CONTRATTO DI PRESTAZIONE DI SERVIZI

Tra

DECRETO DEL DIRETTORE GENERALE - N. 3970 del 07/10/2026 - Allegato Utente 1 (A01)

Ospedale San Raffaele s.r.l., con sede in 20132 Milano, via Olgettina n. 60, iscritta al Repertorio Economico Amministrativo presso la Camera di Commercio di Milano al n. MI-1972938, codice fiscale, partita IVA e numero di iscrizione Registro Imprese di Milano-Monza-Brianza-Lodi 07636600962 (Cap. Soc. € 60.817.200,00 i.v.), in persona dell'Amministratore Unico Ing. Marco Centenari (la "**Committente**" o "**OSR**")

e

FONDAZIONE IRCCS CA'GRANDA OSPEDALE MAGGIORE POLICLINICO, con sede legale in Via Francesco Sforza n. 28, 20122 Milano, Codice Fiscale 04724150968, in persona del Direttore Scientifico Prof. Fabio Blandini, autorizzato alla stipula del presente atto in virtù di delibera consiliare n. 10 del 27.03.2024 (l'"**Appaltatrice**");

(la Committente e l'Appaltatrice: congiuntamente le "**Parti**"; la Committente o l'Appaltatrice: la "**Parte**")

PREMESSE

A. La Committente è un Istituto di Ricovero e Cura a Carattere Scientifico (IRCCS) che svolge attività clinica, di ricerca e di formazione;
B. **La Committente** sta conducendo uno studio clinico profit denominato *"An Open Label, Single Arm, Phase I/II Clinical Study of Autologous CD4+ T-Cells Edited Ex-Vivo at the CD40LG Locus by CRISPR/Cas9 and IDLV-based vector in Patients with X-linked Hyper IgM Syndrome Type 1 (HIGM1)"*, identificato dal codice di protocollo **HIGM1-FT018-01** (di seguito, lo "Studio" o "Progetto"). Nell'ambito del Progetto è prevista l'esecuzione di valutazioni epatologiche specialistiche sui partecipanti pediatrici.
C. L'Appaltatrice, in qualità di Istituto di Ricovero e Cura e Carattere Scientifico (IRCCS), in conformità ai propri principi statutari, persegue, inter alia, secondo standard di eccellenza, finalità di ricerca prevalentemente clinica traslazionale e applicata nel campo biomedico, anche mediante la stipula di accordi e convenzioni con altri di enti di ricerca;
D. la Committente, in ragione di quanto dichiarato dalla Professoressa Marina Aloi Direttrice dell'Unità di Gastroenterologia, Epatologia e Trapianti Pediatrici della Appaltatrice, intende affidarle in appalto i servizi come meglio di seguito descritti ed è interessata a stipulare un contratto con l'Appaltatrice per la fornitura degli stessi ai termini e alle condizioni specificati nel presente contratto (il "**Contratto**").

Tutto ciò premesso, le Parti, come sopra rappresentate, convengono e stipulano quanto segue:

1. Premesse ed allegati

1.1. Le premesse e gli allegati costituiscono parte integrante ed essenziale del Contratto.
1.2. In ogni caso, anche qualora si presentino contrasti tra il contenuto dell'articolato e di qualsiasi allegato al Contratto, le disposizioni contrastanti dovranno essere ragionevolmente e secondo buona fede interpretate nel senso in cui risultino coerenti tra di loro, e nel senso che renda possibile la migliore esecuzione tecnica della fornitura di cui al Contratto, e tale interpretazione coerente dovrà prevalere.

2. Oggetto del Contratto

2.1. Con il Contratto, la Committente affida all'Appaltatrice, che accetta, l'esecuzione dei servizi (di seguito complessivamente i "**Servizio/i**") meglio descritti nell'offerta tecnica, qui inclusa sub **Allegato A**, (di seguito l'"**Offerta**").

2.2. I Servizi verranno prestati dall'Appaltatrice presso l'Unità di Gastroenterologia, Epatologia e Trapianti Pediatrici.

2.3. La Committente si impegna a fornire tutto il materiale occorrente per l'erogazione dei Servizi, se richiesto dall'Appaltatrice.

2.4. Resta inteso che la Committente potrà richiedere all'Appaltatrice, in qualsiasi momento, la prestazione di eventuali servizi aggiuntivi - diversi o incrementali rispetto a quelli già appaltati. A fronte di tali prestazioni, la Committente corrisponderà un importo concordato tra le Parti con separato atto. I Servizi aggiuntivi potranno essere svolti solo previa autorizzazione scritta della Committente e relativo ordine di fornitura e accettazione da parte dell'Appaltatrice.

2.5. L'Appaltatrice, è consapevole che, con la sottoscrizione del presente Contratto, assume una specifica obbligazione di risultato nei confronti della Committente consistente nella corretta e puntuale esecuzione di tutti i Servizi e le prestazioni oggetto del Contratto o comunque propedeutiche, strumentali e/o accessorie agli stessi secondo i termini e le modalità previsti nei successivi articoli. L'Appaltatrice dovrà svolgere tali Servizi con la massima diligenza ed elevati livelli di professionalità, al fine di soddisfare adeguatamente gli obiettivi della Committente.

3. Obblighi e responsabilità dell'Appaltatrice.

3.1. I Servizi dovranno essere prestati a regola d'arte, con la diligenza del miglior professionista, senza arrecare alcun intralcio o disservizio alla Committente, garantendone la continuità di esecuzione. Gli stessi dovranno essere svolti nel rispetto della normativa vigente in materia di sperimentazione clinica, degli standard qualitativi, delle procedure della Committente, dello Studio e di quanto previsto dal Contratto.

3.2. L'Appaltatrice si impegna inoltre a:

a. designare un responsabile ed un suo sostituto quale referente per i Servizi che sia rintracciabile al quale potranno essere indirizzate tutte le comunicazioni e le richieste anche di carattere d'urgenza

b. prestare i Servizi con personale idoneo, di provata capacità, in numero adeguato;

3.3. L'Appaltatrice sarà responsabile dei danni (danno emergente e lucro cessante) causati, direttamente e/o indirettamente alla Committente nell'esecuzione del Contratto e dovrà mantenere manlevata e indenne la Committente da ogni danno, costo, perdita, comprese le eventuali spese legali risultanti da:

a. qualsiasi pretesa e/o richiesta sollevata e/o rivendicata dal personale dell'Appaltatrice e/o di eventuali subappaltatori impegnato nell'esecuzione dei Servizi;

b. qualsiasi pretesa avanzata da terzi (incluso il personale della Committente, i pazienti e i visitatori), per i danni (persone e/o cose) da questi lamentati a seguito dello svolgimento delle attività oggetto del presente Contratto da parte dell'Appaltatrice e/o di eventuali subappaltatori;

c. qualsiasi comportamento, atto e/o attività illegittimi commessi dall'Appaltatrice e/o da eventuali subappaltatori;

d. eventuali multe e/o sanzioni di qualsiasi natura inflitti dalle autorità competenti alla Committente e causate dalle azioni o omissioni dell'Appaltatrice e/o da eventuali subappaltatori in relazione ai Servizi e/o all'esecuzione del presente Contratto.

4. Personale

4.1. L'Appaltatrice dichiara, garantisce e si impegna per tutta la durata del Contratto al rispetto di ogni normativa applicabile, primaria, secondaria, nazionale, locale, collettiva e contrattuale (anche retributiva e contributiva) nei rapporti con il proprio personale. Il personale dell'Appaltatrice dovrà pertanto usufruire di tutte le forme di tutela assicurativa e previdenziale previste dalla legge e dal contratto di categoria di appartenenza in vigore, ivi compresa quella contro gli infortuni, derivanti dalle disposizioni di legge e di regolamenti in vigore.

4.2. L'Appaltatrice assume l'obbligo di applicare nei confronti dei lavoratori dipendenti occupati nei Servizi oggetto del presente Contratto - e se cooperativa anche nei confronti dei soci – condizioni non inferiori a

quelle risultanti dai contratti collettivi di lavoro applicabili alla categoria e nella zona in cui i Servizi si svolgono, nonché le condizioni che risulteranno dalle eventuali successive modifiche dei contratti stessi; assume su di sé altresì l'obbligo di continuare ad applicare i suddetti contratti collettivi anche dopo la loro scadenza e fino alla loro sostituzione o rinnovo. Ove non esista alcun contratto collettivo, l'Appaltatrice si obbliga ad applicare le condizioni più favorevoli per i lavoratori tra quelle contenute nei contratti collettivi o in accordi sindacali vigenti nelle province confinanti. Gli obblighi di cui alla presente clausola vincolano l'Appaltatrice anche nel caso in cui non sia aderente alle associazioni stipulanti o receda da esse.

4.3. Durante tutto il rapporto contrattuale, nel caso in cui l'Appaltatrice dovesse avvalersi della collaborazione di cittadini di Paesi terzi, la stessa si impegna a verificarne la regolarità del permesso di soggiorno inviandone copia alla Committente che, in ogni caso, si riserva la facoltà di effettuare verifiche in loco al fine di garantire la piena conformità all'art. 22 del D.Lgs. 286/98 come modificato dal D.Lgs. 109/2012 e smi. L'inosservanza di tale obbligo comporterà la risoluzione immediata del Contratto ai sensi dell'art. 1456 del Codice civile. In ogni caso, l'Appaltatrice si obbliga, sin da ora, a manlevare e tenere indenne la Committente per eventuali sanzioni che dovessero essere comminate a quest'ultima ai sensi dell'art. 25-duodecies del D.Lgs. 231/01.

4.4. Per tutta la durata del Contratto, l'Appaltatrice provvederà al puntuale pagamento dei trattamenti retributivi, dei contributi previdenziali, dei premi assicurativi previsti dalla legge e all' accantonamento delle quote di TFR in favore del proprio personale. L'Appaltatrice dovrà altresì provvedere al puntuale versamento all'Erario delle ritenute fiscali sui redditi da lavoro dipendente (ritenute IRPEF) e dell'IVA inerente le prestazioni già effettuate oggetto del presente Contratto.

