AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA

Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it

asoalessandria@pec.ospedale.al.it (solo certificata)

C.F. – P.I. 01640560064

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI DELL'AZIENDA OSPEDALIERA SS.ANTONIO E BIAGIO E CESARE ARRIGO DI ALESSANDRIA

Sommario

Art. 1 Oggetto e finalità

1. Il presente Regolamento disciplina, nell'ambito dell'Azienda Ospedaliera SS. Antonio e Biagio e Cesare Arrigo di Alessandria (di seguito Azienda) le modalità di attuazione delle disposizioni contenute nel Codice in materia di protezione dei dati personali, approvato con D.Lgs. 30 giugno 2003 n.196, come modificato dal D.Lgs. 10 agosto 2018 n.101, (di seguito Codice Privacy) e nel Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, (di seguito GDPR), allo scopo di garantire che il trattamento dei dati riguardanti persone fisiche o giuridiche, acquisiti dall'Azienda o ad essa resi dagli interessati o da terzi, ivi comprese altre Amministrazioni Pubbliche, avvenga nel rispetto dei principi stabiliti dalla vigente normativa e nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza ed all'identità personale degli interessati.

2. L'Azienda assicura l'adozione di misure di sicurezza, anche preventive, idonee ad evitare pericoli di accesso abusivo, di trattamento illecito, nonchè di perdita o distruzione anche accidentale dei dati posseduti. L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli artt. 12 e seguenti del GDPR e procede all'individuazione della tipologia di dati trattati e delle relative operazioni eseguibili, per il conseguimento delle finalità di rilevante interesse pubblico rientranti nei compiti istituzionali dell'Azienda medesima.

3. La sicurezza dei dati personali e la loro tutela è costante principio informatore del sistema di qualità aziendale con i relativi strumenti (procedure, istruzioni operative, modelli, verifiche interne, audit).

4. Le disposizioni del presente Regolamento si applicano a tutti i dipendenti dell'Azienda ed a tutti coloro, anche non dipendenti (a mero titolo esemplificativo consulenti, incaricati, tirocinanti, specializzandi, borsisti, volontari, personale di ditte appaltatrici, fornitori), che, nell'ambito di attività autorizzate dall'Azienda stessa, effettuino trattamenti di dati personali, con particolare riferimento alle categorie di dati di cui agli artt. 9.1 e 10 del GDPR.

Art. 2 Definizioni

1. Ai fini del presente Regolamento si intendono:

a) per "*trattamento"*, qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, la conservazione, l'organizzazione, la strutturazione, l'adattamento o la modifica, l'uso, la consultazione, l'organizzazione, l'elaborazione, la modificazione, l'estrazione, il raffronto, l'interconnessione, la comunicazione, la diffusione, la cancellazione, la limitazione e la distruzione dei dati, anche se non contenuti in una banca dati;

b) per "*dato personale*", qualsiasi informazione che identifichi o renda identificabile anche indirettamente, una persona fisica, e che sia acquisita dall'Azienda o ad essa resa dagli interessati o da terzi, per lo

svolgimento di attività istituzionali, e trattata secondo quanto previsto dalla vigente normativa in materia di tutela dei dati personali;

c) per "*dati particolari*", i dati personali idonei a rivelare lo stato di salute e la vita sessuale o l'orientamento sessuale nonchè l'origine razziale ed etnica degli interessati, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale;

d) per "*dati giudiziari*", i dati personali idonei a rivelare provvedimenti adottati a carico degli interessati ed annotati nel casellario giudiziale o nell'anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, nonchè la qualità di imputato o indagato nell'ambito di procedimenti penali;

e) per "*titolare*", l'Azienda, in persona del suo legale rappresentante, cui competono tutte le decisioni in ordine alle finalità e alle modalità di trattamento dei dati ed alle misure di sicurezza da adottare;

f) per "*responsabile del trattamento*", la persona fisica o giuridica, esterna all'Azienda, individuata dal Titolare ai sensi dell'art.28 GDPR, per conto del quale effettui un trattamento, che presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato;

g) per "*delegato interno al trattamento*", ciascun Direttore di Struttura Complessa, ovvero ciascun Dirigente Responsabile di Struttura Semplice dipartimentale o di Struttura Semplice in staff alla Direzione Generale, ovvero ciascun Dirigente o soggetto espressamente individuato dal Titolare ai sensi dell'art.2-quaterdecies del Codice privacy, che, in ragione della funzione assegnata all'interno dell'organizzazione aziendale, svolge compiti di presidio e di governo delle attività di trattamento effettuate nell'ambito delle strutture dirette o a cui afferisce;

h) per "*Responsabile della Protezione dei Dati*" (di seguito RPD o DPO); la persona fisica interna o esterna all'Azienda designata dal Titolare con i compiti di cui all'art.39 GDPR;

i) per "*soggetto autorizzato al trattamento"*, ogni soggetto chiamato a svolgere operazioni di trattamento, secondo le istruzioni impartite dal Titolare o dal Delegato interno al trattamento, ai sensi dell'art. 29 del GDPR;

j) per "*amministratore di sistema*", la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning), le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali, ai sensi del Provvedimento del Garante del 27 novembre 2008;

k) per "*interessato*", la persona fisica identificata o identificabile, a cui si riferiscono i dati;

l) per "*strumenti elettronici*", qualunque strumento o dispositivo automatizzato che consenta il trattamento di dati;

m) per "*banche dati*", qualsiasi complesso organizzato di dati, raccolto in una o più unità cartacee o informatiche;

n) per "*misure di sicurezza*", il complesso delle misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio di cui all'art.32 GDPR, compatibilmente con lo stato dell'arte, i costi di attuazione, nonché con la natura, l'oggetto, il contesto e le finalità del trattamento;

o) per "*operazioni eseguibili"*, le differenti forme di trattamento realizzabili sulla tipologia di dati individuati dall'Azienda;

p) per "*rilevanti finalità di interesse pubblico*", le finalità individuate da qualunque disposizione di legge o di regolamento o da atti amministrativi generali o da provvedimenti del Garante, perseguite dall'Azienda nello svolgimento della sua attività istituzionale e rientranti nella "*mission aziendale*", che comportino il trattamento di dati.

2. Per ogni altra definizione non presente nel presente articolo, si rinvia alle definizioni contenute nell'art. 4 del GDPR.

Art. 3 Titolare del trattamento dei dati personali

1. Il Titolare del trattamento, ai sensi dell'art.24 del GDPR, è l'Azienda Ospedaliera di Alessandria nel suo complesso, in persona del suo legale rappresentante.

2. Il Titolare provvede a mettere in atto tutte le misure tecniche ed organizzative adeguate a garantire e a dimostrare la conformità dei trattamenti alle disposizioni vigenti.

3. Provvede inoltre:

a) a nominare i Responsabili del trattamento dei dati ed i Delegati interni al trattamento e ad impartire loro le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza;

b) alla formazione dei Delegati interni al trattamento e dei soggetti Autorizzati al trattamento dei dati attraverso la previsione di interventi formativi, al fine di renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare medesimo;

c) a nominare il Responsabile per la Protezione dei Dati;

d) ad ogni altro incombente espressamente previsto dalle vigenti disposizioni.

Art. 4 Contitolari del trattamento

1. Ai sensi dell'art.26 del GDPR, nell'ipotesi che l'Azienda effettui un trattamento in regime di contitolarità con altri soggetti, è necessario stipulare un accordo interno che indichi in modo trasparente nei confronti dell'interessato, gli obblighi e le responsabilità di ciascun Contitolare in merito all'osservanza del GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e i rispettivi ruoli nella comunicazione delle informazioni previste dagli artt. 13 e 14 del GDPR.

