ATTO DI DESIGNAZIONE A

RESPONSABILE AL TRATTAMENTO DEI DATI PERSONALI

Art. 28, Regolamento (UE) 2016/679

Considerato che:

- con provvedimento del Direttore dell' U.O./Servizio …… n. …….. del ……., a seguito di (es. : gara a procedura ristretta, ecc.), tra l'IRCCS Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" – IRST S.r.l. (in seguito IRST) e la Ditta/Società …… è stato stipulato/prorogato/ rinnovato/ecc. il contratto/convenzione relativo a ……..……..;
- nella esecuzione del suddetto rapporto contrattuale/convenzionale e nel compimento degli atti conseguenti, la suddetta Ditta/Società compie necessariamente operazioni di trattamento di dati personali per conto dell'IRST, Titolare del trattamento;
- l'ambito del trattamento e i dati che ne sono oggetto sono meglio specificati nell'**Allegato 1** "Ambito del trattamento", parte integrante del presente Atto;
- Il Regolamento Generale (UE) 2016/679 sulla protezione dei dati personali (di seguito GDPR o Regolamento) definitivamente applicabile in Italia dal 25.05.2018, dispone che qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che garantiscono la adozione di misure tecniche ed organizzative adeguate, in modo che il trattamento sia conforme alla normativa in materia di protezione dei dati e garantisca la tutela dei diritti dell'interessato;
- il presente atto di nomina costituisce parte integrante del contratto/convenzione sopracitato stipulato/prorogato/rinnovato/ ecc. fra l'IRST e la Ditta/Società _____

Tutto ciò premesso, al fine di provvedere alla corretta gestione degli adempimenti previsti dal GDPR,

tra

L'IRST con sede in Meldola Via Piero Maroncelli, 40 codice fiscale/P.I. 03154520401 in persona del Direttore Generale (nel seguito Titolare)

e

La Ditta/Società con sede in _____ Via _____ codice fiscale /P.I. _____ in personale del legale rappresentante _____ (nel seguito Responsabile del trattamento)

si conviene e si stipula quanto segue

1. **Nomina del Responsabile del trattamento**

Con il presente Atto si nomina la Ditta/Società…… Responsabile del trattamento dei dati personali, per quanto sia necessario alla corretta esecuzione del rapporto contrattuale/convenzionale indicato in premessa.

2. **Obblighi e compiti del Responsabile del trattamento**

La Ditta/Società …..... Responsabile del trattamento, tratta dati personali per conto del Titolare del trattamento solo ed esclusivamente ai fini della esecuzione dei servizi oggetto del contratto/convenzione, nel rispetto della normativa vigente in materia di protezione dei dati personali, nonché delle istruzioni impartite dal Titolare nel presente Atto o in atti successivi.

Ogni trattamento di dati personali da parte del Responsabile del trattamento deve avvenire nel rispetto dei principi, dei limiti e delle modalità di cui all'art. 5 del GDPR.

Il Responsabile del trattamento, operando nell'ambito dei suddetti principi, **deve attenersi ai seguenti compiti**, con riferimento rispettivamente a:

- ***persone preposte allo svolgimento di operazioni di trattamento sui dati personali:***
    - sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, **designa** espressamente e per iscritto i dipendenti e i collaboratori autorizzati/incaricati allo svolgimento di operazioni di trattamento sui dati personali oggetto del contratto, attribuendo loro specifici compiti e funzioni ed impartendo adeguate informazioni ed istruzioni;
    - al fine di garantire un trattamento corretto, lecito e sicuro **si adopera** per rendere effettive le suddette istruzioni, curando la formazione di tali soggetti - sia in tema di protezione dei dati personali che, ove occorra, di sicurezza informatica - vigilando sul loro operato, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento delle loro attività, anche **successivamente alla cessazione del rapporto di lavoro/collaborazione con la Ditta/Società stessa;**
    - comunica al Titolare del trattamento, su specifica richiesta l'elenco aggiornato dei dipendenti/collaboratori autorizzati al trattamento, nonché qualsiasi variazione dei profili autorizzativi concessi a tali persone per motivi di sicurezza;

- ***registro delle attività di trattamento:***
    - ove ne sia tenuto, **identifica e censisce** i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività oggetto del contratto/convenzione al fine di predisporre il registro delle attività di trattamento svolte per conto dell'IRST/Titolare da esibire in caso di ispezione dell'Autorità Garante e contenente almeno le seguenti informazioni:
        1. il nome e i dati di contatto del Responsabile, del Titolare del trattamento per conto del quale il Responsabile agisce e, ove applicabile, del Responsabile della protezione dei dati;
        2. le categorie dei trattamenti effettuati per conto del Titolare;
        3. se del caso, i trasferimenti di dati personali verso paesi terzi, compresa l'identificazione del paese terzo e la relativa documentazione di garanzia;
        4. la descrizione generale delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;