4.5. La Committente ha il diritto di richiedere l'esibizione da parte della Appaltatrice della documentazione attestante l'adempimento degli obblighi di cui al precedente capoverso, la cui correttezza costituisce condizione essenziale per procedere al pagamento degli importi ancora dovuti dalla Committente per le prestazioni ricevute dall'Appaltatrice. Nel caso in cui l'Appaltatrice risultasse inadempiente agli obblighi di cui sopra, la Committente potrà sospendere il pagamento del corrispettivo di cui al presente Contratto sino a che l'Appaltatrice non abbia dato prova del corretto adempimento delle sue obbligazioni.

4.6. L'Appaltatrice si impegna in ogni caso a presentare, su richiesta della Committente, i seguenti documenti:

a. comunicazioni di assunzione al competente centro per l'impiego e copia Libro Unico;
b. posizione INPS e posizione INAIL;
c. DURC- Documento unico di regolarità contributiva in corso di validità;
d. dichiarazione di non essere oggetto di provvedimenti di sospensione o interdittivi di cui all'art. 14 del D.Lgs. 81/2008 (lavoro irregolare).
e. elenco dei nominativi del personale impegnato nell'appalto ed in eventuali subappalti, relativi dati anagrafici completi e fotocopie delle carte d'identità, relativa copia tesserini di riconoscimento nonché indicazione delle caratteristiche del lavoro svolto. Tale elenco, se necessario, dovrà essere aggiornato durante tutta la durata del Contratto;
f. per i lavoratori impiegati nella fornitura dei Servizi aventi cittadinanza straniera, copia del permesso di lavoro e del permesso di soggiorno rilasciato dalla Questura di residenza;
g. Dichiarazione sottoscritta del legale rappresentante relativa al contratto collettivo stipulato dalle organizzazioni sindacali comparativamente più rappresentative, applicato ai lavoratori dipendenti;
h. Copia polizze assicurative infortuni dipendenti e per responsabilità civile e professionale, in corso di validità, e relativa quietanza di pagamento del premio, impegnandosi a mantenerle in vigore fino a 12 mesi successivi alla scadenza del presente Contratto;
i. Eventuale presenza di imprese e/o lavoratori autonomi in subappalto e eventuale copia del contratto di subappalto.
j. DURF (*se dovuto o se in ogni caso disponibile)*

4.7. Qualora l'Appaltatrice non provveda a consegnare i sopraddetti documenti e/o a dotare il personale di un'apposita tessera di riconoscimento, come sopra descritto, è facoltà della stessa Committente di risolvere il Contratto ai sensi e per gli effetti dell'art. 1456 c.c., mediante semplice comunicazione scritta a mezzo raccomandata A/R o PEC, senza oneri a carico della Committente.

4.8. Le Parti si danno reciprocamente atto che lo svolgimento di quanto previsto nel Contratto non potrà in alcun modo dar luogo ad un rapporto di lavoro subordinato o di altra natura tra la Committente e i dipendenti e/o collaboratori dell'Appaltatrice.

4.9. L'Appaltatrice si obbliga, in particolare, a tenere indenne e manlevare la Committente nel caso in cui quest'ultima sia chiamata, direttamente o in solido, sia estragiudizialmente che giudizialmente, a pagare importi, in via esemplificativa e non esaustiva, a titolo di retribuzioni, corrispettivi per prestazioni autonome e parasubordinate, ritenute fiscali, contributi previdenziali e assistenziali, premi, sanzioni (penali, amministrative, fiscali, o di altra natura) in relazione al personale - subordinato, autonomo o parasubordinato - impiegato dall'Appaltatrice nell'esecuzione dei Servizi o comunque sia chiamata, direttamente o in solido, sia estragiudizialmente che giudizialmente, al risarcimento di danni per comportamenti ascrivibili a dolo e/o colpa dell'Appaltatrice, nonché al risarcimento di danni subiti dal personale - subordinato, autonomo o parasubordinato – dell'Appaltatrice, impiegato sempre per l'esecuzione dei Servizi, che non risultino indennizzati ad opera dell'Inail.

4.10. Le obbligazioni e le garanzie relative al personale impiegato nell'esecuzione dei Servizi pattuite nella presente clausola, sopravvivranno alla scadenza, al recesso e/o alla risoluzione del Contratto per qualunque causa essa avvenga, sino a che il diritto oggetto della possibile pretesa, azione e/o rivendicazione del terzo e/o del personale dell'Appaltatore impiegato nell'esecuzione dei Servizi non risulti definitivamente prescritto.

4.11. La direzione, l'organizzazione e l'esercizio del potere disciplinare del personale utilizzato per l'esecuzione delle attività oggetto del presente Contratto saranno di esclusiva competenza e responsabilità dell'Appaltatrice.

5. Dichiarazioni e garanzie dell'Appaltatrice

5.1. L'Appaltatrice rilascia le dichiarazioni e le garanzie che seguono, impegnandosi a comunicare tempestivamente eventuali variazioni a seguito delle quali la Committente valuterà la sussistenza dei requisiti necessari per proseguire nel rapporto contrattuale. Nello specifico, l'Appaltatrice dichiara e garantisce che:

a. ha una propria sede legale e operativa del tutto autonoma e distaccata da quella della Committente, con propri uffici e propria autonoma organizzazione di mezzi e persone;
b. è libera di intrattenere, così come in effetti intrattiene, rapporti non solo con la Committente, ma anche con altre committenti;
c. ha acceso le seguenti posizioni assicurative, sulle quali versa i contributi per il personale: posizione INPS 4967548636 posizione INAIL 5132202;
d. possiede tutti i requisiti, le autorizzazioni, le assicurazioni di legge necessarie per la prestazione dei Servizi.

5.2. L'Appaltatrice si impegna a provare per iscritto l'adempimento di tali obblighi a semplice richiesta della Committente, restando inteso che il mancato riscontro entro 30 giorni dalla richiesta, autorizzerà la Committente a sospendere ogni pagamento in favore dell'Appaltatrice.

6. Modalità di esecuzione del Contratto

6.1. Le direttive e le procedure eventualmente indicate dalla Committente all'Appaltatrice sono esclusivamente dirette a consentire a quest'ultima di organizzare la propria attività in vista del regolare svolgimento dei Servizi forniti in adempimento del Contratto e verranno comunicate all'Appaltatrice senza influire sui suoi normali poteri organizzativi e direttivi. L'Appaltatrice conserva, pertanto, la piena ed assoluta autonomia e responsabilità nell'esercizio di tali poteri nei confronti di tutto il personale impiegato nell'appalto.

6.2. L'Appaltatrice si impegna ad eseguire l'appalto disciplinato dal Contratto secondo le eventuali istruzioni e direttive comunicate dalla Committente che siano dirette a realizzare la più puntuale ed utile esecuzione dello stesso Servizio appaltato.

6.3. L'Appaltatrice è tenuta a dare immediata notizia alla Committente di eventuali difficoltà che possano compromettere e/o limitare la regolare esecuzione dei Servizi.

7. Durata del Contratto e facoltà di recesso.

7.1. Il Contratto avrà efficacia a decorrere dalla data di firma dell'ultima Parte contraente fino alla conclusione dello Studio, conclusione prevista per Dicembre 2031. (

7.2. Resta inteso che ciascuna Parte e avrà la facoltà di recedere in qualsiasi momento dallo stesso inviando una comunicazione a mezzo PEC o lettera raccomandata a/r con un preavviso di almeno 30 (trenta) giorni. In tal caso, in deroga all'art. 1671 del codice civile, l'Appaltatrice avrà diritto al solo corrispettivo per i Servizi effettuati fino alla data di recesso, senza poter pretendere nessun altro importo, a nessun titolo.

7.3. In caso di cessazione, a qualunque titolo, del Contratto, l'Appaltatrice si obbliga, salvo diverso accordo scritto con la Committente:

(i) a garantire la fornitura dei Servizi, nel rispetto degli obblighi previsti dal Contratto, fino alla cessazione del Contratto, incluso l'eventuale periodo di preavviso di recesso o altro tipo di cessazione;

(ii) a trasferire alla Committente (e/o ad altri soggetti terzi da essa indicati) ogni informazione, dato e documentazione generata dall'esecuzione dei Servizi in favore della Committente, e/o comunque utili al fine di consentire alla Committente (e/o ad altri soggetti terzi da essa incaricati) la continuità dei Servizi, senza alcun onere o costo aggiuntivo per la Committente.

8. Corrispettivo

8.1. La Committente si impegna a corrispondere all'Appaltatrice per l'esecuzione delle Attività la somma massima totale massima complessiva di € 62.880,00 (sessantaduemilaottocentoottanta/00) oltre IVA per le visite dei pazienti inclusi nello Studio, il tutto risulta comunquemeglio dettagliato nell'allegato A (di seguito il "Corrispettivo").

Il Corrispettivo sarà versato - mediante bonifico bancario - da parte della Committente a cadenza annuale, decorrente dalla data di ultima sottoscrizione ed entro 90 (novanta) giorni dffm data dalla fattura fine mese emessa dall'Appaltatrice. La fattura verrà accompagnata dalla rendicontazione delle analisi effettuate, rendicontazione previamente approvata da parte della Committente per tramite del Prof. Alessandro Aiuti o persona da esso delegata.

A tal proposito, di seguito si riportano i riferimenti bancari dell'Appaltatrice:

Nome del Beneficiario	**Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico**
Indirizzo del Beneficiario	Via Francesco Sforza, 28 20122 – Milano, Italy
Partita IVA/codice fiscale:	04724150968
Nome della banca	Gruppo Intesa San Paolo
Indirizzo della banca	CORSO ITALIA, 20-22
Valuta ricevente/Receiving currency:	Euro/Eur
Codice ABI: ABI Code:	A030
Codice CAB/CAB Code:	6901
Numero di c/c/ Account number:	100000300006
IBAN/IBAN:	IT54A0306901791100000300006
Codice SWIFT (8 o 11 caratteri)/SWIFT Code (8 or 11 characters):	BCITITMM
Informazioni di contatto	
Ufficio competente:	Gestione Economica DS
Numero di telefono ed e-mail	trial.economiaefinanza@policlinico.mi.it

Ai fini del pagamento le fatture dovranno:

(i) indicare il numero d'ordine che verrà comunicato al seguente indirizzo e-mail (riferimento appaltatrice al punto 18.8);

(ii) essere intestate a Ospedale San Raffaele S.r.l, via Olgettina 60, Milano, C.F. e P.IVA n. 07636600962;

(iii) le fatture elettroniche in formato "xml" devono essere trasmesse tramite il Sistema di Interscambio (SDI) tramite apposito codice alfanumerico **0D3UYWQ**.