2. Ciascun Accordo di Contitolarità da stipulare secondo lo schema allegato al presente Regolamento (All.1), è soggetto al preventivo parere favorevole del DPO, che si avvale del supporto tecnico della SC ICT.

Art. 5 Responsabili del trattamento dei dati personali

1. I Responsabili del trattamento dei dati personali vengono nominati dal Titolare per iscritto e sono individuati tra soggetti esterni che forniscano sufficienti garanzie circa il rispetto delle disposizioni vigenti in materia di privacy, da richiedere quale requisito di partecipazione alla procedura di gara, o comunque da verificare preliminarmente a cura della SC ICT (ad es. adesione a codici deontologici ovvero a schemi di certificazione, esibizione di procedure interne di gestione dei dati quali DPIA o documento di verifica della compliance al GDPR).

2. I rapporti con i Responsabili del trattamento sono disciplinati da un contratto o altro atto giuridico (All.2) che vincoli il responsabile del trattamento:

a) ad effettuare il trattamento solo su istruzione documentata dal titolare;

b) a garantire che le persone autorizzate al trattamento si sono impegnate alla riservatezza anche come obbligo legale;

c) a dichiarare di aver adottato le misure tecniche e organizzative per garantire un livello di sicurezza adeguato rispetto ai rischi che corrono i dati e che derivano da distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o trattati;

d) a dichiarare di rispettare le condizioni della responsability chain, (o catena dei responsabili) e conseguentemente a nominare un sub-responsabile, solo previa informazione e consenso del titolare;

e) a definire le modalità attraverso le quali un interessato esercita i suoi diritti;

f) ad assistere il titolare in caso di violazioni sul trattamento;

g) a cancellare i dati e a restituire le informazioni ricevute al termine del trattamento;

h) a mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi.

3. I Responsabili esterni sono soggetti a verifiche periodiche da parte del DPO per valutare il rispetto delle indicazioni ricevute dal Titolare e la compliance al GDPR.

4. Per quanto concerne l'attività libero professionale *intramoenia* svolta presso studi privati autorizzati dall'Azienda, il Responsabile del trattamento dei dati è il singolo professionista.

Art. 6 Delegati interni al trattamento dei dati

1. I Delegati interni al trattamento dei dati personali provvedono all'organizzazione, alla gestione e alla supervisione di tutte le operazioni di trattamento dei dati personali gestiti nell'ambito della funzione ricoperta, nel pieno rispetto delle vigenti disposizioni in materia e delle istruzioni ricevute dal titolare al momento del conferimento dell'incarico secondo il modulo allegato al presente Regolamento (all.3).

2. I Delegati interni sono altresì competenti all'individuazione dei soggetti autorizzati al trattamento dei dati di cui all'art.7.

3. I Delegati interni non possono delegare la funzione (che non prevede alcuna remunerazione aggiuntiva) ad altro soggetto.

4. Con specifico riferimento agli studi sperimentali autorizzati e condotti all'interno dell'Azienda, il delegato interno al trattamento dei dati è espressamente individuato nello "sperimentatore principale" risultante dal protocollo di studi.

Art. 7 Soggetti autorizzati al trattamento

1. Le attività di trattamento sono effettuate dai soggetti "Autorizzati al trattamento dei dati" per le finalità strettamente connesse all'esecuzione della prestazione lavorativa.

2. Di norma, tutto il personale medico, sanitario, tecnico, professionale ed amministrativo operante presso ciascuna Struttura, ivi compreso il personale non dipendente (a mero titolo esemplificativo, personale in convenzione, liberi professionisti, studenti, specializzandi, tirocinanti, borsisti, volontari, interinali, personale di società in house) è individuato quale "autorizzato al trattamento", nei limiti delle rispettive attribuzioni.

3. I soggetti autorizzati al trattamento sono raggruppati nelle seguenti classi omogenee**:**

   a) personale medico e sanitario, infermieri, tecnici sanitari e personale riabilitazione, autorizzato al trattamento dei dati particolari, (stato di salute, dati genetici, vita sessuale) dei pazienti/utenti;

   b) personale amministrativo, in servizio presso strutture sanitarie, autorizzati al trattamento dei dati particolari, (stato di salute, dati genetici, vita sessuale) dei pazienti/utenti (ad es. personale amministrativo di reparto, CUP);

c) personale amministrativo, tecnico e professionale che tratta dati particolari, (stato di salute, opinioni politiche, appartenenza sindacale, carichi pendenti e precedenti giudiziari) del personale o di terzi;

d) personale amministrativo, tecnico e professionale, che non tratta dati particolari e giudiziari;

4. La designazione dei soggetti autorizzati al trattamento viene effettuata ad opera del Titolare ovvero dei Delegati interni al trattamento di cui all'art.6 secondo il modello di autorizzazione al trattamento dei dati personali semplificato (come previsto dallo stesso Garante con Provvedimento del 19 giugno 2008), allegato al presente Regolamento, (all. 4), contenente le istruzioni generali rivolte ai soggetti autorizzati.

5. L'ambito di trattamento effettuato sia con, che senza strumenti elettronici, consentito ai singoli soggetti autorizzati, è definito in stretta relazione alla struttura di assegnazione, alla qualifica ricoperta ed ai compiti assegnati dal Delegato interno, e deve intendersi automaticamente modificato in occasione di spostamenti da una struttura all'altra, debitamente disposti e validati nel quadro delle procedure aziendali anche nell'ambito del medesimo Dipartimento, ovvero in occasione di mutamenti di mansioni e/o profili funzionali

6. Fermo restando l'obbligo del segreto d'ufficio e/o professionale che grava su tutti i dipendenti, è disposto in via generale che ogni trattamento dei dati effettuato da parte di ciascun autorizzato avvenga:

- secondo le indicazioni fornite dal Titolare ovvero dal Delegato interno al trattamento;
- in modo lecito e secondo correttezza, fermo restando in ogni caso il rispetto dei generali doveri attinenti il segreto d'ufficio e professionale;
- per gli scopi strettamente inerenti l'attività di competenza di ciascun incaricato;
- in modo tale da assicurarne esattezza, completezza, pertinenza e non eccedenza rispetto alle finalità per le quali sono stati raccolti o trattati;
- assicurando un'adeguata chiusura dei locali nei quali sono custoditi o trattati i dati personali, durante le pause di lavoro, o al di fuori del normale orario di servizio, e comunque curando di evitare la possibilità di accesso ai dati per i quali è in corso un trattamento da parte di soggetti non autorizzati, in caso di allontanamento anche temporaneo dalla postazione di lavoro;
- nel rispetto delle misure di sicurezza predisposte dall'Azienda ai fini della loro conservazione;
- nel rispetto delle norme del codice di comportamento aziendale nel tempo vigente dedicate al rispetto della normativa privacy.

Art. 8 Diritti dell'interessato

1. Ai sensi degli artt.12 e seguenti del GDPR, all'interessato sono riconosciuti i seguenti diritti:

a) di ricevere informazioni e comunicazioni in forma coincisa, trasparente ed intelligibile;

b) di ottenere la conferma, mediante accesso gratuito, dell'esistenza o meno di dati personali che lo riguardano;

c) di ottenere la rettifica dei dati personali inesatti;

d) di ottenere la cancellazione dei dati personali o la limitazione dei trattamenti, fatti salvi i casi in cui ciò non sia consentito da disposizioni di legge che impongano la loro conservazione integrale;

e) di opporsi al trattamento, fatti salvi i casi in cui il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico;

2. I diritti di cui al punto 1 possono essere esercitati dall'interessato, personalmente o tramite persone fisiche o associazioni alle quali abbia conferito delega o procura per iscritto, con richiesta scritta rivolta al DPO o all'Ufficio Relazioni con il Pubblico, il quale provvederà a dare riscontro al richiedente entro il termine massimo di 30 giorni, ed avvalendosi del supporto di un Dirigente medico, qualora la richiesta comporti la comunicazione di dati attinenti la salute dell'interessato.