- ***obblighi di sicurezza:***
  - **adotta** le misure tecniche e organizzative adeguate per proteggere la sicurezza, la riservatezza e l'integrità dei dati personali tenendo conto dei rischi di varia probabilità e gravità (di distruzione o perdita, di modifica, di divulgazione non autorizzata o di accesso accidentale o illegale a dati trasmessi, conservati o comunque trattati), dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento;
  - **conserva** i dati personali garantendo la separazione di tipo logico dai dati personali trattati per conto di terze parti o per proprio conto;
  - **definisce** una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati; le modalità per garantire tali livelli di sicurezza dovranno essere comunicate al Titolare nel caso di esplicita richiesta;
  - **si impegna** ad utilizzare strumenti, applicazioni e/o servizi che rispettino i principi di protezione dei dati personali fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*);
  - **assicura** la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
  - **definisce** una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
  - ulteriori misure di sicurezza sono individuate in relazione allo specifico trattamento di dati da parte del fornitore.

- ***"Data Breach":***
  - **comunica** al Titolare del trattamento, senza ingiustificato ritardo dopo esserne venuto a conoscenza - e comunque entro 24 ore - qualsiasi evento che possa comportare una violazione, anche accidentale, dei dati personali oggetto di trattamento, fornendo tutte le informazioni disponibili sull'evento e prestando la necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità Garante e/o di comunicazione delle stesse agli interessati; a tal fine il Responsabile porrà in essere per quanto compatibile con il contesto e la natura della violazione, la procedura predisposta dal Titolare del trattamento che verrà successivamente messa a disposizione.

- ***valutazione di impatto:***
  - **fornisce** tutte le informazioni e tutti gli elementi utili al Titolare per la effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, nonché della eventuale consultazione preventiva all'Autorità Garante ai sensi degli artt. 35 e 36 del GDPR;

- ***amministratori di sistema (se necessario in base al fornitore che si sta nominando):***

  conformemente al Provvedimento dell'Autorità Garante del 27 novembre 2008 e s.i.m., in tema di amministratori di sistema, si impegna a:
  - **designare** quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;

- **predisporre** e **conservare** l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- **comunicare** periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema;
- **verificare** annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
- **mantenere** i file di log previsti in conformità a quanto previsto nel suddetto Provvedimento.

- ***istanze degli interessati:***

- **collaborare** con il Titolare per fornire tempestivamente tutte le informazioni necessarie e/o i documenti utili al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste degli interessati di cui al Capo III del GDPR (ad es.: esercizio dei diritti di accesso, rettifica, limitazione, opposizione al trattamento dei dati);
- **collaborare** con il Data Protection Officer (DPO) del Titolare del trattamento, provvedendo a fornire ogni informazione dal medesimo richiesta;
- qualora il trattamento dei dati personali oggetto della convenzione/contratto comporti la raccolta di dati personali da parte del Responsabile del trattamento, questi provvede al rilascio della relativa informativa ai soggetti interessati; inoltre, qualora tale raccolta di dati personali avvenga in luoghi ad accesso pubblico, il Responsabile esterno del trattamento provvede ad affiggere in tali luoghi i cartelli contenenti l'informativa, con la precisazione che l'informazione resa attraverso la cartellonistica integra, ma non sostituisce l'obbligo di informativa in forma orale o scritta.
- **provvedere ad informare** immediatamente il Titolare del trattamento di ogni richiesta, ordine ovvero attività di controllo da parte dell'Autorità Garante per la protezione dei dati personali o dell'Autorità Giudiziaria e coadiuvare il Titolare stesso nella difesa in caso di procedimenti dinanzi alle suddette Autorità che riguardino il trattamento dei dati oggetto della convenzione;

- ***Ulteriori obblighi:***

- **mettere a disposizione** del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente Atto di designazione e consentire al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto. Resta inteso che qualsiasi verifica condotta ai sensi del presente comma dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso;

si impegna, altresì, a:

- **effettuare** a richiesta del Titolare un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare stesso (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
- **collaborare**, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei Dati Personali;

- **realizzare** quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente Atto di designazione;
- **informare** prontamente il Titolare di ogni questione rilevante ai fini di legge; a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che il trattamento dei dati personali violi la normativa in materia di protezione dei dati personali o presenti comunque rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato o qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati oppure qualora il Responsabile del trattamento sia soggetto ad obblighi di legge che gli rendono illecito o impossibile agire secondo le istruzioni ricevute dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

Come sancito dal GDPR, qualora il Responsabile del trattamento determini autonomamente le finalità e i mezzi di trattamento in violazione del GDPR medesimo, sarà considerato Titolare del trattamento, assumendone i conseguenti oneri, rischi e responsabilità;

- ***Trasferimento di dati fuori dall'Area economica europea ("EEA")***

dichiara che non trasferisce e tratta dati personali fuori dall' Area economica europea.