In assenza dell'indicazione del numero d'ordine, le fatture verranno restituite ai fini della corretta emissione e, dall'invio dei nuovi documenti correttamente emessi, decorreranno nuovi termini per il pagamento.

Resta inteso che il Corrispettivo di cui al presente articolo è da intendersi comprensivo di tutti i costi diretti e indiretti in qualunque forma sostenuti dal Policlinico per l'esecuzione del Contratto.

8.2. I costi della sicurezza, se applicabili, sono definiti d'intesa tra le Parti all'interno del documento di valutazione delle interferenze (DUVRI) per la gestione degli eventuali casi specifici di interferenza, che costituirà parte integrante del Contratto.

8.3. In caso di ritardato pagamento, verranno calcolati gli interessi di mora solamente se espressamente richiesti per iscritto e, in ogni caso, nella misura legale.

8.4. L'Appaltatrice riconosce che i corrispettivi, come sopra riportati, sono omnicomprensivi rispetto a tutti i Servizi prestati e comprendono qualsiasi onere, costo e spesa che possano essere sostenuti dall'Appaltatrice in relazione alla prestazione dei Servizi medesimi (inclusi oneri, costi e spese per il personale, per i materiali di consumo, per gli attrezzi ed i materiali).

8.5. L'Appaltatrice s'impegna a:

(i) non sollevare obiezioni al fine di ritardare, sospendere o eliminare la fornitura dei Servizi in conformità con l'Articolo 1462 c.c., compreso il mancato adempimento da parte della Committente delle proprie obbligazioni ai sensi del presente Contratto;

(ii) non concedere a terzi mandati per il recupero crediti e/o deleghe di pagamento.

9. Divieto di cessione del contratto e dei crediti, subappalto.

9.1. L'Appaltatrice non potrà cedere, in tutto o in parte, neanche parzialmente, il Contratto e/o i diritti/obblighi che ne derivano. I crediti nei confronti di OSR derivanti dal Contratto, dunque, non potranno formare oggetto di cessione o di mandato all'incasso o di qualsiasi altro atto di disposizione a favore di terzi, siano anche intermediari bancari e finanziari autorizzati e vigilati dalla Banca d'Italia; la presente clausola è derogabile dalle parti solo tramite diverso accordo scritto.

9.2. È vietato il subappalto, salva espressa autorizzazione scritta preventiva della Committente.

10. Sistema di monitoraggio delle attività

10.1. L'Appaltatrice si impegna a consentire ai rappresentanti delegati da OSR o suoi delegati di verificare, presso i suoi locali, la buona tenuta e conservazione ai sensi di legge della documentazione relativa al Progetto e, in generale, le attività oggetto del Contratto e, se del caso, ad applicare misure correttive richieste da OSR.

10.2. Inoltre, l'Appaltatrice si obbliga a prestare tutta l'assistenza necessaria qualora le Autorità Competenti chiedessero accesso ai suoi locali e alla documentazione relativa al Progetto.

10.3. L'Appaltatrice si impegna a garantire a OSR e/o ad ogni società di audit da questi eventualmente nominata nonché ad ogni autorità regolatoria, per tutta la durata del Contratto e per i 12 (dodici) mesi successivi alla sua scadenza o cessazione, il diritto di accedere ed esaminare direttamente ogni documentazione relativa al Contratto ("Audit"), ai fini del controllo e del monitoraggio della corretta esecuzione dello stesso e dalla presenza di un sistema di qualità idoneo. Ciascun Audit sarà pianificato durante il normale orario di lavoro e richiesto con almeno 15 (quindici) giorni di preavviso.

11. Risoluzione del Contratto

11.1. Fatte salve le ipotesi di cessazione definite nel Contratto e previste dalla legge, la Committente avrà diritto di risolvere immediatamente il Contratto ai sensi dell'art. 1456 c.c., fatto salvo il diritto al risarcimento del danno, tramite comunicazione scritta a mezzo PEC o raccomandata A/R da inviarsi all'Appaltatrice, a tale fine farà fede la data di ricezione della comunicazione, laddove l'Appaltatrice non adempia agli obblighi di cui agli artt. 9 (Divieto di cessione e di subappalto), 10 (Obbligo all'esecuzione della prestazione), 11 (sistema di monitoraggio delle attività e penali), art. 13 (assicurazioni), 15 (Igiene e sicurezza) e 16 (clausola 231).

11.2. La Committente si riserva la facoltà di chiedere la risoluzione del Contratto ai sensi dell'art. 1454 del codice civile, nel caso in cui l'Appaltatrice non dovesse porre rimedio ad un determinato inadempimento - la cui gravità vada a condizionare il regolare svolgimento dell'attività ospedaliera - entro cinque giornate lavorative dalla relativa contestazione scritta.

11.3. In caso di cessazione del presente Contratto per qualsivoglia altro motivo, l'Appaltatrice non avrà diritto ad ulteriori rimborsi, risarcimenti, contributi, indennità, anche per il mancato guadagno, ovvero a qualsiasi altro titolo, anche in deroga alle norme di legge applicabili, salvo il pagamento delle spese sostenute e documentate, nonché delle prestazioni effettivamente rese fino alla data di efficacia del Contratto, e OSR non sarà responsabile per eventuali perdite o danni subiti dall'Appaltatrice, a meno che non siano direttamente imputabili ad una violazione del presente Contratto o della normativa applicabile da parte di OSR.

12. Assicurazione

12.1. L'Appaltatrice dichiara e garantisce di essere in possesso di una polizza di assicurazione, a primo rischio, per responsabilità civile con massimale idoneo per la tipologia di attività esercitata, senza diritto di regresso nei confronti della Committente e senza franchigia opponibile a terzi, a copertura, per tutta la durata del Contratto (i) dei danni (alla persona o alle cose), diretti e/o indiretti, che durante lo svolgimento dei Servizi oggetto del presente Contratto l'Appaltatrice dovesse arrecare alla Committente, al suo personale, e/o a terzi in generale, inclusi i pazienti/utenti della Committente, nonché (ii) dei danni (alla persona o alle cose) che il Personale dell'Appaltatrice dovesse subire durante lo svolgimento delle attività appaltate, indipendentemente dalla causa e dal responsabile.

13. Igiene e Sicurezza.

13.1. L'Appaltatrice ha dichiarato di essere in possesso di tutti i requisiti tecnico professionali obbligatori connessi alla natura specifica della prestazione oggetto del Contratto e di impegnarsi ad adottare, per tutta la durata del Contratto, tutti i provvedimenti e le cautele necessari a garantire il rispetto della normativa sull'igiene e la sicurezza del personale e dei terzi (in generale la "Normativa sull'Igiene e Sicurezza"), ottemperando a tutte le disposizioni applicabili in materia, con particolare riferimento al D. Lgs. 81/2008.

13.2. Le Parti si impegnano a collaborare per la piena applicazione dell'art. 26 del D.Lgs. 81/08, fermi restando gli obblighi in capo alle stesse relativamente ai commi 1 e 2 del suddetto articolo.

13.3. Le Parti dichiarano che l'esecuzione dei Servizi non comporta la necessità per l'Appaltatrice di recarsi presso le strutture della Committente

14. Modello Organizzativo ex D.lgs. 231/2001, Codice Etico e rispetto normativa anticorruzione

14.1 Le Parti dichiarano di essere consapevoli

- che il D.lgs. 8 giugno 2001 n. 231 (il "Decreto") prevede la responsabilità diretta delle società in relazione alla commissione di una serie di reati realizzati da suoi dipendenti, fornitori o partner commerciali, che si aggiunge alla responsabilità personale di colui che ha commesso l'illecito.
- della legge sulle disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (legge 190/2012 ed eventuali successive modifiche e integrazioni).

14.2 Le Parti prendono rispettivamente atto, inoltre, che

(i) OSR ha adottato un modello di organizzazione, gestione e controllo in conformità ai principi previsti dal Decreto ("Modello Organizzativo"), un Codice Etico ("Codice Etico"), nonché una Policy Anticorruzione liberamente consultabili sul sito internet di OSR al link https://www.hsr.it/strutture/ospedale-san-raffaele/trasparenza, al fine di prevenire la responsabilità prevista per la commissione dei reati previsti dal Decreto e l'applicazione delle relative sanzioni;

(ii) l'Appaltatrice, nel rispetto delle disposizioni di cui alla L. 190/2012 e s.m.i. e della normativa in materia di trasparenza di cui al Dlgs 33/2013 e s.m.i., ha adottato un proprio codice etico ed un piano triennale per la prevenzione della corruzione e della trasparenza, pubblicati sul sito istituzionale al link www.policlinico.mi.it/trasparenza, impegnandosi a rispettarne le regole e i principi espressi.

14.3 Le Parti si impegnano a conformarsi alle regole di cui sopra, per quanto a ciascuna applicabili, nell' esecuzione del presente Contratto. La violazione del predetto impegno costituirà un inadempimento grave degli obblighi di cui al Contratto e legittimerà l'altra Parte a risolvere la stessa con effetto immediato, ai sensi e per gli effetti di cui all'articolo 1456 del Codice civile, fermo restando il risarcimento dei danni eventualmente causati.

14.4 OSR si riserva la facoltà di recedere unilateralmente e con effetto immediato dal contratto, qualora Fondazione

non ottemperando a quanto previsto all'articolo "Modello Organizzativo ex D. Lgs. 231/2001 e Codice Etico", non fornisca la documentazione richiesta da OSR o fornisca dati falsi e/o incompleti, ovvero si opponga alle attività di audit di cui OSR richiede l'esecuzione.

15. Riservatezza

15.1. Fatto salvo quanto altrimenti espressamente previsto nel presente Contratto, le informazioni relative al presente Contratto o ad esso conseguenti (compresi, ma senza limitazione, il contenuto del presente Contratto), comunicate tra le Parti, saranno ritenute strettamente riservate (di seguito, "**Informazioni Riservate**").

15.2. Per prevenire la rivelazione a terzi delle Informazioni Riservate, ciascuna Parte adotterà le stesse cautele adottate per proteggere le proprie Informazioni Riservate e, in ogni caso, cautele quanto meno ragionevoli per evitare la diffusione o la conoscenza da parte di terzi non autorizzati delle Informazioni Riservate.