3. I diritti di cui al punto 1 sono limitati nelle ipotesi contemplate dall'art.2 – undecies del Codice Privacy.

4. Nel caso di dati personali concernenti persone decedute, i diritti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

Art. 9 Informativa all'interessato

1. L'interessato, ai sensi dell'art.13 GDPR, deve essere preventivamente informato oralmente o per iscritto sui seguenti aspetti:

a) finalità e modalità con le quali verranno trattati i dati;

b) obbligatorietà o meno del conferimento dei dati;

c) conseguenze di un eventuale rifiuto a fornire i dati;

d) soggetti o categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione di dati medesimi;

e) diritti di cui agli artt.12 e seguenti del GDPR;

f) individuazione del Titolare, del Responsabile del Trattamento dei dati e del Responsabile della protezione dei dati;

2. L'informativa all'interessato viene data prima dell'erogazione della prestazione richiesta, e può essere resa anche tramite affissione di appositi avvisi nei locali di accesso all'utenza, è pubblicata sul sito istituzionale, o somministrata utilizzando apposito modello all'uopo adottato dall'Azienda. L'informativa nelle procedure concorsuali e di gara risulta inserita nei bandi relativi. L'informativa al personale dipendente, non dipendente

borsista, frequentatore, tirocinante viene resa utilizzando lo specifico modulo in uso presso la SC Area Politiche Risorse Umane.

Le attività di sperimentazione, ricerca, studio vengono effettuate rispettando le indicazioni del Comitato Etico e le specifiche normative al riguardo.

3. L'informativa può intervenire senza ritardo anche successivamente alla richiesta della prestazione, nei seguenti casi:

a) emergenza sanitaria o igiene pubblica, per la quale sia stata adottata un'ordinanza contingibile ed urgente da parte dell'autorità competente;

b) interventi urgenti ed indispensabili per la tutela della salute e dell'incolumità fisica dell'interessato, ovvero nei casi di impossibilità fisica o di incapacità di intendere e di volere dell'interessato, quando non siano presenti gli esercenti la patria potestà o altri prossimi congiunti;

c) ogniqualvolta l'efficacia e la tempestività della prestazione medica possano essere pregiudicate dall'acquisizione preventiva del consenso.

4. Si prescinde dal rilascio dell'informativa anche quando i dati siano trattati per lo svolgimento di attività ispettive e di controllo, di attività investigative difensive o per far valere o difendere un diritto in sede giudiziaria di terzi o dell'Azienda, ma comunque solo per il periodo strettamente necessario al perseguimento dei suddetti scopi.

5. L'informativa è estesa altresì alla costituzione ed alimentazione del dossier sanitario elettronico nel rispetto delle Linee Guida adottate dal Garante della Privacy il 4 giugno 2015, e può essere resa ed archiviata anche con modalità informatizzate.

Art. 10 Consenso al trattamento dei dati idonei a rivelare lo stato di salute

1. Il trattamento dei dati idonei a rivelare lo stato di salute è consentito nei casi di cui all'art.9 comma 2 e seguenti del GDPR, per le rilevanti finalità di interesse pubblico elencate all'art. 2-sexies del Codice Privacy e nel rispetto delle misure di garanzia di cui al successivo art. 2-septies.

2. Ove necessario, il consenso dell'interessato, ovvero di chi eserciti la patria potestà nel caso di soggetti minori, è raccolto utilizzando apposito modulo aziendale sottoscritto ed allegato alla cartella clinica, per prestazioni di ricovero, o alla restante documentazione sanitaria in caso di prestazioni ambulatoriali, o al fascicolo d'ufficio, in caso di procedimenti amministrativi. E' consentito all'Azienda di acquisire ed archiviare il consenso anche con modalità informatizzate.

3. Il consenso al trattamento dei dati idonei a rivelare lo stato di salute del personale dipendente viene acquisito, utilizzando lo specifico modulo in uso presso la SC Area Politiche Risorse Umane.

Art. 11 Principi generali per il trattamento dei dati personali

1. Il trattamento dei dati personali deve essere effettuato esclusivamente per lo svolgimento di compiti istituzionali, con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato e dei principi di indispensabilità, liceità, correttezza, esattezza, pertinenza, completezza e non eccedenza.

2. I dati personali sono raccolti, di norma, direttamente presso l'interessato, e devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in operazioni di trattamento in termini non incompatibili con tali scopi. Essi devono essere conservati e custoditi nel rispetto delle vigenti disposizioni impartite dall'Azienda, in modo da evitare ogni rischio di contraffazione, sottrazione, accesso non autorizzato, diffusione generalizzata, distruzione o perdita anche accidentale, trattamento non consentito o non conforme dei dati custoditi.

3. La comunicazione di dati personali a privati ed enti pubblici economici è ammessa solo in presenza di una espressa disposizione di legge o regolamentare che lo consenta, mentre la comunicazione ad altri enti pubblici, è ammessa anche in assenza della suddetta norma, quando ciò sia necessario per il perseguimento delle finalità istituzionali dell'ente richiedente.

4. Fermo restando che, ove possibile, le riunioni si svolgono in presenza, la proposizione, riproduzione, condivisione e registrazione delle riunioni in video conferenza avviene solo se debitamente autorizzata da un dirigente/responsabile in qualità di delegato al trattamento.

5. La conservazione dei dati avviene nel rispetto dei tempi previsti dalle norme di legge e regolamentari interne. La cancellazione e la distruzione dei dati alla fine del periodo di conservazione avviene secondo procedure interne e misure organizzative che ne determinino la completa anonimizzazione ed impossibilità di ricostruzione ovvero la distruzione di qualsiasi copia cartacea e informatica.

Art. 12 Ulteriori principi applicabili al trattamento dei dati particolari

1. Il trattamento dei dati particolari di cui agli artt.9 e 10 GDPR da parte dell'Azienda avviene solo in presenza di una espressa disposizione di legge che specifichi i tipi di dati trattati, le operazioni eseguibili e le finalità di rilevante pubblico interesse sottese al trattamento stesso.

2. Nell'ambito delle attività dell'Azienda le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili sono individuate nelle schede allegate al presente regolamento approvato con D.P.G.R. 4 luglio 2016 n.9.

3. I dati particolari di cui agli artt.9 e 10 GDPR tenuti in elenchi, registri o banche dati, anche senza l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o codici identificativi che li rendano intelligibili solo agli operatori autorizzati al trattamento, consentendo di risalire all'identità dell'interessato solo in caso di necessità, e sono conservati separatamente dagli altri dati personali trattati per la medesima finalità, ove ciò sia tecnicamente possibile. Analogamente, in ottemperanza ai principi di necessità, pertinenza e non eccedenza dei dati, la

pubblicazione all'Albo informatico delle deliberazioni contenenti dati particolari di cui agli artt.9 e 10 GDPR, deve avvenire adottando opportune misure che consentano di risalire all'identità dell'interessato solo in caso di necessità, (ad esempio, riportando solo le iniziali del nome e del cognome, ovvero codici numerici, ovvero riportati in allegati non costituenti parte integrante del provvedimento medesimo ecc.). In ogni caso, la pubblicazione deve avvenire nel rispetto delle disposizioni impartite dall'Autorità Garante in materia.