OPPURE

qualora trasferisca e tratti dati personali fuori dall'Area economica europea, dichiara in un documento allegato che tale trasferimento avviene nel rispetto delle condizioni di cui agli artt. 44 e ss. del Regolamento, descrivedole (ad es.: decisione di adeguatezza, norme vincolanti d'impresa, clausole tipo...) .

Il documento costituirà parte integrante del presente Atto.

- ***Altri Responsabili (Sub–responsabili):***

- per l'esecuzione di specifiche attività di trattamento per conto del Titolare e solamente previa autorizzazione scritta, specifica o generale del titolare stesso, il Responsabile del trattamento può ricorrere ad altro responsabile (c.d. Sub-responsabile del trattamento); quando ciò avvenga il Responsabile del trattamento si obbliga ad imporre per iscritto a tale Sub-responsabile, mediante atto giuridico vincolante, gli stessi obblighi in materia di protezione dei dati personali cui è soggetto il Responsabile stesso, in particolare in relazione agli obblighi in materia di sicurezza. Nel caso in cui il Responsabile del trattamento ricorra a un Sub-responsabile stabilito in un Paese extra-UE, sarà suo onere adottare adeguati strumenti per legittimare il trasferimento ai sensi degli artt. 44 e ss. del Regolamento.

Il Titolare ha il diritto di chiedere al Responsabile del trattamento:

- il rilascio di copia degli accordi stipulati tra Responsabile e Sub-responsabile (omettendo le sole informazioni strettamente confidenziali e gli accordi economici, se del caso);
- di sottoporre ad audit i propri Sub-responsabili o comunque fornire conferma che tali audit siano stati condotti per dimostrare la conformità dei Sub-responsabili alla normativa in materia di protezione dei dati personali, nonché agli obblighi di cui al presente Atto.

Il Responsabile del trattamento si impegna espressamente ad informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di eventuali Sub-responsabili del trattamento, dandogli così l'opportunità di opporsi a tali

modifiche. Il Responsabile del trattamento non può ricorrere ai Sub-responsabili nei cui confronti il Titolare abbia manifestato la sua opposizione.
Qualora il Sub-responsabile ometta di adempiere ai propri obblighi, il Responsabile del trattamento conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'inadempimento degli obblighi del Sub-responsabile.

- ***responsabile della protezione dei dati:***

Il Responsabile del trattamento comunica al Titolare del trattamento il nome e i dati di contatto del proprio Responsabile della protezione dei dati, ove designato.

3. **Condizioni della nomina**

Chiunque subisca un danno materiale o immateriale causato da una violazione della normativa in materia di protezione dati ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile del trattamento. In particolare, il Responsabile del Trattamento risponde per tale danno (anche per eventuali suoi Sub-responsabili) se non ha adempiuto agli obblighi che la normativa pone direttamente in capo ai responsabili o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare nel presente Atto o ad ulteriori istruzioni eventualmente trasmesse per iscritto dal Titolare.
In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile del trattamento, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.
Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
Resta inteso inoltre che la presente designazione non comporta alcun diritto per il Responsabile del trattamento ad uno specifico compenso, indennità o rimborso per l'attività svolta in qualità di Responsabile, ulteriore rispetto a quanto già previsto nel contratto/convenzione stipulato con il Titolare, indicati al presente Atto.

4. **Durata del trattamento**

Il presente Atto di designazione decorre dalla data in cui viene sottoscritto dalle parti ed è condizionato, per oggetto e per durata, al rapporto contrattuale/convenzionale in corso tra l'IRST e [*nome società*] e si intenderà revocato di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso.
La nomina si intende comunque estesa ad eventuali future proroghe e/o rinnovi di contratti/convenzioni, aventi ad oggetto le medesime o ulteriori attività che comportino un trattamento di dati personali analoghi da parte di [*nome società*] in nome e per conto del Titolare.
Resta fermo che, anche successivamente alla cessazione o alla revoca del contratto/convenzione, il Responsabile del trattamento dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

5. **Restituzione e cancellazione dei dati**

Al termine del periodo di conservazione o all'atto della conclusione o della revoca del contratto/convenzione, su richiesta, o in qualsiasi altro momento per sopravvenute necessità,[*nome società*] dovrà interrompere ogni operazione di trattamento dei dati personali e dovrà provvedere, a scelta del Titolare, all'immediata restituzione dei dati allo stesso

comprese tutte le eventuali informazioni necessarie alla corretta ricostruzione dei dati, tutte le eventuali copie di backup e tutta la documentazione cartacea rilasciando contestualmente attestazione scritta che presso il Responsabile del trattamento non ne esista alcuna copia. Qualora l'operatore economico restituisca di dati mediante la produzioni di una immagine (detta anche "dump") di un archivio elettronico (database) è tenuto a fornire un riepilogo della struttura di tutte le tabelle che compongono il database stesso.
In caso di richiesta scritta del Titolare, il Responsabile del Trattamento è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

6. Clausola di salvaguardia

Per quanto non espressamente previsto nel presente atto di designazione, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali, nonché alle disposizioni di cui al contratto / convenzione stipulato tra le parti, sopra individuato.

