# Convenzione tra l'ASST Grande Ospedale Metropolitano Niguarda e la Fondazione IRCCS Ca' Granda "Ospedale Maggiore Policlinico" di Milano per prestazioni di chirurgia plastica

**TRA**



**L'ASST Grande Ospedale Metropolitano Niguarda** (di seguito indicata come **"ASST Niguarda"**), con sede in Milano, Piazza Ospedale Maggiore 3 - codice fiscale e partita IVA 09315660960, rappresentata dal Direttore Generale **Dott. Alberto Zoli**

**E**

la **Fondazione IRCCS Ca' Granda "Ospedale Maggiore Policlinico" di Milano** (di seguito indicata come **"Fondazione"**) con sede in Milano, Via Francesco Sforza n. 28, codice fiscale n. 04724150968, nella persona del Direttore Generale **Dott. Matteo Stocco**.

**PREMESSO CHE**

- la Fondazione ha manifestato con nota pec 18594U del 08/05/2025, la necessità di rinnovare la convenzione avente ad oggetto prestazioni medico-specialistiche di chirurgia plastica da svolgersi in favore dei propri pazienti ricoverati affetti da infezioni necrotizzanti dei tessuti molli e gravi infezioni di ferita;

- l'ASST Niguarda avvalendosi della propra S.C. Centro Ustioni e Chirurgia Plastica Ricostruttiva, possiede le competenze e le professionalità necessarie a poter soddisfare tali esigenze ed è disponibile a garantire, dietro corrispettivo, le prestazioni richieste per il tramite dei propri dirigenti medici a rapporto di lavoro esclusivo ex art. 15-*quinquies* del D. Lgs. 502/1992 e s.m.i.;

- l'art. 15 della legge n. 241/1990 stabilisce che le amministrazioni pubbliche possono concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune e che per tali accordi si osservano, in quanto applicabili, le disposizioni previste dall'art.11, commi 2 e 3 della medesima legge;

- l'art. 1, commi 2 e 3, della Legge Regionale n. 30/2006, e s.m.i., al fine di contribuire alla realizzazione degli obiettivi della programmazione regionale ed al raggiungimento degli obiettivi di finanza pubblica mediante il contenimento e la razionalizzazione della spesa, nonché al fine di garantire la valorizzazione degli investimenti, prevede la possibilità che gli enti appartenenti al Sistema Regionale, tra i quali sono ricompresi anche gli enti del Servizio Sanitario Regionale, possano svolgere tra loro le prestazioni dirette alla produzione di beni e servizi mediante la stipula di apposite convenzioni che regolino i rapporti reciproci, con riguardo alla disciplina dei servizi relativi al personale appartenente ai soggetti del Sistema, nonché alla produzione di beni e servizi strumentali alle rispettive attività;

- la convenzione viene stipulata secondo quanto previsto dall'art. 91 comma 2 del C.C.N.L dell'Area della Sanità triennio 2019-2021 sottoscritto in data 23/01/2024;

**SI CONVIENE E STIPULA QUANTO SEGUE:**

## Art. 1 - Oggetto della convenzione e compensi

La presente convenzione ha per oggetto lo svolgimento di consulenze di chirurgia plastica ed eventuali interventi a favore di pazienti della Fondazione affetti da infezioni necrotizzanti dei tessuti molli e gravi infezioni di ferita per mezzo di:

- consulenze specialistiche di chirurgia plastica;
- accessi per esecuzione di interventi chirurgici di chirurgia plastica.

Per le attività di cui sopra verrà applicata la seguente tariffazione:

- consulenza specialistica di chirurgia plastica → € 250,00 ;
- esecuzione di intervento chirurgico di chirurgia plastica → € 500,00.

Laddove venga richiesta l'esecuzione di consulenza e di intervento nella medesima giornata, verranno fatturate entrambe le prestazioni.

**Art. 2 - Modalità operative**

La Fondazione si impegna a concordare direttamente con il direttore della struttura sanitaria dell'ASST Niguarda o di un suo delegato, con congruo preavviso la data di accesso alla propria sede e le prestazioni da effettuare.