15.3. Ciascuna Informazione Riservata sarà utilizzata dalla Parte ricevente (inclusi i propri rappresentanti, subappaltatori o dipendenti) unicamente ai fini dell'esecuzione dal presente Contratto, e non sarà divulgata a soggetti non previsti dal Contratto o per fini diversi dall'esecuzione dello stesso senza il preventivo consenso scritto della Parte a cui appartiene o da cui proviene tale Informazione Riservata. Non costituirà violazione del disposto del precedente periodo la divulgazione di Informazioni Riservate (i) già note alla Parte ricevente senza vincoli di riservatezza, (ii) di pubblico dominio o divenute di pubblico dominio per atto non vietato alla Parte ricevente, (iii) legittimamente ricevute da terzi, (iv) autonomamente elaborate dalla Parte ricevente senza l'uso di Informazioni Riservate ricevute da un'altra Parte, (v) la cui divulgazione sia stata autorizzata per iscritto dall'altra Parte, (vi) delle quali sia imposta la divulgazione in conseguenza di disposizioni di una pubblica autorità o di legge (purché la Parte divulgante abbia informato di tale imposizione la Parte proprietaria prima di tale divulgazione, nei limiti consentiti dalla legge), oppure (vii) per esercitare diritti di difesa nell'ambito di procedimenti amministrativi o giudiziari.

15.4. Ciascuna Parte potrà divulgare Informazioni Riservate ai propri consulenti, partner commerciali e legittimi subappaltatori (ad esclusione dei concorrenti dell'altra Parte) limitatamente a quanto strettamente necessario e consentito da ciascuna Parte per l'esecuzione delle attività svolte ai sensi del presente Contratto.

15.5. In caso di cessazione (per qualsivoglia motivo) del presente Contratto, gli obblighi di riservatezza di cui al presente articolo restano validi ed efficaci per i 5 (cinque) anni successivi alla predetta cessazione del presente Contratto.

15.6. Resta in ogni caso inteso che le Informazioni Riservate restano di proprietà della Parte che le ha generate e che nessuna Parte acquisirà alcun diritto di utilizzo di Informazioni Riservate di proprietà dell'altra Parte anche dopo il decorso del termine di cui al paragrafo che precede.

16. Diritti di proprietà industriale e intellettuale

16.1. Le Parti si danno reciprocamente atto sin da ora che nel corso dell'esecuzione del Contratto tra loro verranno, e/o potrebbero essere, utilizzati in varia misura know-how e/o beni coperti da diritti di proprietà industriale e/o intellettuale nella titolarità di ciascuna di esse, su cui l'altra Parte non acquisirà alcun autonomo diritto di utilizzazione a qualunque titolo (di seguito "Background").

16.2. Resta, altresì, fermo che ciascuna Parte rimane esclusiva proprietaria di ogni informazione, conoscenza, dato e risultato acquisito indipendentemente e/o precedentemente alla data di sottoscrizione del Contratto e risultante da prova documentale, con la conseguenza che l'altra Parte non ne acquisirà alcun diritto di utilizzazione a qualsivoglia titolo.

16.3. Le Parti danno atto che i risultati, gli elaborati e i dati, prodotti e risultanti direttamente dall'esecuzione delle Attività oggetto del Contratto sono di esclusiva proprietà di OSR.

17. Privacy.

17.1. In conformità a quanto previsto dal D.Lgs. n. 196 del 30 giugno 2003 (di seguito anche solo "Codice Privacy"), e successive modifiche ed integrazioni, nonché dal Regolamento 2016/679/UE (di seguito anche solo "Regolamento UE"), i dati personali dei rispettivi referenti aziendali della Committente e della Appaltatrice che verranno scambiati fra le Parti nel corso dello svolgimento del Contratto saranno trattati rispettivamente da ciascuna delle Parti per le sole finalità amministrative volte all'adempimento dei rispettivi obblighi contrattuali, nonché per adempiere ad eventuali obblighi di legge, secondo principi di liceità e correttezza ed

in modo da tutelare la riservatezza e i diritti riconosciuti dalla normativa vigente, nel rispetto di adeguate misure di sicurezza e di protezione dei dati.

17.2. Poiché nell'esecuzione del Contratto, l'Appaltatrice tratterà dati personali per conto della Committente, l'Appaltatrice viene designata, senza alcun onere aggiunto per la Committente, quale Responsabile del Trattamento a norma dell'art. 28 del Regolamento UE, con apposito atto allegato al presente Contratto sub **Allegato B.**

17.3. Nello svolgimento delle attività oggetto del presente Contratto, il personale impiegato dall'Appaltatrice non potrà prendere conoscenza di nessun dato personale che non sia strettamente necessario per lo svolgimento delle mansioni loro assegnate.

17.4. Il personale impiegato dall'Appaltatrice dovrà in ogni caso mantenere la massima riservatezza con riferimento ai dati di cui dovesse venire, anche accidentalmente, a conoscenza nell'ambito dei Servizi, astenendosi dal rivelare le informazioni di cui ha preso conoscenza e/o di estrarne copia sotto qualsiasi forma.

17.5. Resta inteso che L'Appaltatrice dovrà manlevare e tenere indenne la Committente da qualunque richiesta di risarcimento per eventuali danni arrecati a terzi a seguito della violazione della normativa in materia di privacy addebitabile alla condotta della Appaltatrice e/o del proprio personale.

18. Disposizioni generali

18.1. Il Contratto costituisce manifestazione di integrale accordo tra le Parti e supera e sostituisce qualsiasi precedente accordo e/o intesa e/o comunicazione, sia verbale sia scritta, tra le stesse in relazione ai contenuti del Contratto.

18.2. L'eventuale tolleranza di una Parte ai comportamenti delle altre Parti posti in essere in violazione delle disposizioni contenute nel Contratto non costituisce rinuncia ai diritti derivanti dalle disposizioni violate né al diritto di esigere l'esatto adempimento delle prestazioni dovute.

18.3. Qualora una clausola del Contratto venisse dichiarata invalida, le Parti saranno sollevate dagli obblighi derivanti da tale clausola, ma soltanto per la parte di essa che sia stata dichiarata invalida. In tale ipotesi le Parti si impegnano a rinegoziare in buona fede una nuova clausola che abbia effetti giuridici ed economici quanto più possibile equivalenti a quelli della clausola dichiarata invalida, fatta salva l'applicazione automatica di norme imperative ai sensi dell'articolo 1419 cod. civ.

18.4. Qualsiasi modifica e/o integrazione al Contratto, o rinuncia a diritti da esso nascenti, non sarà valida e vincolante ove non risulti da atto sottoscritto da tutte le Parti.

18.5. L'Appaltatrice non utilizzerà i marchi e/o loghi di proprietà di OSR, ovvero di una delle società del Gruppo San Donato, senza il preventivo consenso scritto della società interessata, restando inteso che i predetti i marchi e/o loghi, in caso di autorizzazione, verranno utilizzati esclusivamente secondo i termini e alle condizioni previste dalla società interessata e nel rispetto delle direttive dalla stessa impartite.

18.6. L'Appaltatrice non avrà il diritto di fare qualsiasi annuncio e/o comunicazione a terzi, compresi i media, in relazione o in qualsiasi modo collegati ai Servizi, compresa l'esistenza del Contratto, senza il preventivo consenso scritto di OSR.

18.7. Il Contratto non crea alcun rapporto virtuale o effettivo di associazione o partnership o joint venture tra le Parti.

18.8. Tutte le comunicazioni relative al Contratto dovranno essere effettuate per iscritto a mezzo di posta elettronica certificata o di lettera raccomandata a/r o, salvo nei casi ove diversamente specificato, via e-mail, ai seguenti indirizzi:

per OSR: aiuti.alessandro@hsr.it - clinicaltrialcenter@hsr.postecert.it

per l'Appaltatrice: giuridico.ricerca@policlinico.mi.it

ovvero presso il diverso indirizzo che le Parti potranno comunicare successivamente in conformità al presente Contratto.

18.9. Le Parti danno atto che il Contratto è stato liberamente e direttamente negoziato dalle Parti stesse, e che, pertanto, non si rende applicabile alla fattispecie il disposto di cui agli artt. 1341 e 1342 c.c.

18.10. Il presente Contratto sarà registrato in caso d'uso. I costi di registrazione del presente Contratto graveranno invia esclusiva sulla Parte richiedente la registrazione dello stesso. Le Parti convengono che l'imposta di bollo è a carico di OSR.

19. LEGGE APPLICABILE E FORO COMPETENTE

19.1. Il Contratto ed i diritti e le obbligazioni delle Parti ricadono nella giurisdizione esclusiva della Repubblica Italiana e saranno regolati, interpretati ed eseguiti in conformità della legge italiana stessa. Per qualsiasi controversia connessa e/o collegata e/o relativa al Contratto (inclusa, a titolo non esaustivo, la sua negoziazione, interpretazione, esecuzione e risoluzione) promossa a qualsivoglia titolo (anche pre-contrattuale ed extracontrattuale) sarà competente in via esclusiva e inderogabile il Foro di Milano.

Elenco Allegati:

A) Offerta Progettuale ed Economica

B) Nomina a Responsabile del Trattamento Dati Personali

Ospedale San Raffaele s.r.l

L'Amministratore Unico

Ing. Marco Centenari

Firmato Digitalmente

FONDAZIONE IRCCS CA'GRANDA

OSPEDALE MAGGIORE POLICLINICO,

Direttore Scientifico Prof. Fabio Blandini,

Firmato Digitalmente

PER PRESA VISIONE ED ACCETTAZIONE

Principal Investigator	Direttrice dell'Unità di Gastroenterologia, Epatologia e Trapianti Pediatrici
_____	_____
Prof. Alessandro Aiuti	Prof. Marina Aloi
Data: _____	Data: _____

Allegato A

Oggetto: Proposta di Collaborazione Clinica per Studio di Fase 1-2 HIGM1-FT018-01 "*Studio clinico di Fase I/II, sull'uso di linfociti T CD4+ autologhi modificati ex vivo nel locus CD40LG mediante CRISPR/Cas9 e vettore basato su IDLV in pazienti con sindrome da iper-IgM legata al cromosoma X di tipo 1 (HIGM1)*" condotto presso l'IRCSS Ospedale San Raffaele di Milano e sponsorizzato da Fondazione Telethon ETS e Ospedale San Raffaele.