7. Diritto applicabile e giurisdizione

Il presente Atto di nomina è regolato dalla legge Italiana.
Per tutte le controversie derivanti da o in connessione con il presente Atto di nomina il Foro Competente esclusivo sarà il Tribunale della sede legale l'IRST.

Il presente documento è redatto e sottoscritto in unico originale digitale e trasmesso alla Ditta / Società …… per la sottoscrizione per accettazione.

Il Titolare
dott. MARTELLI Giorgio

ACCETTAZIONE DELLA NOMINA

Il legale rappresentante della Ditta/Società ……..nella sua qualità di Responsabile del trattamento dei dati di cui in premessa:

- **accetta** la nomina;
- **si impegna** a procedere al trattamento dei dati personali attenendosi alle disposizioni di cui alla normativa in materia di protezione dei dati personali ed alle istruzioni impartite dal Titolare nel presente Atto o in atti successivi;
- **dichiara** di aver ricevuto ed esaminato i compiti e le istruzioni sopra indicate;

Il Responsabile del trattamento
_____

ALLEGATO 1 Ambito del trattamento (art. 28, paragrafo 3, GDPR)

Il presente Allegato costituisce parte integrante dell'Atto di designazione di [*nome società*] quale Responsabile del trattamento dei dati da parte del Titolare e definisce in particolare:

Categorie di interessati (ad es. persone fisiche assistiti e assistibili, parenti, affini o conviventi; dipendenti, collaboratori,consulenti e altro personale che a qualunque titolo svolge attività lavorativa presso l'Azienda.
Tipo di dati personali oggetto di trattamento (indicare se dati personali, particolari, genetici, giudiziari e dati relativi alla salute;
Oggetto, natura e finalità del trattamento (ad es. descrizione sintetica del servizio di trattamento dati reso dal Responsabile del trattamento al Titolare del trattamento o fare specifico rinvio all'oggetto del contratto principale - se presente - stipulato con il Responsabile del trattamento)

Allegato 2 Misure di sicurezza (art. 32 GDPR)

(IN RELAZIONE AL CONTRATTO UTILIZZARE UNA DELLE MISURE DI SICUREZZE SOTTOINDICATE O DEFINIRE NUOVE MISURE APPROPRIATE AL TRATTAMENTO DEI DATI)

1. Servizi di Assistenza, Manutenzione, Supporto, Collaborazione, che prevedano accesso ai sistemi di IRST

Quanto descritto nella presente sezione si applica al Responsabile del trattamento (Amministratore di sistema) il cui rapporto con IRST preveda l'accesso ai sistemi informativi per l'erogazione di servizi di assistenza, manutenzione, supporto, collaborazione e erogazione per conto, di qualsiasi di tipo.

1. L'accesso ai sistemi IRST deve avvenire esclusivamente con modalità sicure, concordate con IRST. E' fatto divieto di adottare sistemi di collegamento e comunicazione non concordati con IRST.
2. L'accesso ai sistemi IRST deve avvenire a seguito di emissione di credenziali IRST, che sono personali e non condivisibili; la persona fisica associata alle credenziali sarà ritenuta responsabile, insieme al Responsabile del trattamento, di ogni azione svolta con tali credenziali e ritenuta responsabile di eventuali usi impropri (es. condivisione delle credenziali con colleghi).
   - Eccezioni all'abbinamento nominale delle credenziali aziendali possono essere valutate dal Servizio Informatico solo in contesti tecnici che richiedessero tali modalità quale condizione non derogabile per l'erogazione del servizio. Tale eccezione sarà regolata con apposito emendamento al contratto di nomina a Responsabile del trattamento.
   - A seguito di cessazione del rapporto di operatori con il Responsabile del trattamento, questo è tenuto a comunicarlo al Servizio Informatico entro 12h allo scopo di procedere all'immediata disabilitazione delle credenziali.
3. Qualsiasi accesso a dati deve essere motivato da esplicita richiesta da parte di IRST o da procedura operativa concordata tra Responsabile del trattamento e IRST. È obbligo del Responsabile del trattamento mantenere documentazione delle motivazioni degli accessi, che IRST si riserva di richiedere in fase di istruttoria relativa a specifici accessi.
4. In nessun caso è consentito il trasferimento di dati in copia unica dalla IRST verso sistemi informativi del Responsabile del trattamento (es. esportazione di dati storici verso i sistemi del Responsabile del trattamento con cancellazione dai sistemi di IRST). Anche quando si rendesse necessario trasferire copia di dati verso i sistemi del Responsabile del trattamento, una copia deve rimanere archiviata sui sistemi di titolarità dell'IRST o presso l'infrastruttura IRST con modalità concordate con IRST.
5. Eventuali copie di dati verso i sistemi del Responsabile del trattamento dovranno essere autorizzate (singolarmente o tramite definizione di procedure operative) da IRST e non potranno comunque eccedere l'insieme di dati oggetto del rapporto tra il Responsabile del trattamento e IRST.
6. Eventuali copie di dati verso i sistemi del Responsabile del trattamento dovranno essere archiviate e gestite secondo modalità conformi con la normativa vigente e su sistemi che rispettino le Misure Minime di Sicurezza ICT definite da AGID come obbligatorie per le pubbliche amministrazioni. La durata dell'archiviazione deve essere limitata al soddisfacimento delle sole esigenze espresse da IRST.
7. Qualsiasi alterazione volontaria di dati (personali o non) da parte del Responsabile del trattamento sui sistemi di IRST dovrà essere preventivamente esplicitamente autorizzata da IRST.