**Art. 3 - Doveri dell'ASST Niguarda**

L'ASST Niguarda, sotto la responsabilità del direttore della S.C. Centro Ustioni e Chirurgia Plastica Ricostruttiva, avvalendosi dei propri dirigenti medici si impegna a garantire le attività richieste salvaguardando gli impegni e le attività istituzionali, così come previsto dalle norme vigenti. L'attività verrà effettuata **fuori orario di servizio.**

**Art. 4 - Doveri della Fondazione**

La Fondazione si impegna al rispetto di quanto indicato dalla presente convenzione nei confronti di terzi e garantirà la corretta gestione, in termini di privacy, dell'esito degli esami effettuati dell'ASST Niguarda concordando con il Direttore della S.C. interessata le modalità ritenute più idonee in merito.

**Art. 5 - Rendicontazione e fatturazione**

Tutti i rapporti di carattere amministrativo, economico e finanziario, connessi con l'espletamento delle prestazioni, oggetto della presente convenzione, intercorrono esclusivamente fra le amministrazioni dell'ASST Niguarda e della Fondazione.

Con riferimento alle modalità di emissione delle fatture da parte dell'ASST Niguarda, secondo quanto previsto dalla legge di bilancio 2018 (L. 205 del 27/12/2017) in materia di emissione e trasmissione degli Ordini elettronici, la Fondazione, appartenendo al Sistema Sociosanitario Lombardo dichiara di adeguarsi alle Linee guida regionali v2.0 del 30.06.2021 (par. 8.2 Ordini elettronici relativi a partite intercompany) pertanto, trasmetterà all'ASST Niguarda, tramite il Nodo Smistamento degli ordini NSO, gli ordini di acquisto in formato elettronico. L'ordine, dovrà essere esclusivamente **un ordine a budget annuale o in alternativa un ordine a convalida** successivo all'emissione della fattura.

Nel caso in cui l'ASST Niguarda emetta fatture senza l'indicazione dell'ordine, per mancata generazione dello stesso da parte della Fondazione, esse non potranno essere rifiutate come riportato nella nota di Regione Lombardia del 5 dicembre 2022 prot. A1.2022.00996023.

Il pagamento delle prestazioni rese dovrà essere effettuato entro e non oltre 60 giorni dalla data di emissione della fattura.
Il mancato rispetto dei termini sopra indicati comporterà l'applicazione degli interessi moratori, non superiori al tasso legale nel tempo in vigore, oltre alla richiesta di rimborso dei costi sostenuti per il recupero delle somme non tempestivamente corrisposte ai sensi di quanto stabilito dal D.lgs. 231/2002 fatta salva la facoltà di recesso anticipato dalla convenzione con preavviso di 30 giorni, da comunicare anche all'indirizzo mail protocollo@pec.policlinico.mi.it.

**Art. 6 – Durata, rinnovo, disdetta e revisione convenzione**

Il presente accordo ha durata **dalla data di sottoscrizione** fino al **31/12/2027**.

Le parti convengono che, nelle more del perfezionamento degli atti amministrativi, i pregressi rapporti verranno regolati, ai sensi del presente accordo, a partire dal 09/05/2025.

La convenzione potrà essere rinnovata per iscritto, mediante formale richiesta su carta intestata firmata dal legale rappresentante, da inviare all'indirizzo e-mail convenzioni@ospedaleniguarda.it della SS Area Privata, oppure tramite posta elettronica certificata.

La richiesta di rinnovo dovrà essere trasmessa almeno 60 giorni prima della scadenza. Non ricevendo alcuna richiesta entro tale data l'ASST Niguarda potrà non garantire il rinnovo della convenzione stessa.

La presente convenzione potrà essere disdettata in ogni momento, purché notificata tra le parti a mezzo posta elettronica certificata con preavviso di 30 giorni, fermo restando che la stessa si intenderà immediatamente risolta qualora sopravvenissero nuove disposizioni di leggi statali, regionali, regolamentari, ovvero esigenze di servizio improrogabili e con essa incompatibili.

L'ASST Niguarda si riserva la facoltà di disdetta anche nel caso di ritardato pagamento del corrispettivo secondo quanto stabilito nell'articolo 5.

Qualora tuttavia, in corso di vigenza, si rendesse necessario procedere alla revisione delle specifiche condizioni operative ed economiche o all'integrazione con nuove prestazioni, sarà necessario trasmettere una nota formale di richiesta e si procederà alla stipula di nuova convenzione o di atto integrativo.