Dettagli operativi e organizzativi della collaborazione con l'Unità di Gastroenterologia, Epatologia e Trapianti Pediatrici, Policlinico di Milano

Numero di Pazienti: massimo 6 pazienti pediatrici

Durata del Follow-Up: 2 anni per paziente

Sede delle Valutazioni Epatologiche: Ambulatori Pediatrici, Padiglione Regina Elena, Via Fanti 6, Milano

Frequenza delle Valutazioni:

- Screening pre-terapia genica
- +6 mesi post-terapia genica
- +1 anno post-terapia genica
- +2 anni post-terapia genica

Visite e Esami Previsti:

1. **Valutazione Epatologica:** da effettuare a ogni visita.
2. **Biopsia epatica:** da effettuare solo su indicazione dell'epatologo
3. **Eventuali ulteriori esami di approfondimento per diagnostica differenziale**: da effettuare solo a seguito di valutazione dell'epatologo

Note Aggiuntive: Nessuna

Durata Stimata di Ogni Visita: Circa 1 h/visita

Modalità di Trasporto: Trasferimento dei pazienti presso il Policlinico in auto privata o ambulanza, a seconda delle necessità cliniche e logistiche.

Condivisione dei risultati: I risultati (es. referto dell'anatomia patologica, lettera di dimissione) saranno trasmessi via e-mail in formato protetto da password ai seguenti indirizzi: aiuti.alessandro@hsr.it; ferrua.francesca@hsr.it; canarutto.daniele@hsr.it; locatelli.sara@hsr.it e JofraHernandez.Raisa@hsr.it.

La password verrà comunicata separatamente tramite telefono cellulare al seguente numero: +39 3666803779.

Conservazione dei campioni. Nel caso di biopsia epatica il materiale viene sempre incluso in toto per cui non esiste riserva da smaltire; le inclusioni in paraffina restano quindi disponibili nell'archivio di Anatomia Patologica. Il tempo minimo per la conservazione delle inclusioni è 10 anni, ma le Anatomie Patologiche cercano di non smaltire mai le inclusioni.

Corrispettivo. Per l'esecuzione delle visite dei pazienti in studio verranno corrisposti dei pagamenti secondo la rendicontazione degli esami effettuati dal Policlinico, come indicato nella tabella sottostante.

	Visita Epatologica	**Biopsia**[§] Eseguita in regime di ricovero (durata stimata di 2/3 giorni).		Eventuali ulteriori esami di approfondimento per diagnostica differenziale[§]
Screening	120 €	Costo totale primo giorno	850 €	Il costo degli esami verrà indicato di volta in volta a seguito della valutazione dell'Epatologo dopo la visita
		Giorni successivi di ricovero (2/3)	500 € ciascuno (1500 € totale)	
		Esame istologico	150 €	
+6 mesi	120 €	Costo totale primo giorno	850 €	
		Giorni successivi di ricovero (2/3)	500 € ciascuno (1500 € totale)	
		Esame istologico	150 €	
+12 mesi	120 €	Costo totale primo giorno	850 €	
		Giorni successivi di ricovero (2/3)	500 € ciascuno (1500 € totale)	
		Esame istologico	150 €	
+24 mesi	120 €	Costo totale primo giorno	850 €	
		Giorni successivi di ricovero (2/3)	500 € ciascuno (1500 € totale)	
		Esame istologico	150 €	

[§] opzionale, solo in caso di ulteriori necessità cliniche

Allegato B

CONTRATTO PER IL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679 (INFRA "REGOLAMENTO")

TRA

Ospedale San Raffaele S.r.l., con sede legale in Milano (MI) via Olgettina n. 60 iscritta al Repertorio Economico Amministrativo presso la Camera di Commercio di Milano al n. MI-1972938 codice fiscale, partita IVA e numero di iscrizione Registro Imprese di Milano 07636600962 (Cap. Soc. € 60.817.200,00) società con socio unico, soggetta a direzione e coordinamento di Gruppo San Donato S.p.A., in persona del dell'Amministratore Unico Ing. Marco Centenari , (di seguito anche **"OSR"** o il **"Titolare"**); (di seguito anche il "**Titolare**")

E

FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO, con sede legale a Milano, in Via Francesco Sforza 28, Codice Fiscale e Partita IVA 04724150968, legalmente rappresentata dal Direttore Scientifico, Prof. Fabio Blandini (di seguito anche **"Fornitore"** o il "**Responsabile**");

OSR e il Fornitore, potranno essere definiti anche singolarmente la "**Parte"** e congiuntamente le **Parti**.

PREMESSO CHE

- il titolare dei trattamenti di dati personali è il soggetto cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali;
- in base all'art. 28 del Regolamento, il titolare dei trattamenti di dati personali può proporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale responsabile del trattamento dei dati, che sia selezionato tra soggetti che, per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso i profili di sicurezza;
- il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
- il responsabile del trattamento deve procedere al trattamento secondo le istruzioni impartite per iscritto dal titolare del trattamento con contratto o altro atto giuridico che vincoli il responsabile del trattamento e che specifichi durata, natura e finalità del trattamento, tipo di dati personali, categorie di interessati, obblighi e diritti del Titolare;
- il titolare del trattamento consente al responsabile del trattamento e alle persone autorizzate al trattamento l'accesso ai soli dati personali la cui conoscenza sia necessaria per adempiere ai compiti loro attribuiti;
- OSR e il Fornitore hanno sottoscritto un accordo di servizi (l'"**Accordo**"), di cui tale contratto è parte integrante, avente ad oggetto i servizi meglio precisati all'Allegato I;

TUTTO CIÒ PREMESSO,

1) OSR, nella sua qualità di titolare del trattamento e in persona del suo legale rappresentante, designa il Fornitore quale responsabile del trattamento dei dati personali effettuati nell'ambito dell'Accordo di servizi in vigore. Nessuna previsione di cui all'Accordo potrà applicarsi al presente Contratto al fine di prevedere limitazioni o esclusioni di responsabilità in capo al Responsabile.

2) In ogni caso, OSR affida al Fornitore tutte – ed esclusivamente – le operazioni di trattamento dei dati personali necessarie per dare piena esecuzione all'Accordo. In caso di danni derivanti dal trattamento svolto dal Fornitore, questi manterrà manlevato e indenne OSR da qualsiasi danno diretto e indiretto (incluse eventuali sanzioni amministrative comminate da legittime autorità nei confronti di OSR)

qualora questi non abbia adempiuto agli obblighi del Regolamento specificatamente diretti ai responsabili del trattamento o abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento (art. 83 e ss. Regolamento).

3) OSR si impegna a comunicare ufficialmente al Fornitore qualsiasi variazione si dovesse rendere necessaria nelle operazioni di trattamento dei dati. Il Fornitore o le persone dallo stesso autorizzate non potranno effettuare nessuna operazione di trattamento dei dati al di fuori di quelle necessarie sopra ricordate.

4) Il Fornitore, per quanto di propria competenza, è tenuto in forza di legge e del presente contratto, per sé e per i propri dipendenti e per chiunque collabori con la sua attività, al rispetto delle disposizioni del Regolamento, della normativa nazionale e dell'UE di settore applicabile, dei provvedimenti e/o delle autorizzazioni e/o linee guida del Garante per la Protezione dei Dati Personali.

5) Il Fornitore dovrà eseguire i trattamenti funzionali ai Servizi, così in conformità con quanto precisato nell'Allegato I del presente contratto. Qualora sorgesse la necessità di ulteriori trattamenti, il Fornitore si impegna ad informare preventivamente e in tempo utile OSR il quale potrà opporsi.

6) Il Fornitore, per quanto di propria competenza, è tenuto in forza di legge e del presente contratto, 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 pro tempore vigente in materia di trattamento di dati personali, fornendo assistenza a OSR nel garantire il rispetto della medesima. Il Fornitore, 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 Fornitore deve garantire l'adozione delle misure descritte nell'Allegato IV "Misure di sicurezza".

7) Il Fornitore applicherà 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 Fornitore implementerà 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 a OSR la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito adottate.

Qualora dovesse raccogliere dati presso gli interessati o questi ne richiedessero una copia, il Fornitore sottometterà agli stessi l'informativa redatta da OSR, secondo le istruzioni che gli saranno fornite.

Il Fornitore deve, altresì, gestire tramite adeguate procedure, secondo criteri di efficienza e garantendone la custodia, la non alterazione e l'agevole reperimento della documentazione relativa agli adempimenti formali previsti dal Regolamento. Il Fornitore, su richiesta di OSR, coadiuva quest'ultimo nelle procedure davanti al Garante o all'autorità giudiziaria in relazione alle attività rientranti nella sua competenza.

8) Il Fornitore metterà a disposizione di OSR tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento; consentirà e contribuirà alle attività di revisione, comprese le ispezioni, realizzati da OSR o da un altro soggetto da questi indicato e appositamente delegato. A tal fine, il Fornitore informerà immediatamente OSR qualora, a suo parere, un'istruzione violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

9) Il Fornitore dichiara di aver nominato, nell'ambito della propria struttura aziendale, le persone autorizzate al trattamento dei dati personali e di aver fornito loro adeguate istruzioni scritte circa le modalità del trattamento, in ottemperanza a quanto disposto dall'art. 29 del Regolamento e dal presente mandato. A titolo esemplificativo e non esaustivo, il Fornitore dichiara di:

- consentire alle persone autorizzate l'accesso solo a quei dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- con riferimento ai trattamenti elettronici, verificare che le persone autorizzate applichino tutte le disposizioni in materia di sicurezza relativa alla custodia delle parole chiave;
- con riferimento ai trattamenti cartacei, verificare che le persone autorizzate conservino in luogo sicuro i supporti non informatici contenenti atti o documenti con dati comuni o particolari, tramite l'archiviazione degli stessi in contenitori con serratura. In particolare, i documenti contenenti dati particolari devono essere conservati in un apposito archivio ad accesso limitato;
- aver vincolato le persone autorizzate al segreto, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Fornitore, in relazione alle operazioni di trattamento da essi eseguite;
- aver nominato i soggetti a cui è delegata la gestione e la manutenzione di un impianto di elaborazione, gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi quali "Amministratore di Sistema" ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 modificato in base al provvedimento del 25 giugno 2009, in quanto applicabile. Il Fornitore, in particolare, si impegna a conservare direttamente e specificamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema, e a fornirli prontamente al Titolare su richiesta del medesimo.