2. Erogazione di Servizi per Conto, che prevedano accesso ai sistemi di IRST

Quanto descritto nella presente sezione si applica al Responsabile del trattamento il cui rapporto con IRST preveda l'accesso ai sistemi informativi per l'erogazione di servizi per conto, di qualsiasi di tipo.

1. L'accesso ai sistemi IRST deve avvenire esclusivamente con modalità sicure, concordate con IRST. E' fatto divieto di adottare sistemi di collegamento e comunicazione non concordati con IRST.
2. L'accesso ai sistemi IRST deve avvenire a seguito di emissione di credenziali IRST, che sono personali e non condivisibili; la persona fisica associata alle credenziali sarà ritenuta responsabile, insieme al Responsabile del trattamento, di ogni azione svolta con tali credenziali e ritenuta responsabile di eventuali usi impropri (es. condivisione delle credenziali con colleghi).
    - Eccezioni all'abbinamento nominale delle credenziali aziendali possono essere valutate dal Servizio Informatico solo in contesti tecnici che richiedessero tali modalità quale condizione non derogabile per l'erogazione del servizio. Tale eccezione sarà regolata con apposito emendamento al contratto di nomina a Responsabile del trattamento.
    - A seguito di cessazione del rapporto di operatori con il Responsabile del trattamento, questo è tenuto a comunicarlo al Servizio Informatico entro 12h allo scopo di procedere all'immediata disabilitazione delle credenziali.
3. Qualsiasi accesso a dati deve essere motivato da esplicita richiesta da parte di IRST o da procedura operativa concordata tra Responsabile del trattamento e IRST. È obbligo del Responsabile del trattamento mantenere documentazione delle motivazioni degli accessi, che IRST si riserva di richiedere in fase di istruttoria relativa a specifici accessi.
4. In nessun caso è consentito il trasferimento di dati in copia unica dall'IRST verso sistemi informativi del Responsabile del trattamento (es. esportazione di dati storici verso i sistemi del Responsabile del trattamento con cancellazione dai sistemi di IRST). Anche quando si rendesse necessario trasferire copia di dati verso i sistemi del Responsabile del trattamento, una copia deve rimanere archiviata sui sistemi di titolarità della IRST o presso l'infrastruttura IRST con modalità concordate con IRST.
5. Eventuali copie di dati verso i sistemi del Responsabile del trattamento dovranno essere autorizzate (singolarmente o tramite definizione di procedure operative) da IRST e non potranno comunque eccedere l'insieme di dati oggetto del rapporto tra il Responsabile del trattamento e IRST.
6. Eventuali copie di dati verso i sistemi del Responsabile del trattamento dovranno essere archiviate e gestite secondo modalità conformi con la normativa vigente e su sistemi che rispettino le Misure Minime di Sicurezza ICT definite da AGID come obbligatorie per le pubbliche amministrazioni. La durata dell'archiviazione deve essere limitata al soddisfacimento delle sole esigenze espresse da IRST.
7. Qualsiasi alterazione volontaria di dati (personali o non) da parte del Responsabile del trattamento sui sistemi di IRST dovrà essere preventivamente esplicitamente autorizzata da IRST.

3. Servizi in Outsourcing Totale

Fornitori di servizi IT (amministratori di sistema)

Quanto descritto nella presente sezione di applica al Responsabile del trattamento il cui rapporto con IRST preveda la fornitura di servizi verso IRST la cui infrastruttura tecnica sia totalmente in gestione al Responsabile del trattamento (es. soluzioni Cloud quali SAAS, IAAS, PAAS o gestione di sottoreti o sistemi informatici presso i locali di IRST ma a totale carico del Responsabile del trattamento).