## Art. 7 - Assicurazione

L'ASST Niguarda, in relazione alla presente convenzione, garantisce al personale dipendente interessato le tutele previste dalla normativa vigente e dalla contrattazione collettiva nella formulazione in essere alla data di sottoscrizione della stessa.

## Art. 8 – Trattamento dei dati

Le parti convengono che per l'esecuzione della convenzione la controparte, nella persona del legale rappresentante pro tempore, è nominato "Responsabile esterno del Trattamento".

Le Parti convengono che il Responsabile è in possesso di adeguate competenze tecniche e know-how circa gli scopi e le modalità di trattamento dei dati personali, delle misure di sicurezza da adottare al fine di garantire la riservatezza, la completezza e l'integrità dei dati personali trattati, nonché circa le norme che disciplinano la protezione dei dati personali.

Le modalità e le istruzioni per il trattamento dei dati personali impartite dal Titolare al Responsabile costituiscono parte integrante della presente Convenzione (Allegato 1).
Resta inteso che il Titolare ha facoltà di modificare, sostituire o aggiungere istruzioni di trattamento per tutta la durata del trattamento dei dati personali.
Le istruzioni saranno sempre documentate e rese per iscritto, anche tramite supporto elettronico.
Laddove le esigenze contingenti richiedano forma diversa, le istruzioni trasmesse verbalmente o telefonicamente saranno oggetto di formalizzazione scritta non appena possibile.
Qualora le istruzioni fornite siano, a parere del Responsabile, in contrasto con il GDPR o altre disposizioni nazionali ed europee in materia di protezione dei dati personali, il Responsabile dovrà immediatamente informare il Titolare.

Il Responsabile si impegna ad uniformarsi alle disposizioni del GDPR, nonché ad ogni altra disposizione normativa in materia di trattamento dei dati personali attualmente in vigore e/o che venga a modificare, integrare o sostituire l'attuale disciplina.

Nello svolgimento delle attività di trattamento oggetto, il Responsabile tratta i dati personali nella misura funzionale alla prestazione delle attività oggetto della Convenzione e adotta tutte le misure opportune ai sensi dell'art. 32 GDPR.

Il Responsabile garantisce che il personale da esso impiegato è vincolato alla confidenzialità e che lo stesso è formalmente autorizzato al trattamento dei dati personali necessari per l'esecuzione delle attività di cui alla Convenzione e puntualmente istruito sulle modalità di esecuzione di tali attività.

Salva l'eventuale nomina di Sub-responsabili, il Responsabile si impegna a non comunicare a terzi né a diffondere per qualsiasi ragione i dati personali senza l'autorizzazione del Titolare, a meno che tale comunicazione non sia necessaria per adempiere obblighi di legge o per ottemperare a un ordine dell'autorità. In tali ipotesi, il Responsabile avviserà tempestivamente per iscritto il Titolare prima di ottemperare a qualsiasi richiesta di comunicazione, salvo che al Responsabile sia proibito da disposizioni normative vigenti.

Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR, anche tramite ispezioni realizzate dal Titolare o da altro soggetto da questi incaricato. A tale scopo il Responsabile riconosce al Titolare, e agli incaricati dal medesimo, il diritto di accedere a locali di pertinenza del Responsabile, supportato e accompagnato dal personale indicato dal Responsabile, ove hanno svolgimento le operazioni di trattamento. Tali ispezioni potranno aver luogo a seguito di comunicazione da parte del Titolare da inviare con un preavviso di almeno cinque giorni lavorativi.

Il Responsabile si impegna collaborare con il Titolare nel rispondere alle richieste dell'Autorità competente.
Il Responsabile si obbliga, altresì, a prestare assistenza al Titolare, nel garantire il rispetto degli obblighi previsti dagli artt. 33 (Notifica di una violazione dei dati personali all'Autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato) e 35 (Valutazione di impatto sulla protezione dei dati – al riguardo, si rimanda alla sezione 2 al presente accordo) GDPR, tenendo conto della natura del trattamento e delle informazioni di cui ha la disponibilità.
Il Responsabile si impegna a prestare la propria collaborazione per agevolare i Titolari del Trattamento nel garantire il soddisfacimento dei diritti riconosciuti agli interessati dagli artt. 15 – 22 GDPR.

Il Responsabile mette a disposizione del Titolare l'estratto del Registro dei trattamenti ex art. 30 GDPR relativo ai trattamenti eseguiti su sua istruzione.