4. I dati particolari di cui agli artt.9 e 10 GDPR possono essere comunicati ad altri soggetti pubblici e/o privati nei seguenti casi:

a) quando la comunicazione è prevista da un'espressa norma di legge statale o regionale o da altra fonte equiparata;

b) quando la richiesta della comunicazione è avanzata da altro soggetto pubblico per il perseguimento di finalità che per legge o per il proprio ordinamento sono considerate di rilevante interesse pubblico; in tal caso il richiedente deve indicare, per iscritto, la finalità perseguita e la disposizione di legge o del proprio ordinamento che attribuisce alla medesima il carattere di rilevante interesse pubblico;

c) quando la richiesta è avanzata da un soggetto privato per far valere, innanzi all'Autorità giudiziaria (penale, civile, amministrativa), un proprio diritto di rango equiparabile a quello alla riservatezza dell'interessato, ovvero un diritto della personalità o altro diritto o libertà fondamentale ed inviolabile, purché siano dimostrabili l'esistenza di un procedimento in corso, ovvero la pertinenza, la non eccedenza e la necessità di conoscere i dati richiesti, ed il conseguente trattamento avvenga nel rispetto della vigente normativa in tema di privacy;

d) nel caso di ordine di esibizione e/o comunicazione dell'Autorità giudiziaria.

5. I dati idonei a rivelare lo stato di salute possono resi noti all'interessato solo con le seguenti modalità:

a) attraverso la consegna dei dati al medico di fiducia che, a sua volta, li renderà noti all'interessato;

b) attraverso una spiegazione orale o un giudizio scritto da parte di un medico della struttura operativa che ha reso la prestazione.

6. La documentazione sanitaria può essere ritirata anche da persona diversa dall'interessato, purché sulla base di una delega scritta da questi rilasciata su apposito modulo, previa identificazione del delegato e mediante consegna dei documenti in busta chiusa.

7. La comunicazione a terzi di dati idonei a rivelare lo stato di salute dell'interessato può avvenire solo per finalità di ricerca scientifica o di statistica ed in forma rigorosamente anonima. E' fatto divieto assoluto di diffusione dei dati idonei a rivelare lo stato di salute.

8. I dati genetici sono trattati esclusivamente all'interno di locali protetti accessibili ai soli soggetti autorizzati ad effettuare i trattamenti; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico avviene utilizzando appositi sistemi di cifratura.

9. La trasmissione di dati particolari a mezzo posta elettronica è consentita nel rispetto dei limiti previsti dalla vigente normativa, e fatto salvo il ricorso ad adeguate tecniche di cifratura dei dati con chiavi indisponibili ai riceventi.

Art. 13 Misure di sicurezza

1. I dati personali devono essere trattati nel rispetto delle disposizioni impartite e delle adeguate misure di sicurezza di natura tecnica ed organizzativa, volte ad assicurare la protezione degli archivi cartacei e di quelli elettronici, individuate ed attuate dall'Azienda, in relazione alle conoscenze tecniche possedute, alla natura dei dati, alle modalità del trattamento ed alle risorse economiche disponibili, al fine di prevenire o ridurre al minimo ogni rischio di distruzione, perdita anche accidentale, contraffazione, sottrazione, accesso non autorizzato, diffusione generalizzata, trattamento non consentito o non conforme dei dati custoditi.

Art. 14 Misure di sicurezza per trattamenti con strumenti elettronici

1. Il trattamento dei dati personali effettuato con strumenti elettronici avviene nel rispetto delle seguenti misure di sicurezza:

a) autenticazione informatica: l'accesso ai dati è consentito ai soggetti autorizzati al trattamento, che devono accedervi per motivi di servizio, attraverso l'attribuzione a ciascuno di un codice identificativo personale, associato ad una parola chiave riservata, conosciuta solamente dal medesimo operatore per l'utilizzazione dello strumento elettronico; ogni autorizzato deve soddisfare una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa abbia i requisiti per il possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico; l'autorizzato è responsabile della gestione delle proprie credenziali; tali credenziali non possono essere assegnate a soggetti diversi, neppure in tempi differenti, fatta eccezione per l'utenza di Amministratore di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso;

b) adozione di procedure di gestione delle credenziali di autenticazione, in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso allo strumento o di mancato utilizzo delle medesime per un periodo superiore a sei mesi; ad ogni operatore sono state impartite precise istruzioni per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, per custodire con la massima cura la parola chiave riservata e per provvedere autonomamente alla sua sostituzione ad intervalli non superiori a tre mesi, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico. La chiave di autenticazione personale dell'autorizzato può essere rilasciata ed utilizzata temporaneamente dall'Amministratore di Sistema per necessità contingenti, indispensabili ed indifferibili di assistenza al profilo del soggetto autorizzato, oppure per assicurare la sicurezza del sistema; al termine dell'intervento l'autorizzato deve essere informato e deve provvedere alla sostituzione della parola chiave

autorizzata. Tutti gli accessi di ciascun soggetto autorizzato sono tracciati attraverso specifici *log di sistema*;

c) previsione di un sistema di autorizzazione, attraverso l'attribuzione a ciascun soggetto autorizzato, di profili di autorizzazione differenziati in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento; ciascun profilo viene verificato ed aggiornato in base alla sussistenza delle condizioni del trattamento e alle esigenze specifiche di gestione e manutenzione;

d) strumenti di protezione della rete informatica da eventuali intrusioni, danneggiamenti o perdite di dati, tra cui firewall ed antivirus, nonché sistemi di monitoraggio delle vulnerabilità a livello di rete e infrastruttura che prevengano e vadano ad individuare eventuali difetti e punti di accesso ai dati non autorizzati;

e) adozione delle misure di backup dei dati trattati all'interno dell'azienda, per permettere il loro ripristino nel caso di perdita di dati, di danneggiamento o attacco malevolo dalla rete esterna;

f) previsione di tecniche di cifratura o pseudonimizzazione dei dati a livello database, affinché gli stessi siano resi intellegibili solo agli operatori autorizzati al trattamento;

2. Il data center aziendale è ubicato presso i locali della SC ICT, dotati di specifiche misure di sicurezza e di protezione, ed ai quali l'accesso è selezionato e consentito solo al personale autorizzato ed identificato, così come tutti gli armadi di rete che consento l'accesso alla rete interna aziendale;

3. Ogni volta che si renda necessario avvalersi di soggetti esterni per l'adozione di misure di sicurezza, il loro aggiornamento o l'assessment dello attuale stato di monitoraggio delle vulnerabilità, l'installatore deve rilasciare una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni di legge.

Art. 15 Misure di sicurezza per trattamenti effettuati senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici avviene nel rispetto delle seguenti misure di sicurezza:

a) previsione di un sistema di individuazione dell'ambito del trattamento consentito a ciascun autorizzato, soggetto a verifica periodica, almeno annuale;

b) adozione di procedure per la conservazione dei documenti in armadi o cassetti dotati di serratura o, in alternativa, collocati in locali protetti da sistemi di chiusura che ne consentano un accesso selezionato;

c) divieto di conservazione di documenti e fascicoli contenenti dati personali in spazi liberamente accessibili al pubblico (corridoi d'accesso, sale d'attesa ecc.);

d) conservazione delle chiavi di apertura di locali, armadi e cassetti in luogo sicuro.

2. Gli archivi cartacei contenenti documentazione sanitaria ed amministrativa sono custoditi in appositi locali ad accesso selezionato e dotati di specifiche misure di sicurezza e di protezione.