1. Il Responsabile del trattamento si avvale misure tecniche e organizzative appropriate al fine di assicurare un livello di sicurezza adeguato al rischio, incluso inter alia, se del caso:
    a) La pseudonimizzazione o la cifratura dei dati personali
    b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
    c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
    d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."
In particolare:

- È richiesta una lista completa degli amministratori di sistema e dei manutentori, che sia completa di credenziali, data concessione, privilegi, sistemi utilizzati, sistema-cliente assegnato.
- È richiesta l'adozione di una procedura d'emergenza per subentrare alla persona destinataria delle credenziali.
- È richiesta l'adozione di una procedura di risposta (Incident Response e Business Continuity) per ripristino disponibilità dei dati in seguito a distruzione o danneggiamento.
- È richiesta l'adozione di una procedura di verifica dell'efficacia delle misure tecniche adottate.
- È richiesta l'adozione di una procedura di verifica dell'appartenenza al ruolo degli amministratori di sistema e dei manutentori, annotata nella lista.
- È necessario che vengano predisposte delle raccomandazioni sulle modalità di gestione sicura delle credenziali in possesso ed uso esclusivo dell'autorizzato.
- È richiesta l'adozione di un registro degli incidenti.
- È richiesta l'adozione di un registro dei risultati degli audit.
- È richiesta l'adozione di un registro delle anomalie (traffico, operazioni sui sistemi, tentativi di intrusione / accesso, navigazione internet, uso improprio delle P. di L. / di P. di L. non autorizzate, ecc.).
- È necessario che siano svolti degli audit per verificare il rispetto delle procedure e delle istruzioni operative del proprio personale.
- È richiesta la verifica periodica del log tecnico e della lista degli amministratori di sistema e dei manutentori, atta a rilevare incidenti di cui non si è avuta evidenza.
- È necessario predisporre una cifratura del canale di trasmissione utilizzato per la manutenzione da remoto.
- È richiesta l'adozione di un meccanismo automatico di autentificazione: conferma dell'identità dell'amministratore/manutentore tramite password, fattore biometrico, token.
- È richiesta l'adozione di un meccanismo di autorizzazione (preimpostato manualmente): gestione dell'accesso ai sistemi e dei privilegi accordati (tipi di operazioni che si è autorizzati a compiere).
- È richiesta l'adozione di un meccanismo automatico di identificazione: presentazione dell'identità dell'amministratore/manutentore tramite UserID.
- È richiesta l'adozione di un meccanismo di disabilitazione automatica degli utenti inattivi oltre un certo periodo.
- È richiesta l'adozione di un meccanismo di gestione automatica del ciclo di vita delle password (preimpostato manualmente): tempo di cambiamento e della nomenclatura (lunghezza, presenza di minuscole, maiuscole, numeri, caratteri speciali).
- È richiesta l'adozione di un tool di gestione delle richieste di assistenza/interventi programmati; richiesta di accesso all'utente-amministratore dell'azienda-cliente per consentire l'accesso.
- È necessario che siano predisposti il tracciamento e la registrazione delle operazioni compiute dall'amministratore di sistema-manutentore sull'applicativo e l'apparato (produzione log tecnico).
- È richiesta l'adozione di soluzioni (organizzative, tecniche e procedurali) volte a garantire la protezione dei dati nell'ambito di comunicazioni, elettroniche e non, all'interno dell'organizzazione;

L'IRST si riserva di chiedere approfondimenti tecnici e di rispondenza alle normative della documentazione fornita.

2. Le modalità di trattamento informatico del dato, oltre ad essere conformi alla normativa vigente, devono **rispettare le Misure Minime di Sicurezza ICT definite da AGID** come obbligatorie per le pubbliche amministrazioni.
3. Il Responsabile del trattamento deve consentire in qualsiasi momento una verifica della integrità dei dati, ed essere reso disponibile alla conclusione del rapporto tra Responsabile del trattamento e IRST per il recupero dei dati e il loro trasferimento su sistemi di gestione IRST o di altri Responsabile del trattamento. Tali dati devono essere disponibili in formato leggibile, con strutturazione e codifica documentate e coerenti con le modalità di fruizione e archiviazione applicative (es. non è considerato accesso massivo accettabile il riversamento in formati solo testuali destrutturati, PDF, immagini o comunque non riconducibile a dati strutturati e codificati).

4. Il Responsabile del trattamento deve garantire l'accesso ai log di sistema (operazioni di accesso e modifica) relativi ai trattamenti dei dati di IRST. Tale accesso deve essere reso disponibile in tempo reale ad un insieme concordato di utenti IRST, o comunque reso disponibile entro 24h dalla richiesta.
5. Il Responsabile del trattamento deve garantire ad IRST, qualora fossero necessarie operazioni massive sui dati (es. rettifica di dati per prevenire o riparare a malfunzionamenti o errati inserimenti di dati), di poter accedere in modifica con modalità massive ai dati ospitati sui sistemi del Responsabile del trattamento.
6. **Qualsiasi alterazione volontaria di dati** (personali o non) da parte del Responsabile del trattamento sui dati di IRST dovrà essere **preventivamente esplicitamente autorizzata** dalla IRST.
7. Il Responsabile del trattamento deve garantire ad IRST di poter oscurare volontariamente e in modo tracciato i dati (pur mantenendo l'oscuramento dell'operazione di oscuramento).
8. Il Responsabile del trattamento deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità IRST da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da IRST.