È fatto divieto al Responsabile di utilizzare, consultare, accedere o porre in essere qualsiasi altro trattamento dei dati personali di cui viene a conoscenza per finalità ulteriori e diverse rispetto a quelle relative al rapporto contrattuale con il Titolare.
Per i trattamenti concernenti dati personali che esulano dall'ambito della presente Convenzione, Titolare e Responsabile danno atto e convengono che ognuna agisce in qualità di autonomo Titolare e sotto la propria distinta responsabilità.

Il Responsabile dichiara di avere una struttura ed una organizzazione adeguata all'esecuzione dell'incarico di trattamento dei dati personali correlato alla presente Convenzione e si impegna ad adeguarla ovvero a mantenerla adeguata alle necessità dell'incarico stesso, garantendo il pieno rispetto (con riguardo ai propri dipendenti ed ai collaboratori interni ed esterni) delle istruzioni sul trattamento dei dati.

Il Responsabile è autorizzato a nominare ulteriori Responsabili del trattamento dei dati personali per l'esecuzione dei trattamenti oggetto del presente accordo e si impegna, altresì, a comunicare immediatamente al Titolare il nome di eventuali ulteriori fornitori di cui intenda avvalersi nell'espletamento dell'incarico ai fini dell'esercizio del diritto di opposizione, che potrà essere comunicata anche a mezzo di posta elettronica.
Il Titolare si riserva il diritto di verificare i Sub-Responsabili e di esercitare il proprio diritto di opposizione qualora i soggetti designati non appaiano in grado di garantire il rispetto della normativa vigente e degli obblighi assunti dal Responsabile.
Il Responsabile si obbliga altresì ad individuare tali operatori tra i soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e venga altresì garantita la tutela dei diritti dell'interessato.
Il Responsabile si obbliga inoltre a stipulare con tali operatori un accordo scritto atto a garantire un grado di protezione pari a quello proprio delle disposizioni della presente Convenzione, con particolare attenzione al diritto di ispezione e verifica, nonché a verificare il rispetto delle prescrizioni in oggetto ed a fornire al Titolare evidenza delle verifiche condotte, su richiesta, ex art. 28, paragrafo 1, GDPR.

Il Responsabile, anche nell'ambito dei sub-affidamenti, non può trasferire i dati personali oggetto dei trattamenti verso le destinazioni di cui all'articolo 44 GDPR senza l'autorizzazione espressa e preventiva del Titolare. Il Responsabile è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del GDPR. Il Titolare rilascia l'autorizzazione di cui sopra a suo insindacabile giudizio e comunque previa verifica del rispetto delle condizioni di cui al capo V del GDPR.

Le Parti concordano che, con l'accettazione della presente clausola (che rappresenta l'atto di formalizzazione di cui all'art. 28 GDPR), il Responsabile del Trattamento accetta l'incarico che gli è conferito dal Titolare.
Il Responsabile prende altresì atto che l'incarico di effettuare le operazioni di trattamento è affidato per l'esclusiva ragione che il profilo professionale/societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto idoneo a soddisfare i requisiti di esperienza, capacità, affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti, che possa sollevare incertezze sul loro mantenimento, dovranno essere preventivamente segnalati al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali ed eccezioni di sorta.

La presente nomina a Responsabile Esterno del trattamento ha validità per tutta la durata delle operazioni di trattamento descritte ai paragrafi che precedono e, in ogni caso, per tutta la durata della Convenzione.
Nel caso in cui termini, per qualsiasi ragione, il rapporto contrattuale esistente tra le parti quale presupposto della presente nomina, quest'ultima si intenderà revocata e comunque non produrrà più alcun effetto.
Al momento della cessazione della Convenzione, il Responsabile si impegna a restituire e cancellare tutti i dati trattati per conto del Titolare nello svolgimento delle attività ad esso affidate.

## Art. 9 - Piano Triennale di Prevenzione della Corruzione e Codice di Comportamento

Le parti dichiarano di accettare il contenuto dei rispettivi Piani Triennali di Prevenzione della Corruzione ex L. 190/2012, assorbiti nei rispetti PIAO vigenti, e Codici di Comportamento dei propri dipendenti ai sensi del DPR 62/2013 di cui hanno preso visione sui rispettivi siti aziendali

e di impegnarsi ad adottare, nello svolgimento delle funzioni connesse alla convenzione in oggetto, comportamenti conformi alle previsioni in essi contenute.