10) Nel caso in cui il Fornitore riceva istanze dagli interessati per l'esercizio dei diritti di cui agli artt. 15 e 22 del Regolamento dovrà:

- darne tempestiva comunicazione scritta a OSR, allegando copia della richiesta;
- tenendo conto della natura del trattamento, assistere OSR con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo di OSR di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

11) È vietata la nomina di sub-responsabili da parte del Fornitore, in assenza di specifica autorizzazione scritta di OSR. Resta inteso che i soggetti eventualmente indicati nell'Allegato II di cui al presente Contratto si intendono espressamente autorizzati nella prestazione del Servizio.
Nel caso in cui faccia effettivo ricorso a sub-responsabili, il Fornitore si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti per mettere in atto le misure tecniche e organizzative adeguate descritte nell'Allegato IV "Misure di sicurezza" in modo tale che il trattamento soddisfi i requisiti di cui alla normativa pro tempore applicabile e garantisca la tutela dei diritti degli interessati. Il Fornitore si impegna altresì a stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili a mezzo dei quali il Fornitore descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con riferimento alla disciplina sulla protezione dei dati personali, imposti da OSR al Fornitore ai sensi del presente contratto, della normativa pro tempore vigente e degli applicabili provvedimenti speciali della competente Autorità di Controllo.
Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Fornitore riconosce di conservare nei confronti di OSR l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti, nonché si impegna a manlevare e tenere indenne OSR da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare a OSR stesso dalla mancata osservanza di tali obblighi e più in generale dalla violazione della applicabile normativa sulla tutela dei dati personali da parte del Fornitore e dei suoi sub-responsabili.
Il Fornitore si impegna altresì ad informare OSR di eventuali modifiche o sostituzioni previste riguardanti i sub-responsabili, dando così a OSR la possibilità di opporsi a tali modifiche.
OSR autorizza espressamente, altresì, il Fornitore, che a ciò si impegna, a stipulare per suo conto con eventuali sub-fornitori, quando stabiliti in un paese al di fuori dell'Unione Europea per il quale la Commissione Europea non abbia emesso un giudizio di adeguatezza del livello di protezione dei dati personali, un accordo per il trasferimento dei dati all'estero contenente le apposite clausole contrattuali

(e successive modifiche) adottate dalla stessa Commissione Europea con Decisione 2010/87/EU del 5 febbraio 2010 (di seguito: "Clausole Contrattuali Tipo") e l'Allegato IV "Misure di sicurezza" che dovrà essere inteso come Appendix 2 delle Clausole Contrattuali Tipo.

12) Il Fornitore tratterà i dati personali soltanto su istruzione documentata di OSR, anche in caso di trasferimento di dati personali verso un paese terzo al di fuori dell'Unione Europea o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Fornitore; in tal caso, il Fornitore informerà OSR circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico , e agirà conformemente a quanto previsto dagli articoli 44, 45, 46 e 49 del Regolamento.

13) OSR dichiara, inoltre, che i dati, di cui al precedente punto 1), da lui trasmessi al Fornitore:
- sono pertinenti e non eccedenti rispetto alle finalità per le quali sono stati raccolti e successivamente trattati;
- in ogni caso, i dati personali e/o le categorie particolari di dati personali, oggetto delle operazioni di trattamento affidate al Fornitore, sono raccolti e trasmessi rispettando ogni prescrizione della normativa applicabile. Resta inteso che rimane a carico di OSR l'onere di individuare la base legale del trattamento dei dati personali degli interessati.

14) Il Fornitore mette a disposizione di OSR tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente contratto e della normativa applicabile, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate da OSR o da un altro soggetto da questi appositamente designato. A tale scopo il Fornitore riconosce a OSR, e ai soggetti designati dallo stesso, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di trattamento o dove sono custoditi dati o documentazione relativa al presente contratto. In ogni caso OSR si impegna per sé e per i terzi incaricati da quest'ultimo, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per tali finalità. Il Fornitore sarà, inoltre, tenuto a comunicare tempestivamente a OSR istanze degli interessati, contestazioni, ispezioni o richieste dell'Autorità di Controllo e dalle Autorità Giudiziarie, ed ogni altra notizia rilevante in relazione al trattamento dei dati personali.

15) In caso di violazione dei dati personali, il Fornitore si impegna a informare OSR della violazione, senza ingiustificato ritardo e non al più tardi di 12 ore dal momento in cui ne ha avuto conoscenza, tramite comunicazione inviata a mezzo e-mail con oggetto "SEGNALAZIONE VIOLAZIONE DATI / DATA BREACH" e con indicazione di priorità ai seguenti indirizzi:

DPO: dpo@hsr.it e privacy.executive@hsr.it
Indirizzo del referente OSR:
aiuti.alessandro@hsr.it
tcto@hsr.it

Il Fornitore deve assistere OSR avviando un'analisi preliminare finalizzata alla raccolta dei dati concernenti l'anomalia e alla compilazione della "**Scheda Evento"** utilizzando il modello Allegato III al presente contratto, contenente tutte le informazioni raccolte:

- Data evento, anche la data presunta di avvenuta violazione (in tal caso va specificato)
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero interessati coinvolti;
- Numerosità di dati personali di cui si presume una violazione;
- Indicazione della data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza;

- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Una volta condotta l' analisi preliminare, il Fornitore deve condurre un'analisi di primo livello per verificare che la segnalazione non tratti un falso positivo; all'esito dell'accertamento il responsabile recupera le informazioni di dettaglio sull'evento necessarie alle analisi di II livello, e le riporta nella Scheda Evento che deve essere inviata via email tempestivamente e non oltre 12 ore dalla conoscenza della violazione, al proprio referente interno di OSR e al DPO di OSR che, nelle more, devono essere costantemente allineati.
L'evento deve essere inserito in un apposito registro delle violazioni.
Il Fornitore si impegna a garantire il rispetto della suddetta tempistica, nonché a manlevare e tenere indenne OSR da qualsiasi danno, pretesa, risarcimento, e/o sanzione possa derivare al OSR dalla mancata osservanza di tali obblighi.
Il Fornitore si impegna a fornire la più ampia collaborazione a OSR nonché alle Autorità di Controllo competenti e coinvolte al fine di soddisfare ogni applicabile obbligo imposto dalla normativa pro tempore applicabile (es. notifica della violazione dei dati personali all'Autorità Controllo compente; eventuale comunicazione di una violazione dei dati personali agli interessati).

16) Le comunicazioni tra le parti, ai fini del presente incarico, dovranno avvenire:
- per OSR: all'indirizzo email del DPO: dpo@hsr.it e all'indirizzo del referente OSR: aiuti.alessandro@hsr.it
- per il Fornitore: all'indirizzo email del DPO: dpo@policlinico.mi.it e all'indirizzo del referente privacy della ricerca per Policlinico: margherita.clerici@policlinico.mi.it

17) La presente nomina avrà la medesima durata dell'Accordo. Qualora questo venisse meno o perdesse efficacia, qualsiasi ne sia il motivo, anche la presente nomina verrà automaticamente meno senza bisogno di comunicazioni o revoche, ed il Responsabile non sarà più legittimato a trattare i dati del Titolare.

18) Al termine delle operazioni di trattamento o alla cessazione dell'Accordo, per qualsiasi causa siano esse dovute, il Fornitore sarà tenuto, a discrezione di OSR, a:
(i) restituire a OSR i dati personali oggetti del trattamento; oppure
(ii) provvedere alla loro integrale distruzione
salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge o altri fini (contabili, fiscali, ecc.), dandone immediata comunicazione a OSR. Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.

19) Ai sensi dell'art 30 del Regolamento, il Fornitore si impegna a tenere un registro relativo a tutte le categorie di attività di trattamento svolte per conto di OSR, in cui siano riportate le seguenti voci:
- nome e dati di contatto del Responsabile, del Titolare e, se nominato, del relativo responsabile della protezione dei dati;
- le categorie dei trattamenti effettuati per conto di OSR;
- gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del Regolamento, la documentazione delle garanzie adeguate;
- una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del Regolamento.

20) Resta inteso che la presente nomina non comporta alcun diritto del Fornitore ad uno specifico compenso e/o indennità e/o rimborso derivante dalla nomina medesima.

Con la presente nomina si intende espressamente revocare e sostituire ogni altra eventuale nomina per qualsivoglia tipologia di dati.

Si allega

- ALLEGATO I “DESCRIZIONE DELLE ATTIVITÀ DI TRATTAMENTO”
- ALLEGATO II “SUB-RESPONSABILI”
- ALLEGATO III “SCHEDA EVENTO”
- ALLEGATO IV “MISURE DI SICUREZZA”

Luogo, data: _____

Per Ospedale San Raffaele
per il Responsabile

_____

L’AMMINISTRATORE UNICO
Ing. Marco Centenari

Per accettazione dell’incarico a Responsabile

_____

Il DIRETTORE SCIENTIFICO
Prof. Fabio Blandini

Per specifica accettazione del mandato conferito ai sensi dell’art.1704 Codice civile alla nomina da parte del Fornitore di altri responsabili ai sensi dell’art. 28, c.2, del Regolamento.

per il Responsabile
Per accettazione

_____

Direttore Scientifico
Prof. Fabio Blandini

ALLEGATO I
Descrizione delle attività di trattamento

Categorie di interessati
- Il personale OSR impegnato a qualsiasi titolo nelle attività relative al Progetto
- I soggetti che in qualità di pazienti partecipano al Progetto

Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati)
- Dati Comuni: anagrafici e di contatto;
- Dati Particolari: clinici, demografici (per es. peso ecc.) relativi allo stato di salute (la patologia specifica di cui è affetto il paziente)

Natura e finalità del trattamento
- Il trattamento dei Dati effettuato nell'ambito del contratto è necessario per condurre la sperimentazione clinica in oggetto.
- In particolare, i pazienti coinvolti nel Progetto dovranno eseguire una valutazione epatologica presso la controparte
- Per l'esecuzione di tali attività il Policlinico di Milano avrà accesso, utilizzerà e conserverà, nei tempi e nei modi contrattualmente convenuti, Dati Comuni e Particolari dei pazienti
- Le attività affidate alla controparte comportano che quest'ultima tratti, per conto dei Titolari, ai Dati comuni del personale amministrativo e operativo coinvolto.

