Sua storia clinico-sanitaria.

Tale strumento, può essere consultato, integrato o modificato, e pertanto reso accessibile, da tutti i professionisti sanitari che di volta in volta La prenderanno in cura all'interno dell'Azienda Sanitaria Locale 3 Genovese, 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 Dossier Sanitario Elettronico, 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 e nel rispetto dell'autorizzazione generale dell'Autorità garante per la protezione dei dati personale n. 2/2014.

La costituzione del Dossier Sanitario Elettronico è facoltativa e libera: pertanto qualora ritenesse di voler attivare il suo Dossier, è necessario che rilasci uno specifico consenso.
Il Dossier Sanitario Elettronico sarà alimentato dalle informazioni di salute che La riguardano, generate presso l'Azienda Sanitaria Locale 3 Genovese.
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 Dossier Sanitario Elettronico 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 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 presso gli Uffici Relazioni con il Pubblico e sul sito internet della ASL 3 Genovese (www.asl3.liguria.it) anche successivamente all'avvenuta produzione della documentazione clinico-sanitaria,. L'Azienda Sanitaria Locale 3 Genovese 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 correlate 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.

Tale documentazione sanitaria sarà inserita nel Dossier Sanitario Elettronico solo su Sua specifica richiesta.

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, i Suoi dati rimarranno comunque accessibili ai soli professionisti sanitari che li hanno generati e prodotti durante il percorso di cura.
Relativamente al Dossier Sanitario Elettronico La informiamo inoltre che lo specifico trattamento dei dati personali,verrà effettuato in modalità anche automatizzata esclusivamente da parte del personale espressamente autorizzato ai sensi degli articoli 29 e 30 del d.lgs. n. 196/2003, individuato come Responsabile del trattamento, Incaricato del trattamento e 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.

In ogni momento potranno essere esercitati i diritti di cui all'art. 7 del D. Lgs. 196/2003 e s.m.i. che riconosce tra gli altri il diritto al soggetto interessato di poter accedere ai propri dati personali, di chiederne l'aggiornamento, la rettifica ovvero l'integrazione, la cancellazione-trasformazione in forma anonima ed il blocco dei dati se trattati in violazione di legge.

Il titolare del trattamento è l'Azienda Sanitaria Locale 3 "Genovese", con sede in Via Bertani 4 – 16125 Genova.

Allegato P: modello consenso costituzione dossier sanitario

RACCOLTA CONSENSO AL TRATTAMENTO DEI DATI EFFETTUATI TRAMITE DOSSIER SANITARIO ELETTRONICO

Il/La sottoscritto/a (1) _____ _____ _____ _____ _____

nato/a a_ _____ _____ _____ _____ _____ _(_____)

il___ _____ , C.F._____ _____ _____ _____ _____

in nome proprio

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

_____ _____ _____ _____ _____ _____ _____

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 Sanitaria Locale 3 Genovese

☐ 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 presso gli uffici U.R.P. e sul sito internet della ASL 3 "Genovese"

Genova, _ /___/___

Firma dell'interessato

.....

_____ _____ _____ _____ _____ _____ _____ _____ _____

1 A cura dell'operatore incaricato:

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

Rilasciata da .....il.....

Firma dell'operatore incaricato

Allegato Q: modello richiesta oscuramento evento clinico

RICHIESTA DI OSCURAMENTO DI EVENTO CLINICO SUL DOSSIER SANITARIO ELETTRONICO

Il/La sottoscritto/a (1) _____

nato/a a_____ _____ _____(_____)

il_____ _____, C.F._____ _____ _____

in nome proprio

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

_____ _____ _____ _____

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 Sanitaria Locale 3 Genovese di poterlo visionare per una migliore cura.

Genova, __/__/__

Firma dell'interessato

.....

1 A cura dell'operatore incaricato:

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

Rilasciata da .....il.....

Firma dell'operatore incaricato

Allegato R: nomina incaricato trattamento dati tramite dossier sanitario

Struttura .....
Direttore.....
Tel. 010 .....
Fax 010 .....
e-mail.....

Genova, ...

Prot.n. /

Al Sig.

NOMINA AD INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI EFFETTUATI TRAMITE DOSSIER SANITARIO ELETTRONICO

ai sensi dell'art. 30 Del Decreto Legislativo N° 196 del 30/06/2003 e delle linee guida in materia di dossier sanitario (all. A alla deliberazione del garante del 04/06/2015)

Il sottoscritto Dott. ..... Direttore della Struttura..... Responsabile del trattamento dei dati personali ai sensi dell'art. 29 del decreto legislativo 196/03 e s.m.i., con il presente atto **nomina la S.V. "incaricato del trattamento dei dati personali"**, ai sensi del decreto legislativo 196/03 e s.m.i., con riferimento ai trattamenti effettuati tramite Dossier Sanitario Elettronico, svolti per finalità di prevenzione, diagnosi, cura e riabilitazione degli interessati, nell'ambito delle funzioni e competenze cui è preposto.

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 _____ (specificare operazione di trattamento)	SI ☐	NO ☐

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 incaricata di trattare i dati personali e sensibili strettamente necessari allo svolgimento delle mansioni assegnate e a rispettare e le misure di sicurezza predisposte dal titolare del trattamento dei dati e alla puntuale adozione delle istruzioni impartite dal sottoscritto 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 e/o del Responsabile.

Per ogni altra misura si rinvia alle disposizioni di cui al succitato decreto, alle linee guida dell'autorità garante per la protezione dei dati personali in materia di dossier sanitario e al Documento Programmatico sulla Sicurezza (entrambi pubblicati sulla rete Intranet Aziendale nella sezione normativa/privacy) nonché alle istruzioni operative fornite.

Il Responsabile del Trattamento
Dott.....
Direttore .....