La violazione dei Piani Triennali di Prevenzione della Corruzione e Codici di Comportamento da parte dei Contraenti, comporterà la risoluzione del diritto del rapporto contrattuale in essere, nonché il diritto degli stessi di chiedere ed ottenere il risarcimento dei danni patiti per la lesione della propria immagine ed onorabilità.

**Art. 10 - Segnalazione di condotte illecite – Whistleblowing**

Con riferimento all'istituto del whistleblowing, le Parti hanno adottato il Regolamento per la gestione delle segnalazioni di tutela degli illeciti e tutela del segnalante, in conformità al D.Lgs. n. 24/2023 ed alle Linee guida ANAC contenute nella Delibera n. 311 del 12 luglio 2023. I Regolamenti e la documentazione, comprensiva di informativa, sono reperibili sui rispettivi siti web istituzionali nell'apposita sezione "Amministrazione Trasparente". Le segnalazioni di illeciti possono essere inoltrate ai RPCT mediante diversi canali interni che garantiscono la riservatezza del segnalante, ed anche con modalità informatizzata attraverso la piattaforma di WhisteblowingPA, il cui link di accesso è pubblicato nelle sezioni di "Amministrazione Trasparente".

**Art. 11 - Registrazione**

Il presente atto è soggetto:

- ad imposta di bollo a carico della Fondazione, corrisposta in modo virtuale. Autorizzazione n. 59666/2005 del 07/10/2005. In ottemperanza del D.P.R. 26 ottobre 1972, n. 642 - D.P.R. 30 dicembre 1982, n. 955 e successive modificazioni;
- a registrazione solo in caso d'uso, ai sensi dell'art. 5, comma 2°, del D.P.R. 131/86.

**Art. 12 - Foro competente**

In caso di controversia nell'interpretazione o esecuzione del presente Contratto il Foro competente sarà quello di Milano.

| | |
|---|---|
| Fondazione IRCSS Ca' Granda<br>Ospedale Maggiore Policlinico | ASST Grande Ospedale Metropolitano<br>Niguarda |
| IL DIRETTORE GENERALE | IL DIRETTORE GENERALE |
| Matteo Stocco | Alberto Zoli |

Il presente accordo è sottoscritto in forma elettronica ai sensi dell'art. 6 del D.L. 179/2012 convertito in L. n. 221 del 17/12/2012.

**Allegato 1**

**SEZIONE 1**

ELENCO DEI TRATTAMENTI DI DATI PERSONALI DI TITOLARITÀ DI **FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO DI MILANO** CHE SONO IN CARICO **ALL'ASST GRANDE OSPEDALE METROPOLITANO NIGUARDA** DESIGNATA RESPONSABILE DEL TRATTAMENTO DATI.

| Nome Trattamento | Descrizione | Tipologia di dati trattati | Modalità di trattamento | Principali trattamenti |
|---|---|---|---|---|
| Software OFC | Il servizio prevede la realizzazione di verbali operatori | Dati personali | Elettronico | Raccolta, registrazione, elaborazione, archiviazione |

La precedente tabella riporta integralmente i trattamenti di dati personali legati alle attività oggetto della presente nomina. Ulteriori ed eventuali trattamenti di dati personali sottoposti al medesimo Responsabile del trattamento, nominato mediante il presente Atto di nomina, saranno oggetto di comunicazione da parte del Titolare del trattamento.

| Categorie di interessati |
|---|
| Soggetti di cui vengono raccolti e conservati i dati e personali pazienti ricoverati |

| Finalità del trattamento |
|---|
| Sviluppo software //// |

| Durata del trattamento |
|---|
| La durata è definita mediante accordo contrattuale tra le Parti o fino all'espletamento delle attività oggetto della presente nomina. |

**SEZIONE 2**

ISTRUZIONI SUL TRATTAMENTO DEI DATI PERSONALI IMPARTITE DA **FONDAZIONE IRCCS CA' GRANDA OSPEDALE MAGGIORE POLICLINICO DI MILANO** IN QUALITA' DI TITOLARE DEL TRATTAMENTO **ALL'ASST GRANDE OSPEDALE METROPOLITANO NIGUARDA** DESIGNATA RESPONSABILE DEI TRATTAMENTI DI CUI AL SUDDETTO ATTO DI NOMINA