ALLEGATO II
Sub Responsabili

Il Responsabile è autorizzato a sub-appaltare parte delle operazioni di trattamento ai seguenti sub-responsabili (siano essi o meno appartenenti al Gruppo del Responsabile)

La seguente tabella mappa i sub-responsabili ingaggiati dal Responsabile.

Elenco Nominativo Sub-responsabili utilizzati dal Responsabile	Il Sub-Responsabile ha collocati i server di produzione in area EXTRA-UE? (SI/NO, in caso affermativo specificare dove)	Il Sub-Responsabile ha collocati i server di backup in area EXTRA-UE? (SI/NO, in caso affermativo specificare dove)
n/a	n/a	n/a

Restano esclusi i servizi non forniti dal Responsabile e soggetti a separati accordi tra il Sub-responsabile e il Titolare.

La tabella dei sub-responsabili verrà aggiornata di volta in volta e il Titolare verrà notificato di conseguenza in modo che possa opporsi all'impiego di nuovi sub-responsabili.

ALLEGATO III
Scheda evento

[NR. PROGRESSIVO della scheda Es. 1/2018, 2/2018 etc.]	SCHEDA EVENTO
	Azienda coinvolta (specificare se in qualità di titolare o come responsabile di aziende terze)
1	Data e ora in cui si è avuto conoscenza della violazione;
2	Fonte di segnalazione
3	Tipologia evento anomalo
4	Data evento e ora della violazione anche solo presunta (specificando se è presunta);
5	Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

6	Descrizione evento anomalo
7	Numero interessati coinvolti (se noto)
8	Numero dei dati personali di cui si presume la violazione
9	Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Allegato IV
MISURE DI SICUREZZA

Nella tabella di seguito riportata vengono descritti gli obiettivi di controllo che il Responsabile deve garantire, individuati sulla base della metodologia ISO/IEC 27001:2013.
Al Responsabile (di seguito anche "l'organizzazione") è richiesto l'adempimento degli obiettivi di controllo indicati e la capacità di fornire evidenza della conformità agli stessi.
Nel caso in cui il Responsabile non sia in grado di soddisfare in tutto o in parte un obiettivo di controllo è tenuto a comunicarlo al Titolare fornendo i necessari razionali e informazioni ed evidenza degli eventuali controlli compensativi rilevanti.
In caso di ricorso a fornitori (sub-responsabili) per la gestione dei servizi informatici e di sicurezza, l'applicazione delle misure sotto descritte dovrà essere traferita contrattualmente al fornitore stesso.

ID	CATEGORIA DELLA MISURA	DESCRIZIONE
A.5	Security policy	L'organizzazione deve documentare la propria politica per quanto riguarda l'elaborazione dei dati personali come parte della politica di sicurezza informatica, contenente una o più sezioni specifiche per il trattamento di dati personali. La politica di sicurezza deve essere riesaminata e riveduta, se necessario, su base annua. La politica di sicurezza deve almeno riferirsi a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili dei dati o altre terze parti coinvolte nel trattamento di dati personali. La politica deve essere approvata dalla direzione e comunicata a tutti i dipendenti e alle parti esterne pertinenti
A.6.1.1	Information security roles and responsibilities	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le regole di sicurezza. Durante le re-organizzazioni interne o le cessazioni dei rapporti di lavoro o la modifica anche temporanea della mansione, la revoca dei diritti e delle responsabilità e le rispettive autorizzazioni devono essere definite chiaramente. Deve essere effettuata una chiara nomina dei responsabili aventi specifici compiti di sicurezza.
A.6.1.1		Deve essere identificato un responsabile della sicurezza delle informazioni, a cui devono essere comunicati i relativi compiti e responsabilità. Ove applicabile/possibile devono essere evitati conflitti di responsabilità, ad esempio, tra responsabile della sicurezza e DPO.
A.9.1.1	Access control policy	Autorizzazioni specifiche per il controllo dell'accesso ai dati devono essere assegnate a ciascun ruolo (coinvolto nel trattamento dei dati personali) in seguito alla necessità del rispetto del principio del "need to know". I criteri di controllo accesso devono essere dettagliati e documentati. L'organizzazione deve determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per ruoli utente specifici verso i processi e le procedure relative ai dati personali. Il principio della "Segregation of Duty" (ad es. richiesta di accesso, autorizzazione di accesso, amministrazione dell'accesso) deve essere chiaramente definito e documentato.
A.9.1.1		L'azienda, ed i relativi fornitori / responsabili al trattamento, deve essere conforme al c.d. "Provvedimento Amministratori di Sistema" (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008) del Garante per la Protezione dei Dati Personali.
A.8	Asset management	L'organizzazione deve avere un registro delle risorse informatiche utilizzate per l'elaborazione dei dati personali (hardware, software e rete). Il registro deve includere almeno le seguenti informazioni: risorsa IT, tipo (ad esempio server, workstation), posizione (fisico o elettronico). A una persona specifica deve essere assegnato il compito di mantenere e aggiornare il registro (ad es. responsabile IT). Il registro deve essere aggiornato almeno annualmente.

A. 12.1	Operational procedures and responsibilities	L'organizzazione deve assicurare che tutte le modifiche apportate al sistema informativo siano registrate e monitorate da una persona specifica (ad es. IT o Security Officer). Deve essere svolto un controllo periodico di questo processo. Lo sviluppo del software deve essere eseguito in una ambiente speciale che non è collegato al sistema informatico utilizzato per l'elaborazione dei dati personali. Quando è necessario il test, i dati fittizi devono essere utilizzati (non dati reali). Nei casi in cui ciò non sia possibile, devono essere in vigore procedure specifiche di protezione dei dati personali utilizzati nelle prove. Deve essere definita una politica per la gestione dei cambiamenti che deve includere: un processo per l'introduzione di modifiche, i ruoli/utenti che hanno diritti di cambiamento, Timeline per l'introduzione di modifiche. La politica deve essere aggiornata regolarmente.
A.15	Supplier relationships	Linee guida e procedure formali relative al trattamento dei dati personali del Titolare da parte di subfornitori devono essere formalmente definite, documentate e concordate tra il fornitore e i suoi subfornitori prima dell'inizio del trattamento dei dati del titolare. Queste linee guida e procedure devono obbligatoriamente stabilire lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione. I dipendenti del fornitore del trattamento che elaborano i dati personali del Titolare devono essere soggetti a specifici accordi di confidenzialità/non divulgazione. In particolare, nel caso di una violazione dei dati personali in carico al subfornitore, il subfornitore deve informare il fornitore, e questi il Titolare del trattamento senza indebito ritardo.
A.16	Information security incident management	Deve essere definito e documentato un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali. Il piano deve assicurare che le violazioni dei dati personali devono essere immediatamente segnalate alla direzione del fornitore, ed al Titolare entro gli accordi contrattualizzati.
A.16		Incidenti e violazioni dei dati personali devono essere registrate insieme ai dettagli relativi all'evento e alle successive azioni di attenuazione eseguite.
A. 17	Information security aspects of business continuity management	L'organizzazione deve stabilire le principali procedure e i controlli da seguire per garantire il livello di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di violazione dei dati personali/incidenti).
A. 17		Deve essere dettagliato e documentato un Piano di Continuità operativa che preveda azioni ben definite e l'assegnazione dei ruoli. Nel piano deve essere definito un livello di qualità del servizio per i processi aziendali di base che forniscono la protezione dei dati personali. Deve essere identificato e nominato personale specifico con la responsabilità necessaria, l'autorità e la competenza per gestire la continuità aziendale in caso di incidente/violazione dei dati personali. Una struttura alternativa deve essere considerata, a seconda dell'organizzazione e del tempo di inattività accettabile del sistema IT.
A. 7	Human resource security	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere comunicati chiaramente durante il processo di selezione o di incarico dei dipendenti e collaboratori. L'organizzazione deve garantire che tutti i dipendenti comprendano le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. Prima iniziare il rapporto di lavoro ai dipendenti deve essere chiesto di prendere visione del documento o della politica di sicurezza dell'organizzazione e di firmare i rispettivi accordi di riservatezza e di non divulgazione. Prima iniziare il rapporto di lavoro ai dipendenti e collaboratori deve essere chiesto di prendere visione della politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione.
A. 7		I dipendenti coinvolti nel trattamento ad alto rischio dei dati personali devono essere vincolati a specifiche clausole di riservatezza (nel loro contratto di lavoro o altro atto legale).
A.7.2.2	Information security awareness, education and training	L'organizzazione deve garantire che tutti i dipendenti siano adeguatamente informati sulle misure di sicurezza a cui i sistemi su cui operano sono sottoposti, sui requisiti di protezione dei dati e sugli obblighi legali.
A.7.2.2		L'organizzazione deve avere programmi di formazione e sensibilizzazione strutturati e regolari per il personale, compresi programmi specifici relativi alla protezione dei dati per i neoassunti. Il piano di formazione deve essere preparato ed eseguito su base annua, o con altra periodicità ritenuta adeguata.