Fornitori del Servizio Remoto di gestione del paziente

Quanto descritto nella presente sezione di applica al Responsabile del trattamento il cui rapporto con IRST preveda la fornitura di Sistema Remoto di Gestione del paziente ("Sistema RPM") (ove richiesto dalla legge, previo consenso - esplicito - dei pazienti), il Responsabile del trattamento dovrà **generalmente**:

- far funzionare, gestire e mantenere il Sistema RPM;
- consentire il recupero e la memorizzazione dei dati del dispositivo del paziente e dei suoi dati sanitari attraverso un trasmettitore interno;
- consentire al medico o agli operatori sanitari autorizzati di accedere ai dati personali del paziente attraverso il sito/la piattaforma del Sistema RPM;
- fornire al fornitore di assistenza sanitaria la notifica di eventi e segnalazioni specifici;
- consentire un supporto tecnico avanzato da parte del personale di supporto del Responsabile del trattamento.

1. Il Responsabile del trattamento si avvale misure tecniche e organizzative appropriate al fine di assicurare un livello di sicurezza adeguato al rischio, incluso inter alia, se del caso:
   a) La pseudonimizzazione o la cifratura dei dati personali;
   b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati."
In particolare:

- È necessario predisporre istruzioni operative per effettuare il backup.
- È necessario predisporre istruzioni operative per la conservazione delle copie di dati di backup.
- È richiesta una lista completa degli amministratori di sistema e dei manutentori, che sia completa di credenziali, data concessione, privilegi, sistemi utilizzati, sistema-cliente assegnato.
- È richiesta l'adozione di una procedura d'emergenza per subentrare alla persona destinataria delle credenziali.
- È richiesta l'adozione di una procedura di risposta (Incident Response e Business Continuity) per ripristino disponibilità dei dati in seguito a distruzione o danneggiamento.
- È richiesta l'adozione di una procedura di verifica dell'efficacia delle misure tecniche adottate.
- È richiesta l'adozione di una procedura di verifica dell'appartenenza al ruolo degli amministratori di sistema e dei manutentori, annotata nella lista.
- È richiesta l'adozione di una procedura di dismissione/riciclo dei supporti di memoria (esterni come hard disk, nastri, DVD; interni come hard disk di server/NAS) utilizzati per il backup.

- È necessario che vengano predisposte delle raccomandazioni sulle modalità di gestione sicura delle credenziali in possesso ed uso esclusivo dell'autorizzato.
- È richiesta l'adozione di un registro degli incidenti.
- È richiesta l'adozione di un registro dei risultati degli audit.
- È richiesta l'adozione di un registro delle anomalie (traffico, operazioni sui sistemi, tentativi di intrusione / accesso, navigazione internet, uso improprio delle P. di L. / di P. di L. non autorizzate, ecc.).
- È necessario che siano svolti degli audit per verificare il rispetto delle procedure e delle istruzioni operative del proprio personale.
- È richiesta la verifica periodica del log tecnico e della lista degli amministratori di sistema e dei manutentori, atta a rilevare incidenti di cui non si è avuta evidenza.
- È necessario predisporre una cifratura del canale di trasmissione utilizzato per la manutenzione da remoto.
- È richiesta l'adozione di un meccanismo automatico di autenticazione: conferma dell'identità dell'amministratore/manutentore tramite password, fattore biometrico, token.
- È richiesta l'adozione di un meccanismo di autorizzazione (pre impostato manualmente): gestione dell'accesso ai sistemi e dei privilegi accordati (tipi di operazioni che si è autorizzati a compiere).
- È richiesta l'adozione di un meccanismo automatico di identificazione: presentazione dell'identità dell'amministratore/manutentore tramite UserID.
- È richiesta l'adozione di un meccanismo di disabilitazione automatica degli utenti inattivi oltre un certo periodo.
- È richiesta l'adozione di un meccanismo di gestione automatica del ciclo di vita delle password (impostato manualmente): tempo di cambiamento e della nomenclatura (lunghezza, presenza di minuscole, maiuscole, numeri, caratteri speciali).
- È necessario che siano predisposti il tracciamento e la registrazione delle operazioni compiute dall'amministratore di sistema-manutentore sull'applicativo e l'apparato (produzione log tecnico).
- È necessario predisporre il tracciamento e la registrazione delle operazioni compiute dall'utente dell'applicativo software (produzione log utente).

L'IRST si riserva di chiedere approfondimenti tecnici e di rispondenza alle normative della documentazione fornita.