Il ***Responsabile*** del trattamento è tenuto ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dalla normativa privacy e di ulteriori ed eventuali contenuti specifici dell'atto sottoscritto dalle Parti secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli Interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Il ***Responsabile*** è tenuto a trattare i dati personali nel rispetto dei principi di necessità, proporzionalità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati e conservando gli stessi in una forma che consenta l'identificazione dell'Interessato per un periodo non superiore a quello occorrente alle finalità per i quali sono stati raccolti e trattati, e provvedendo, quando necessario, alla loro rettifica e aggiornamento.
Il ***Responsabile*** non tratterà i dati personali oggetto dell'incarico per ulteriori finalità.
Il ***Responsabile*** del trattamento si obbliga a svolgere l'incarico nel rispetto delle istruzioni sul trattamento dei dati personali che vengono fornite, oltre che di tutte le norme di legge in materia applicabili anche ai i propri dipendenti ed ai collaboratori esterni.
Il ***Responsabile*** al fine di agevolare la tempestiva collaborazione con il Titolare del Trattamento dei dati personali nell'esecuzione dell'incarico oggetto del presente accordo, indica nella persona del Privacy Officer o del DPO di ASST GRANDE OSPEDALE METROPOLITANO NIGUARDA il punto di contatto (PDC) al quale il Titolare potrà fare riferimento per ogni comunicazione necessaria o comunque connessa all'esecuzione degli obblighi contrattuali previsti dal presente accordo.
Il ***Responsabile*** è tenuto ad iniziare eventuali nuovi trattamenti solo in seguito a richiesta da parte del Titolare del trattamento.
I server e le infrastrutture informatiche utilizzate per l'esecuzione dei trattamenti di dati personali da parte del ***Responsabile*** si devono trovare all'interno della Comunità Europea e lo stesso vincolo si applica per i server degli ulteriori Responsabili eventualmente nominati secondo quanto previsto dal paragrafo 5 del presente accordo.
Il Responsabile, anche nell'ambito dei sub-affidamenti, non può trasferire i dati personali oggetto dei trattamenti verso le destinazioni di cui all'articolo 44 GDPR senza l'autorizzazione espressa e preventiva del Titolare. Il Responsabile è tenuto a rivolgere al Titolare la richiesta di autorizzazione al trasferimento dei dati in Paesi Extra-UE fornendo la documentazione attestante la legittimità del trasferimento nel rispetto del GDPR e del presente Atto di nomina.
Il Titolare rilascia l'autorizzazione di cui sopra a suo insindacabile giudizio e comunque previa verifica del rispetto delle condizioni di cui al capo V del GDPR. Laddove vengano stipulati accordi relativi al trasferimento transnazionale di dati personali, come, a titolo esemplificativo, Contratti con clausole standard, Norme vincolanti d'impresa o il trasferimento dei dati avvenga secondo Regole Privacy transnazionali, anche tali documenti e l'identità dei paesi o la descrizione delle circostanze in cui i citati accordi sono applicabili verranno debitamente comunicate al Titolare del trattamento.
Il ***Responsabile*** del Trattamento metterà a disposizione del Titolare anche il contratto o il diverso atto vincolante secondo il Diritto dell'Unione o dello Stato Membro con cui l'ulteriore Responsabile del trattamento si è obbligato nei confronti di ASST GRANDE OSPEDALE METROPOLITANO NIGUARDA o è stato comunque individuato.
Il ***Responsabile*** informerà il Titolare in tempo breve e, comunque, non oltre giorni 5, di ogni cambiamento in relazione a quanto sopra. In tali casi, il Titolare avrà il diritto di formulare la propria opposizione o di recedere dal contratto con efficacia immediata.
In caso di revoca della designazione a Responsabile dei trattamenti, o, in ogni caso, dopo il completamento di un trattamento per conto del Titolare, il Responsabile deve, sulla base delle istruzioni impartite da