Art. 16 Violazione dei dati personali

1. L'Azienda si è dotata di apposita procedura aziendale (P29) alla quale si fa espresso rinvio per l'ipotesi in cui si verifichi una violazione dei dati personali (data breach) nel rispetto delle disposizioni di cui agli artt.33 e seguenti del GDPR.

Art. 17 Diritto di accesso a documenti amministrativi e accesso civico

1. L'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali di terzi è disciplinato dagli artt.59-60-92-93 del Codice Privacy.

Art. 18 Disposizione di rinvio

1. Per quanto non espressamente indicato nel presente Regolamento, si rinvia alla vigente normativa in materia di trattamento dei dati personali ed in particolare al D.Lgs. 30 giugno 2003 n.196, e s.m.i. al GDPR 679/2016, nonchè ai provvedimenti adottati dal Garante per la protezione dei dati personali ed ai provvedimenti adottati dall'Azienda Ospedaliera.

2. Il presente Regolamento sarà aggiornato a seguito di eventuali modificazioni alla vigente normativa in materia di trattamento dati personali.

ALLEGATO 1

SCHEMA ACCORDO DI CONTITOLARITÀ NEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 26 DEL REGOLAMENTO 2016/679 (GDPR)

TRA

L'Azienda Ospedaliera SS.Antonio e Biagio e Cesare Arrigo, con sede in Alessandria, Via Venezia 16, (di seguito ASO AL o "Contitolare del trattamento")in persona del Direttore Generale e legale rappresentante pro tempore ……..……

E

……. con sede a …… (di seguito …… o "Contitolare del trattamento") in persona di ……. ……..

congiuntamente denominate "Parti"

PREMESSO

- che le Parti hanno concluso un contratto, di cui il presente accordo costituisce un addendum, in virtù del quale [descrizione attività];

- che le attività oggetto del contratto di cui sopra implicano il trattamento dei dati personali, come definiti all'art. 4.1 del Regolamento (UE) 2016/679 (di seguito "GDPR");

- che ai sensi dell'art.26 del GDPR, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento;

- che i contitolari del trattamento devono determinare in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito agli obblighi e all'osservanza della normativa vigente in materia di trattamento di dati personali con particolare riguardo:

a) all'esercizio dei diritti dell'interessato;

b) alla definizione dei rispettivi compiti nella comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR agli interessati;

c) all'individuazione di un punto di contatto per i soggetti interessati al trattamento;

d) all'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche;

e) alla definizione delle rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR e dell'eventuale danno causato dal trattamento dei dati.

Tutto ciò premesso, le Parti convengono e stipulano quanto segue.

Art.1 Premesse

Le premesse costituiscono parte integrante ed inscindibile del presente accordo.

Art.2. Contitolarità del trattamento

I contitolari in epigrafe indicati, tenuto conto dei rispettivi ruoli e rapporti con gli interessati, si danno reciprocamente atto che:

a) quanto al titolare ASO AL, i trattamenti riguarderanno i dati di seguito elencati:

Categoria interessati	Dati personali	Dati ex art. 9 GDPR	Dati ex art. 10 GDPR
Pazienti/Utenti			
Dipendenti/Coll.esterni			
Fornitori			
Altro (specificare)			

ed avranno ad oggetto: [indicare quali trattamenti fra i seguenti: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma dimessa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione].

b) quanto al titolare …… i trattamenti riguarderanno i dati di seguito elencati:

Categoria interessati	Dati personali	Dati ex art. 9 GDPR	Dati ex art. 10 GDPR
Pazienti/Utenti			
Dipendenti/Coll.esterni			
Fornitori			
Altro (specificare)			

ed avranno ad oggetto: [indicare quali trattamenti fra i seguenti: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma dimessa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione].

Art.3 Obblighi delle parti

Le parti si obbligano reciprocamente al compimento delle seguenti attività:

a) garantire il compimento dei trattamenti definiti all'art.2 in ragione dei servizi compiuti a favore dell'altra parte per come elencati e definiti nel Contratto;

b) garantire che i trattamenti dei Dati personali in contitolarità vengano compiuti nel pieno rispetto della normativa sulla protezione dei dati personali;

c) predisporre l'informativa ex artt. 13 e 14 del GDPR, nella quale dovrà essere data evidenza della contitolarità e del Punto di contatto, provvedendo altresì alla sua somministrazione in favore degli interessati;

d) definire le modalità per la raccolta e la gestione dei consensi ai trattamenti dei dati personali, laddove necessari;

e) garantire agli interessati l'esercizio dei diritti di cui agli artt. 15-22 del GDPR, fornendo all'altra parte la necessaria collaborazione, ove necessario;

f) porre in essere le misure tecniche e organizzative ritenute più idonee, in ragione dell'evoluzione della tecnica e degli specifici trattamenti compiuti, ovvero intese a proteggere i dati personali da distruzione accidentale o illecita, da perdita accidentale, da alterazione, o da rivelazione e accesso non autorizzati che comprendono, tra le altre:

- la pseudonimizzazione e la cifratura dei dati personali;

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

- una procedura per verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.I Contitolari eseguiranno un monitoraggio periodico sul livello di sicurezza raggiunto, al fine di renderlo sempre adeguato al rischio;

g) designare i propri autorizzati che trattano i dati nel rispetto delle istruzioni e delle policy di sicurezza, dei relativi codici etici e dei codici di comportamento;

h) tenere aggiornato il Registro delle attività di trattamento ex art. 30 del GDPR;

i) comunicare all'altra parte tramite Posta Elettronica Certificata qualsiasi violazione dei dati personali ("Data Breach") immediatamente dopo esserne venuto a conoscenza, fornendo tutta la documentazione necessaria per consentire, ove necessario, di notificare la violazione all'Autorità di controllo, e fornendo reciproca collaborazione a fronte di un tale evento e per ogni altra necessità in ragione della quale si renda necessario il contatto con la stessa;

j) fornire reciproca collaborazione nella redazione della valutazione d'impatto sulla protezione dei dati personali ex art. 35 del GDPR, laddove necessaria.

Art.4 Responsabilità

Le Parti saranno responsabili in solido nei confronti dell'interessato per i danni a questo causati in conseguenza della violazione delle disposizioni vigenti ovvero delle clausole del presente contratto, fermo restando, nei rapporti

interni, che ciascun Contitolare potrà agire in via di regresso nei confronti dell'altro Contitolare effettivamente responsabile per le operazioni allo stesso direttamente imputabili in base al presente accordo.

Art.5 Diritti degli interessati

L'interessato può esercitare i propri diritti previsti dagli artt. 15-22 del GDPR nei confronti di e contro ciascun contitolare del trattamento.

Art.6 Legge applicabile

Le presenti clausole sono soggette alla legge italiana.

Il presente accordo, formato in duplice copia, e composto da xxx pagine, da sottoporsi a registrazione solo in caso d'uso, viene letto, firmato e sottoscritto come segue.