2. Le modalità di trattamento informatico del dato, oltre ad essere conformi alla normativa vigente, devono **rispettare le Misure Minime di Sicurezza ICT definite da AGID** come obbligatorie per le pubbliche amministrazioni.
3. Il Responsabile del trattamento deve consentire in qualsiasi momento una verifica della integrità dei dati, ed essere reso disponibile alla conclusione del rapporto tra Responsabile del trattamento e IRST per il recupero dei dati e il loro trasferimento su sistemi di gestione IRST o di altri Responsabile del trattamento. Tali dati devono essere disponibili in formato leggibile, con strutturazione e codifica documentate e coerenti con le modalità di fruizione e archiviazione applicative (es. non è considerato accesso massivo accettabile il riversamento in formati solo testuali destrutturati, PDF, immagini o comunque non riconducibile a dati strutturati e codificati).
4. Il Responsabile del trattamento deve garantire l'accesso ai log di sistema (operazioni di accesso e modifica) relativi ai trattamenti dei dati di IRST. Tale accesso deve essere reso disponibile in tempo reale ad un insieme concordato di utenti IRST, o comunque reso disponibile entro 24h dalla richiesta.
5. Il Responsabile del trattamento deve garantire ad IRST, qualora fossero necessarie operazioni massive sui dati (es. rettifica di dati per prevenire o riparare a malfunzionamenti o errati inserimenti di dati), di poter accedere in modifica con modalità massive ai dati ospitati sui sistemi del Responsabile del trattamento.
6. **Qualsiasi alterazione volontaria di dati** (personali o non) da parte del Responsabile del trattamento sui dati di IRST dovrà essere **preventivamente esplicitamente autorizzata** dall'IRST.
7. Il Responsabile del trattamento deve garantire ad IRST di poter oscurare volontariamente e in modo tracciato i dati (pur mantenendo l'oscuramento dell'operazione di oscuramento).
8. Il Responsabile del trattamento deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità IRST da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da IRST.

4.Prestazioni/Attività svolte mediante strumenti elettronici del Responsabile del trattamento e/o strumenti cartacei

Il Responsabile del trattamento, per quanto di propria competenza, è tenuto in forza di legge e del presente accordo, per sé e per le persone autorizzate al trattamento che collaborano con la sua organizzazione, a dare attuazione alle misure di sicurezza previste dalla normativa vigente in materia di trattamento di dati personali fornendo assistenza all'IRST nel garantire il rispetto della medesima.
Il Responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, deve assicurarsi che le misure di sicurezza predisposte ed adottate siano adeguate a garantire un livello di sicurezza adeguato al rischio, in particolare contro:

- distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- trattamento dei dati non consentito o non conforme alle finalità delle operazioni di trattamento.

Il Responsabile del trattamento applica le misure di sicurezza, di cui al punto precedente, al fine di garantire:

- se del caso, 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.

Il Responsabile del trattamento è tenuto a implementare una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, trasmettendo tempestivamente all'IRST la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate.
Il Responsabile del trattamento assicura l'utilizzo di strumenti, applicazioni e/o servizi che rispettino i principi di protezione dei dati personali fin dalla progettazione (privacy by design) e per impostazione predefinita (privacy by default).

1. Adozione di procedure interne che garantiscano la protezione dei **dati trattati mediante strumenti elettronici** che garantiscano:
   In particolare, il Responsabile del trattamento dovrà prevedere:

a) un sistema di accesso ai dati tramite User ID, password con lunghezza adeguata, definizione delle tempistiche di scadenza delle password in funzione della tipologia di dati trattati, eventuali sistemi di autenticazione rafforzativi;
b) la funzionalità di autorizzazione in grado di creare profili-utente che possano gestire anche le singole operazioni;
c) La generazione del file di log per il tracciamento e la registrazione delle operazioni effettuate da utenti e amministratori di sistema;
d) soluzioni di backup in grado di garantire la disponibilità dei dati in tempi brevissimi e comunque compatibili con la continuità del servizio;
e) soluzioni di protezione dei dati a riposo (copie di backup);
f) soluzioni di protezione da virus/malware sui device funzionali all'erogazione del servizio;
g) soluzioni (organizzative, tecniche e procedurali) volte a garantire la protezione dei dati nell'ambito di comunicazioni, elettroniche e non, all'interno dell'organizzazione.

2. Adozione di procedure interne che garantiscano la protezione dei **dati trattati mediante strumenti cartacei** quali, a titolo meramente esemplificativo e non esaustivo:

a) archiviazione dei documenti cartacei contenenti dati personali in appositi armadi chiusi a chiave il cui accesso sia consentito solo ai soggetti formalmente autorizzati ed istruiti dal Responsabile del trattamento;
b) deposito dei documenti contenenti dati personali in cassetti chiusi a chiavo o, ove non disponibili, in ufficio chiuso a chiave, se non presidiato;
c) utilizzo di modalità sicure di scambio dei documenti al di fuori dell'organizzazione (es. spedizione tramite servizi con tracciamento).