A.9	Access control	Deve essere implementato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema deve consentire di creare, approvare, rivedere ed eliminare gli account utente. Devono essere definiti account nominativi per ogni persona che accede a dati personali, incluso il personale IT, con permessi per l'accesso alle sole informazioni necessarie. L'utilizzo di account utente comuni (c.d. account di gruppo), anche da parte del personale IT, deve essere evitato. Nei casi in cui ciò sia necessario, occorre garantire che tutti gli utenti del gruppo abbiano gli stessi ruoli e responsabilità. Deve essere predisposto un meccanismo di autenticazione, consentendo l'accesso al sistema IT sulla base della politica di controllo accessi e sul sistema. Come minimo deve essere utilizzata una combinazione nome utente/password. Le password devono rispettare un adeguato livello di complessità, definito nelle regole aziendali, comprendente una lunghezza di almeno otto caratteri, salvo dove non sia tecnicamente fattibile. Le password utente devono registrate mediante tecniche di Hashing o altro meccanismo di protezione analogamente robusto.
A.9		Deve essere definito e documentato un criterio di complessità delle password specifico e configurabile. I criteri devono includere almeno la lunghezza della password, la complessità, il periodo di validità, nonché il numero di tentativi di accesso non riusciti accettabili. Il sistema di controllo accessi deve avere la capacità di rilevare e non consentire l'utilizzo di password che non rispettano il livello di complessità previsto.
A.9		L'accesso deve avvenire da dispositivi riconosciuti, presso sedi presidiate dal responsabile o dal titolare, o comunque da ambienti di cui il responsabile o il titolare possano garantire la rispondenza a criteri di sicurezza adeguati In caso di accesso a sistemi utilizzati per il trattamento di dati genetici o che siano stati qualificati come ""a maggior tutela"", l'accesso deve avvenire mediante autenticazione a due fattori, realizzata in linea con le buone pratiche di settore.
A.12.4	Logging and monitoring	I file di log devono essere attivati per ogni sistema/applicazione utilizzato per l'elaborazione dei dati personali. Le registrazioni devono essere marcate temporalmente e adeguatamente protette da manomissioni e accessi non autorizzati. Gli orologi devono essere sincronizzati con un'unica sorgente di tempo di riferimento (es. NTP server). Devono essere attivati i log secondo modalità conformi al Provvedimento Amministratori di Sistema, dove applicabile.
A.12.4		Non deve esserci possibilità di cancellazione o modifica del contenuto dei file di log. L'accesso ai file di log deve inoltre essere registrato per consentire di rilevare l'attività insolita.
A.12.4		"Il log devono includere tutti i tipi di accesso ai dati (vista, modifica, cancellazione). Un sistema di monitoraggio deve elaborare i file di log e produrre report sullo stato del sistema e notificare eventuali anomalie.
A. 12	Operations security	I database e le applicazioni devono essere configurati per operare utilizzando un account specifico e con i privilegi di accesso minimi al sistema operativo per permettere il corretto funzionamento. I database e le applicazioni devono elaborare solo i dati personali effettivamente necessari per il tipo di trattamento per il quale sono utilizzati.
A. 12		Per i file, record o campi più critici devono essere previste soluzioni di cifratura.
A. 12		Deve essere prevista la cifratura delle unità d'archiviazione sulle quali sono presenti dati personali, quali dischi rigidi (HD), in particolare dei personal computer e laptop, dischi e chiavette USB, DVD ecc.
A. 12		Per i file, record o campi più critici devono essere previste soluzioni di pseudonimizzazione, attraverso la separazione dei dati personali dai dati identificativi della persona fisica in modo da non consentirne l'identificazione senza informazioni aggiuntive.
A. 12		Deve essere considerata l'adozione di tecniche di supporto alla privacy a livello di database, come ad esempio le query autorizzate, crittografia ricercabile, ecc.
A. 14.1	Security requirements of information systems	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza. Le applicazioni antivirus e le firme di rilevamento devono essere aggiornate secondo le specifiche del fornitore e comunque verificate almeno giornalmente. I sistemi devono avere un time-out di sessione quando l'utente non è attivo per un determinato periodo di tempo (al più 30 minuti). Devono essere ottenute informazioni sulle vulnerabilità di sicurezza dei sistemi informativi

		utilizzati. Gli aggiornamenti di sicurezza critici rilasciati relativamente ai componenti infrastrutturali, ai sistemi operativi ed alle applicazioni più critiche devono essere installati regolarmente e secondo un processo definito che identifichi e garantisca tempi certi. Le workstation utilizzate per il trattamento dei dati personali non devono essere connesse a Internet, a meno che non siano in vigore misure di sicurezza atte ad impedire l'elaborazione, la copia e il trasferimento non autorizzati di dati personali verso internet (firewall, firewall personali gestiti centralmente ecc.).
A. 14.1		Gli utenti non devono disporre di privilegi per installare o disattivare applicazioni software non autorizzate.
A. 14.1		Gli utenti non devono poter trasferire i dati personali dalle postazioni di lavoro ai dispositivi di memorizzazione esterni (ad esempio USB, DVD, dischi rigidi esterni).
A.13	Communications Security	Tutte le comunicazioni attraverso Internet che prevedano l'autenticazione con le credenziali degli utenti o il trasferimento di dati personali devono essere protette tramite protocolli crittografici (ad esempio TLS/SSL). L'accesso wireless al sistema IT deve essere consentito solo per utenti e processi identificati e deve essere protetto mediante cifratura WPA2 o superiore. Il traffico da e verso il sistema informativo deve essere protetto e monitorato mediante dispositivi opportuni (ad esempio firewall o sistema di rilevamento delle intrusioni). L'accesso da remoto ai servizi interni a supporto del trattamento di dati personali deve avvenire attraverso VPN autorizzate, autenticate e monitorate da personale specificamente incaricato.
A.13		La rete dei sistemi a supporto dei trattamenti di dati personali a maggiore criticità deve essere segregata fisicamente o logicamente dalle altre reti. L'accesso a tale rete deve essere consentito utilizzando tecniche come il Mac/IP filtering o controllo di accesso alla rete (NAC). Devono inoltre essere adottati sistemi di intrusion detection.
A.12.3	Back-Up	Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente legate a ruoli e responsabilità. Ai backup deve essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati originari. L'esecuzione dei backup deve essere monitorata per garantirne la completezza. Backup completi (c.d. full) devono essere eseguiti regolarmente.
A.12.3		I supporti di backup devono essere testati regolarmente per assicurarsi che possano essere utilizzati in caso di emergenza. I backup incrementali pianificati devono essere effettuati almeno su base giornaliera. Le copie del backup devono essere archiviate in modo sicuro in luoghi diversi rispetto a dove si trovano i dati originali.
A.12.3		Nel caso in cui venga utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa. Le copie dei backup devono essere crittografate e archiviate in modo sicuro anche offline.
A. 6.2	Mobile devices and teleworking	Devono essere definite e documentate delle policy e procedure per la gestione e l'uso corretto dei dispositivi mobili, comprendenti l'utilizzo o meno di dispositivi personali e l'utilizzo di dispositivi aziendali per usi personali. Per poter accedere ai sistemi e servizi a supporto del trattamento di dati personali, i dispositivi mobili devono essere preregistrati e pre-autorizzati. L'accesso ai servizi e sistemi attraverso dispositivi mobili deve essere soggetto agli stessi livelli di controllo accesso utilizzati per le postazioni fisse. In particolare, l'accesso al dispositivo mobile deve avvenire almeno tramite password. I dispositivi mobili devono essere protetti fisicamente contro il furto quando non sono in uso.
A. 6.2		Devono essere chiaramente definiti ruoli specifici e responsabilità per quanto riguarda la gestione dei dispositivi mobili. L'organizzazione deve essere in grado di cancellare in remoto i dati personali (relativi alla sua operazione di elaborazione) su un cellulare o dispositivo che è stato compromesso.
A. 6.2		I dispositivi mobili devono supportare la separazione dell'uso privato e aziendale del dispositivo tramite contenitori software protetti (es. MDM)
A. 6.2		Deve essere prevista l'autenticazione a due fattori per i dispositivi mobili Dati personali memorizzati sul cellulare devono essere crittografati.
A.12.6 & A.14.2	Technical vulnerability management &	Nel processo di sviluppo di sistemi e servizi a supporto del trattamento di dati personali, devono essere adottati standard e buone pratiche di settore, che prevedano fra l'altro la chiara identificazione dei requisiti di protezione specifici al trattamento, in linea con i principi di

	Security in development and support processes	data protection by design & by default, e prevedendo l'utilizzo di tecnologie e tecniche specifiche progettate per sostenere la segretezza e la protezione dei dati (Privacy enhancing technology). Devono essere seguite norme e pratiche di sviluppo sicuro. I requisiti di sicurezza iniziali devono essere validati e testati prima del rilascio in produzione.
A.12.6 & A.14.2		Devono essere ottenute informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati.
A.12.6 & A.14.2		Prima dell'inizio del trattamento devono essere effettuati da parte di terze parti attendibili, adeguati Vulnerability Assessment e Penetration test delle applicazioni e delle infrastrutture. Il trattamento non deve iniziare a meno che il livello di sicurezza richiesto non sia raggiunto. Devono essere pianificati Vulneability Assessment e Penetration Test periodici sugli ambienti di produzione rilevanti. Le patch software devono essere testate e valutate prima di essere installate in produzione.
A. 8.3.2 & A. 11.2.7	Disposal of media & Secure disposal or reuse of equipment	Tutti i supporti di memorizzazione, compresi i dispositivi di memorizzazione portatili, devono essere sottoposti a cancellazione sicura, ad esempio mediante sovrascrittura, prima di essere dismessi, salvo quando sia garantito che tutti i dati personali presenti siano cifrati in modo da non permettere il recupero dei dati. Qualora questo non fosse possibile, i supporti devono essere fisicamente distrutti in modo da non permettere il recupero dei dati. La cancellazione sicura deve essere eseguita su tutti i supporti prima della loro eliminazione. Nei casi in cui questo non è possibile la distruzione fisica deve essere eseguita. Devono essere predisposti strumenti e procedure per la distruzione fisica della carta.
A. 8.3.2 & A. 11.2.7		Se sono utilizzati servizi di terze parti per eliminare in modo sicuro i documenti multimediali o cartacei, deve essere in vigore un contratto di servizio e deve essere prodotto un log di distruzione dei documenti.
A. 8.3.2 & A. 11.2.7		Se sono utilizzati servizi di terze parti per la distruzione di file multimediali o cartacei a supporto del trattamento di dati personali ad alto rischio, occorre prevedere che il processo venga eseguito presso la sede del Titolare o Responsabile del trattamento (ed evitare il trasferimento di dati personali)
A.11	Physical and environmental security	Il perimetro fisico dell'infrastruttura del sistema IT non deve essere accessibile da personale non autorizzato.
A.11		Presso i datacenter devono essere previste dotazioni anti-incendio, antiallagamento, di controllo della temperatura e di continuità del servizio elettrico (es. UPS).
A.11		Le zone sicure devono essere definite e protette da opportuni controlli di ingresso. Un registro cartaceo o elettronico di tutti gli accessi deve essere mantenuto e monitorato Sistemi di rilevazione delle intrusioni e un sistema di videosorveglianza devono essere installati in tutte le zone sicure Adeguate barriere fisiche devono, se del caso, essere costruite per impedire l'accesso fisico non autorizzato. Le aree sicure al di fuori del data center devono essere fisicamente protette e riviste periodicamente
A.11		I documenti, gli archivi cartacei e i supporti di memorizzazione devono essere protetti da misure fisiche quando non utilizzati (es. armadi chiusi a chiave)
A.11		Tutto il personale ed i visitatori che accedono ai locali dell'organizzazione dove sono trattati dati personali devono essere identificati attraverso i mezzi adatti, per esempio tramite l'uso di badge.