ALLEGATO 2

NOMINA A RESPONSABILE ESTERNO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART.28 DEL REGOLAMENTO 2016/679 (GDPR)

L'Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" di Alessandria, in persona del suo Direttore Generale (di seguito Azienda o Titolare), con sede legale in Via Venezia, 16 – 15121 Alessandria, in qualità di Titolare del trattamento ai sensi dell'art.24 del Regolamento Europeo 2016/679 (di seguito GDPR)

Premesso che:

a) …….. (di seguito …… o Responsabile), ha in essere con l'Azienda un contratto di …… (SPECIFICARE OGGETTO E INDICARE ESTREMI DEL PROVVEDIMENTO DI AFFIDAMENTO) con decorrenza dal …… al ……;
b) le attività oggetto del contratto comportano il trattamento di dati personali come definiti dall'art.4 n. 1) del GDPR dei quali è Titolare l'Azienda, e meglio elencati nell'Allegato 1;
c) l'art. 28 del GDPR attribuisce al Titolare del trattamento la facoltà di ricorrere ad un Responsabile che presenti, per esperienza, capacità ed affidabilità, garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza e garantisca la tutela dei diritti dell'interessato;
d) il Responsabile dichiara di possedere una competenza qualificata per garantire il rispetto delle disposizioni vigenti in materia di privacy, e l'attuazione degli obblighi derivanti dal presente contratto (SE POSSIBILE DOCUMENTARE ad es. adesione a codici deontologici ovvero a schemi di certificazione, ovvero esibizione di procedure interne di gestione dei dati quali DPIA o documento di verifica della compliance al GDPR o indicazione della pagina internet dove si possono reperire i documenti inerenti la privacy);
e) il Responsabile dichiara altresì di aver adottato e di impegnarsi a mantenere per tutta la durata del servizio le misure tecniche e organizzative per garantire un livello di sicurezza adeguato rispetto ai rischi che corrono i dati e che derivano da distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o trattati;
f) ai sensi dell'art. 28.3 del GDPR i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi ed i diritti del titolare del trattamento.

Tutto ciò premesso, l'Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" di Alessandria

NOMINA

ai sensi e per gli effetti dell'art.28 GDPR

…… con sede in …….. P.Iva…….. C.F. ……, in persona di ……..

Responsabile del trattamento dei dati personali derivanti dall'attività oggetto del contratto di cui in premessa.

Il Responsabile per quanto concerne il trattamento dei dati derivante dall'esecuzione del servizio in oggetto, dovrà attenersi alle disposizioni contenute nel GDPR 2016/679 e nel D.Lgs. n.196/2003 e ss.mm.ii. e a tutte le prescrizioni qui di seguito fornite dal Titolare e a quelle successive che il Titolare del trattamento, riterrà di dettare, senza oneri aggiuntivi per quest'ultimo.

Il Responsabile del trattamento dati, nei limiti della materia disciplinata, della durata del trattamento, della natura e della finalità del trattamento, del tipo di dati trattati e delle categorie di interessati esplicitati nel contratto/convenzione di cui in premessa nonché nel presente atto, deve:

trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali e per la sola durata del contratto stesso;

1) rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza, disponibilità e integrità dei dati trattati, ai sensi di quanto disposto dall'art 32 del GDPR. In particolare – in considerazione dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche, del rischio derivante da distruzione, perdita, modifica, divulgazione non autorizzata o accesso in modo accidentale o illegale a dati personali trattati, AMOS si impegna a mettere in atto le misure tecniche e organizzative previste dal D.Lgs. n. 82/2005 e ss.mm.ii, dalle norme AGID e dalle disposizioni normative e regolamentari in materia, nonché ad ottemperare a tutti i provvedimenti dell'European Data Protection Board (EDPB) e del Garante Privacy applicabili, in particolare quello relativo agli amministratori di sistema;
2) adottare politiche interne e attuare, per quanto di sua competenza, in relazione alla tipologia di prestazione/trattamento da eseguire, misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);
3) individuare e nominare per iscritto le persone fisiche autorizzate al trattamento dei dati, ai sensi dell'art. 29 del GDPR e dell'art. 2 quaterdecies del D.Lgs. 196/2003, fornendo loro le istruzioni operative specifiche alle quali devono attenersi nell'espletamento dell'attività di trattamento;
4) garantire la riservatezza dei trattamenti, anche vincolando alla riservatezza non solo per la durata del contratto, ma anche per tutto il tempo successivo, senza limiti temporali, le persone fisiche autorizzate al trattamento e impegnando loro e chiunque agisca sotto la responsabilità di AMOS e abbia accesso ai dati personali a non trattare tali dati se non per le finalità del trattamento e comunque dopo averli istruiti adeguatamente;
5) non ricorrere ad un altro responsabile (sub responsabile) senza previa autorizzazione scritta, specifica o generale del titolare del trattamento secondo quanto previsto dall'art. 28.2 del GDPR. Il sub-Responsabile del trattamento deve rispettare gli stessi obblighi ai quali è assoggettato il Responsabile AMOS. Spetta al Responsabile assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del GDPR. In caso di violazione

da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile del trattamento è interamente responsabile nei confronti del Titolare del trattamento di tali inadempimenti.

Il Titolare potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit, verifiche e ispezioni, anche avvalendosi di soggetti terzi. Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il sub-Responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare, quest'ultimo diffiderà il Responsabile a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine non superiore a 7 giorni lavorativi.

In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 c.c., l'Azienda potrà, in ragione della gravità della condotta del sub-Responsabile e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto con il Responsabile, salvo il risarcimento del danno.

In alternativa alle verifiche di cui sopra, il Titolare potrà richiedere al Responsabile di fornire annualmente, o comunque su sua richiesta, una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate da parte del sub-Responsabile autorizzato;

6) impegnarsi a non trasferire tutti (o alcuni) dati personali derivanti dall'attività oggetto del contratto verso un paese terzo o un'organizzazione internazionale, senza autorizzazione del Titolare e indicazione della base legale che legittima il trasferimento; l'eventuale trasferimento di dati personali verso un paese terzo (extra UE) o un'organizzazione internazionale è in ogni caso ammesso solo se conforme agli artt. 44 e ss. del GDPR specificando che dovranno essere garantite da parte di AMOS misure tecniche e organizzative adeguate al fine di proteggere i diritti dei terzi interessati, l'esistenza di meccanismi di trasferimento tracciati e la documentazione delle opportune misure di sicurezza messe in atto;

7) notificare al titolare del trattamento tramite pec all'indirizzo asoalessandria@pec.ospedale.al.it immediatamente e comunque entro il primo giorno lavorativo successivo, qualunque richiesta ricevuta inerente l'esercizio dei diritti degli interessati ai sensi degli artt. 15 e ss. del GDPR, evitando di rispondere alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare, al quale dovrà comunque prestare assistenza per consentirgli di evadere le richieste;

8) impegnarsi, su richiesta del Titolare, al termine della prestazione dei servizi oggetto del contratto, a: i) restituire al Titolare del trattamento i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione e, qualora richiesto, alla restituzione dei dati al Titolare unitamente a qualsiasi documento o mezzo contenente detti dati, ai sensi dell'art. 28 paragrafo g) del GDPR;

9) mettere a disposizione del Titolare del trattamento, nel rispetto del principio di rendicontazione (accountability), tutta la documentazione e/o certificazione riguardante le misure di sicurezza adottate necessaria per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire al Titolare - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, ispezioni e audit - previo congruo preavviso se eseguiti presso la sede

del Responsabile - circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali.

Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Responsabile agisca in modo difforme o contrario alle istruzioni fornite dal Titolare, quest'ultimo diffiderà il Responsabile ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 c.c., l'Azienda potrà, in ragione della gravità della condotta del Responsabile e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto, salvo il risarcimento del danno.

In alternativa alle verifiche di cui sopra, il Titolare potrà richiedere al Responsabile di fornire annualmente, o comunque su sua richiesta, una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate;

10) prestare tutta la necessaria collaborazione e disponibilità, per quanto di competenza, a fronte di richieste di informazioni, controlli ed accessi da parte del Garante, di altre pubbliche autorità competenti, avvisando contestualmente e senza ingiustificato ritardo il Titolare in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere, inoltre, per quanto di sua competenza, il Titolare nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del contratto in essere;
11) tenere ed aggiornare periodicamente un Registro delle attività di trattamento effettuate sotto la propria responsabilità ai sensi dell'art. 30 del GDPR e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, mettendo il predetto Registro a disposizione dell'Autorità e del Titolare, laddove ne venga fatta richiesta ai sensi dell'art. 30.4 del GDPR.
12) informare tempestivamente e, in ogni caso, senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni incidente di sicurezza, violazione o sospetta violazione di dati personali (c.d. data breach) tramite una formale comunicazione scritta a ciascuno dei seguenti indirizzi:

    asoalessandria@pec.ospedale.al.it

    dpo@ospedale.al.it (DPO dell'Azienda)

    Tale notifica da effettuarsi tramite il modulo allegato 2 al presente atto, è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali entro i termini previsti dal GDPR; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento si impegna a supportare il Titolare nell'ambito di tale attività.

    Il Responsabile deve mantenere un registro degli incidenti di sicurezza, anche qualora non vi siano violazioni, così come previsto dall'art. 33.5 del GDPR.

In ogni caso il Responsabile dovrà informare il DEC dell'Azienda per coordinare le azioni di mitigazione del rischio, contenimento dei danni, individuazione delle misure di sicurezza da adottare.

A seguito del verificarsi di detti incidenti il Titolare potrà fare attività di audit, anche senza preavviso e avvalendosi di soggetti terzi.

Nel caso in cui alla conclusione di tali verifiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate, Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" di Alessandria, per conto del Titolare, potrà:

- prescrivere ulteriori misure di sicurezza, anche apportando modifiche a quelle in essere, con particolare riferimento al presente accordo;
- far rispondere il Responsabile del trattamento del danno causato, fino alla risoluzione del contratto, a meno che il Responsabile stesso non dimostri che l'evento dannoso non gli sia in alcun modo imputabile;
- su eventuale richiesta del Titolare, assistere quest'ultimo, per quanto di competenza, nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE.
- comunicare tempestivamente al Titolare del trattamento dati eventuali variazioni che richiedano un adeguamento del presente atto di nomina;
- informare tempestivamente ed adeguatamente il Responsabile della Protezione dati (RPD o DPO) dell'Azienda per tutte le questioni riguardanti la protezione dei dati;

Ai sensi dell'art. 37 GDPR le parti indicano qui di seguito i recapiti dei rispettivi DPO o RPD):

per l'Azienda: Dr.ssa Silvia Straneo tel. 0131/206710 email dpo@ospedale.al.it

per il Responsabile:

……

Per tutte le controversie che dovessero sorgere con riferimento al presente Accordo sarà esclusivamente competente il Foro di Alessandria.

Il trattamento dei dati (finalità del trattamento, tipo di dati personali trattati, operazioni eseguite sui dati, categorie di interessati), in esecuzione del contratto principale suindicato, è specificato nell'allegato 1.

Letto, approvato e sottoscritto digitalmente

per l'Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" di Alessandria

_____

per ……

_____

Ai sensi e per gli effetti dell'art. 1341 c.c. il Responsabile dichiara di aver letto con attenzione e di approvare specificatamente le pattuizioni contenute negli articoli oggetto della presente Nomina e negli allegati.

Letto, approvato e sottoscritto digitalmente.

Allegato 1

SPECIFICHE DEI TRATTAMENTI DELEGATI AL RESPONSABILE

I trattamenti delegati al Responsabile da parte del Titolare sono i seguenti:

Trattamento	SPECIFICARE
Durata massima	▪ Sino al termine del periodo contrattuale ed eventuali ulteriori rinnovi come da specifiche di contratto.
Finalità	SPECIFICARE
Tipo di dati personali	▪ Dati personali e personali identificativi: (es: nome, cognome, CF, data e luogo di nascita, ecc….) ▪ Dati personali particolari relativi allo stato di salute
Categorie di interessati	▪ Pazienti ▪ Pazienti minori di età ▪ Dipendenti dell'Azienda ▪ Personale esterno autorizzato ad accedere al servizio ristorazione
Operazioni di trattamento	▪ Raccolta, registrazione, consultazione
Misure di sicurezza specifiche da adottare	Il Responsabile per il trattamento impiega: ▪ Istruzioni sulla gestione delle credenziali di autorizzazione e accesso ▪ Istruzione e formazione del personale ▪ SPECIFICARE ALTRE MISURE TECNICHE
Elenco dei Subresponsabili art. 28 par.4	▪ Non impiegati

Allegato 2

SCHEDA EVENTO DATA BREACH

SCHEDA EVENTO	
CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta);	
Data e ora in cui si è avuto conoscenza della violazione;	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA

Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it

asoalessandria@pec.ospedale.al.it (solo certificata)

C.F. – P.I. 01640560064

ALLEGATO 3

ISTRUZIONI OPERATIVE PER IL DELEGATO INTERNO AL TRATTAMENTO DEI DATI AI SENSI DEL D.LGS.N.196/2003 E SS.MM.II. E DEL GDPR 2016/679

Ai sensi dell'art.2-quaterdecies del D.Lgs. n.196/2003 e ss.mm.ii, (Codice della Privacy) il titolare può prevedere, nell'ambito della propria organizzazione, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.

Con deliberazione n. _ del sono stati individuati quali "Delegati interni al trattamento dei dati" i seguenti soggetti:

- Direttori di Struttura Complessa;
- Dirigenti Responsabili di Struttura Semplice dipartimentale;
- Dirigenti di Struttura Semplice in staff alla Direzione Generale;
- Dirigenti o altri soggetti espressamente individuati,

che, in ragione della funzione assegnata all'interno dell'organizzazione aziendale, svolgono compiti di presidio e di governo delle attività di trattamento dei dati effettuate nell'ambito delle strutture dirette o a cui afferiscono.

Il presente documento contiene le istruzioni operative per i Delegati Interni al trattamento dei dati personali dell'Azienda Ospedaliera "SS.Antonio e Biagio e Cesare Arrigo" di Alessandria (di seguito Azienda), in conformità al Codice della privacy ed al Regolamento UE 2016/679 (GDPR).

Avuto riguardo alle attività della Struttura diretta, ovvero alle attività assegnate nell'ambito della Struttura di appartenenza, il Delegato dovrà effettuare trattamenti di dati personali attenendosi scrupolosamente alle seguenti istruzioni ed in particolare dovrà:

a) individuare e nominare per iscritto i soggetti autorizzati al trattamento dei dati nell'ambito delle risorse di personale assegnate alla struttura e nel rispetto delle rispettive competenze;

b) curare la regolare tenuta e l'aggiornamento dell'elenco dei soggetti autorizzati;

c) fornire ai soggetti autorizzati le istruzioni operative specifiche alle quali i medesimi devono attenersi nell'espletamento dell'attività di trattamento ad essi attribuita, utilizzando la specifica modulistica disponibile sulla Intranet aziendale - Sezione "Assicurazioni e privacy" e verificarne il rispetto, unitamente alle misure di sicurezza generali adottate dal titolare;

d) verificare la sussistenza dei presupposti per il rilascio ed il mantenimento di adeguati profili di autenticazione in capo agli autorizzati, in relazione ai trattamenti ad essi riservati;

e) collaborare con il DPO aziendale, fornendo tutte le informazioni richieste, e segnalando tempestivamente tutte le questioni rilevanti ai fini del rispetto delle disposizioni vigenti;

f) effettuare il censimento dei dati trattati e delle banche dati esistenti presso la propria Struttura;

g) prendere nota dell'inizio di ogni nuovo trattamento, nonché della cessazione o della modifica dei trattamenti già in essere all'interno del proprio settore di competenza, ai fini dell'aggiornamento del registro dei trattamenti di cui all'art.30 del GDPR;

h) verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa, adottando ogni iniziativa per evitare che i dati risultanti eccedenti o non pertinenti o non necessari a seguito delle verifiche, non siano più utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene;

i) informare tempestivamente il Titolare e il DPO su qualsiasi evento che possa compromettere il corretto trattamento e la sicurezza dei dati (anomalie, furti, perdite accidentali o distruzioni dei dati) al fine di attivare, nel caso sia riscontrato un rischio per i diritti e le libertà delle persone fisiche, la specifica procedura aziendale (P29) per l'ipotesi di Data Breach;

j) collaborare con il Titolare e con il DPO nell'espletamento dell'attività di valutazione di impatto, ai sensi dell'art. 35 del GDPR;

k) verificare che ai soggetti interessati vengano fornite le informazioni di cui agli artt. 13 e 14 del GDPR;

l) adottare, previo parere favorevole del DPO aziendale, specifici moduli di consenso al trattamento dei dati, nel caso di trattamenti ulteriori rispetto a quelli per i quali è in uso il modulo aziendale (ad es. sperimentazioni, telemedicina …);

m) partecipare direttamente e favorire la partecipazione dei soggetti autorizzati alle iniziative formative organizzate dall'Azienda sul tema della protezione dei dati;

n) concorrere a favorire la diffusione tra i propri collaboratori di una cultura ispirata al trattamento dei dati personali nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona;

o) provvedere all'espletamento di ogni altra operazione necessaria per il rispetto e la corretta applicazione della normativa europea e nazionale vigente in materia di Privacy.

Il Delegato interno non può delegare la funzione (che non prevede alcuna remunerazione aggiuntiva) ad altro soggetto.

Data_____

Firma _____ (per presa visione e accettazione)

AO AL Azienda Ospedaliera di ALESSANDRIA Santi Antonio e Biagio e Cesare Arrigo

Via Venezia, 16 – 15121 ALESSANDRIA

Tel . 0131 206111 – www.ospedale.al.it
info@ospedale.al.it

asoalessandria@pec.ospedale.al.it (solo certificata)

C.F. – P.I. 01640560064

ALLEGATO 4

AUTORIZZAZIONE SEMPLIFICATA AL TRATTAMENTO DEI DATI AI SENSI DEL D.LGS.N.196/2003 E SS.MM.II. E DEL GDPR 2016/679

Il/La sottoscritto/a _____

Direttore/Responsabile della Struttura_____

in qualità di Delegato al Trattamento dei dati:

AUTORIZZA

ai sensi dell'art. 29 del Regolamento Europeo n. 2016/679 (GDPR)

i soggetti sotto riportati in servizio e/o preposti ad attività presso la struttura/ufficio, al trattamento dei dati, effettuati sia con strumenti elettronici sia senza strumenti elettronici, per le finalità strettamente pertinenti all'esecuzione della prestazione lavorativa.

L'autorizzazione comprende tutte le operazioni di trattamento dei dati[1] (personali, relativi alla salute, alla vita sessuale, genetici, biometrici, giudiziari) che siano strettamente necessarie per adempiere ai compiti assegnati in relazione alle attività svolte nell'ambito della struttura di appartenenza, compresa l'attività svolta in regime di libera professione intramuraria e intramuraria "allargata", e di quant'altro definito di volta in volta ed in modo specifico dal Titolare o dal Delegato al trattamento.

Per completezza di analisi, si riportano gli ambiti di trattamenti di dati puntualmente individuati consentiti agli autorizzati al trattamento.

1 **Ai sensi dell'art. 4 del Regolamento Generale sulla protezione dei dati**, costituisce trattamento dei dati: "qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto, o l'interconnessione, la limitazione, la cancellazione o la distruzione;"

NOMINATIVO	SETTORE	TRATTAMENTO (ambito del trattamento, descrizione operazioni, banche dati)

I Soggetti autorizzati, individualmente menzionati nel predetto elenco, da aggiornarsi periodicamente, operano sotto la diretta autorità del Delegato al trattamento e sono tenuti al rigoroso rispetto dei principi del Regolamento Privacy Europeo, della normativa nazionale e delle disposizioni aziendali emanate in materia (regolamenti, procedure aziendali, circolari interne, ordini di servizio etc.) nonché delle seguenti istruzioni di carattere generale:

- trattare i dati in modo lecito e corretto;
- trattare i dati relativi allo stato di salute ed alla vita sessuale, alle convinzioni religiose, e politiche, i dati genetici, i dati giudiziari contenuti in elenchi, registri o banche di dati tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, ove possibile, con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi, che permettano di identificare gli interessati solo in caso di necessità;
- raccogliere e registrare i dati unicamente per gli scopi inerenti l'attività svolta;
- verificare ove possibile, che siano esatti e, se necessario, aggiornarli;
- verificare che i dati 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 Delegato;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Titolare o del Delegato;
- evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del Delegato del trattamento;
- adottare credenziali di autenticazione alla rete aziendale che forniscano sufficienti garanzie di sicurezza, mantenerle assolutamente riservate e provvedere periodicamente alla loro modifica;
- mantenere la massima riservatezza sui dati trattati;
- non comunicare a terzi o diffondere, con o senza strumenti elettronici, le notizie, le

informazioni o i dati appresi in relazione a fatti e circostanze di cui sia venuto a conoscenza nella propria qualità di soggetto autorizzato;

- non comunicare e diffondere i dati personali provenienti da banche dati aziendali, in assenza dell'autorizzazione del Titolare o del Delegato del trattamento;
- richiedere preventivamente l'autorizzazione al Delegato ogni qualvolta si renda necessaria la comunicazione all'esterno dei dati oggetto del trattamento;
- assicurare che ogni attività di trattamento avvenga con la massima cautela e diligenza, anche durante le pause di lavoro, o al di fuori del normale orario di servizio, in modo da evitare indebite acquisizioni di notizie ed informazioni da parte di soggetti estranei o non autorizzati;
- osservare tutte le misure di protezione e sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali, attenendosi inoltre, nel trattamento dei dati con o senza l'ausilio di strumenti elettronici, alle ulteriori particolareggiate istruzioni a tal fine impartite dal Delegato;
- passare le consegne in modo preciso e dettagliato nel caso di trasferimento dell'attività svolta da altro soggetto;
- informare il Delegato ed il DPO qualora si verifichi qualsiasi evento che possa compromettere la sicurezza dei dati personali: (anomalie, furti, perdite accidentali di dati) al fine di attivare, nel caso sia riscontrato un rischio grave per i diritti e le libertà delle persone fisiche, la procedura aziendale del Data Breach;
- rispettare le disposizioni contenute nel Codice di Comportamento Aziendale.

Si precisa che gli obblighi sopra descritti rientrano nell'ambito della prestazione lavorativa e non comportano alcuna modifica della qualifica professionale o delle mansioni assegnate e sono dovuti senza alcuna remunerazione aggiuntiva. La violazione delle presenti istruzioni può comportare l'applicazione di sanzioni disciplinari.

La presente nomina sarà resa nota agli interessati a mezzo (e-mail, raccolta firme, ecc…), viene affissa nella bacheca della struttura e conservata agli atti della medesima.

Data,

IL DELEGATO INTERNO

AL TRATTAMENTO DEI DATI PERSONALI

_____