quest'ultimo, restituire o cancellare i dati personali, salvo che il diritto dell'Unione o degli Stati membri, cui è soggetto il Responsabile, prescriva la conservazione dei dati personali.
Il ***Responsabile*** deve assicurare in ogni momento che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti, ai documenti contrattuali ed alle specifiche dei Servizi definiti dal ***Titolare***. Le misure di sicurezza adottate dovranno in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.
Il ***Responsabile***, in ogni caso, venuto a conoscenza di una specifica violazione dei dati personali, sarà tenuto a comunicare al ***Titolare***, ai sensi dell'art. 33, par. 2 Reg. UE 2016/679, senza ingiustificato ritardo e comunque entro 24 ore dalla scoperta, tali violazioni, eventualmente intervenute durante la vigenza della presente nomina. In ipotesi di intervenute violazioni dei dati personali, il Responsabile del trattamento collaborerà attivamente con il Titolare del trattamento per la corretta gestione della comunicazione delle violazioni summenzionate.
A tal fine, il Responsabile si impegna a comunicare nel termine più breve dalla scoperta e, comunque, non oltre 24 ore da questa, ogni accesso non autorizzato ai dati personali nonché ogni accesso non autorizzato agli strumenti elettronici impiegati per l'esecuzione del trattamento o, comunque, ogni accesso non autorizzato verificatosi presso le strutture del Responsabile che abbiano causato la perdita, la modifica o la rivelazione non dovuta di dati personali.
Nell'ipotesi di violazione dei dati personali ai sensi dell'art. 33 del Regolamento, il Responsabile si doterà di un registro contenente una descrizione dell'evento, del periodo di estensione dello stesso, delle conseguenze prodotte, del nominativo di colui che lo ha riportato oltre che dei soggetti a cui è stato comunicato, della descrizione delle azioni messe in atto per la risoluzione dell'evento (compresa l'indicazione della persona responsabile e i dati recuperati) nonché contenente l'indicazione che è stata cagionata la perdita, la rivelazione o la alterazione di dati personali.
Il Responsabile si impegna inoltre, nei limiti delle proprie competenze, ad adottare, d'intesa con il Titolare, tempestivamente tutte le azioni di contrasto per il contenimento e la mitigazione degli effetti della violazione e ad assistere il Titolare, se richiesto, nella redazione della notifica della violazione all'Autorità di Controllo competente o nella comunicazione agli Interessati coinvolti, a norma degli artt. 33 e 34 GDPR.
Il **Responsabile** implementerà un sistema di gestione del controllo degli accessi ai sistemi e ai dati personali trattati fornendo al Titolare del trattamento nominato, ove occorre, il controllo della gestione degli accessi, ad esempio attribuendo i diritti da amministratore o la gestione delle utenze d'accesso da terminare.
Nelle ipotesi in cui più di una persona abbia accesso ai dati personali archiviati, ognuna di esse verrà dotata di un'autonoma "username" da utilizzare per l'identificazione, autenticazione e per l'individuazione dei livelli di autorizzazione.
Il Responsabile porrà in essere procedure aziendali per la registrazione degli utenti e per la loro de-registrazione, contenenti precise istruzioni per fronteggiare la compromissione del controllo degli accessi da parte degli utenti o degli altri dati relativi alla registrazione (ad es. a causa della compromissione delle credenziali di accesso dell'utente, come nel caso di mal funzionamento o la compromissione di password dovuta a rivelazione involontaria).
Il Responsabile fornirà ogni opportuna e necessaria informazione al Titolare del trattamento in merito all'uso di sistemi di crittografia per la protezione dei dati personali e provvederà altresì a collaborare con il Titolare, fornendo ove necessario ogni necessaria informazione, nel consentire l'applicazione da parte di questi dello stesso livello di protezione dei dati personali.
Il Titolare impiegherà attrezzature contenenti supporti di memorizzazione assicurandosi che tutti i dati personali e i software precedentemente impiegati siano stati rimossi o sovrascritti in maniera sicura, prima dell'eliminazione o del riutilizzo dei supporti stessi.
Nell'assicurare un approccio coerente ed efficace per la gestione degli incidenti relativi alla sicurezza delle informazioni, il Titolare ed il Responsabile prevederanno controlli periodici volti a prevenire e affrontare in maniera adeguata ed efficace gli incidenti di sicurezza.
Un eventuale incidente nella sicurezza delle informazioni dovrà comportare un processo di valutazione da parte del Responsabile del trattamento, come parte del suo processo di gestione degli incidenti, volto a determinare se una violazione delle informazioni riguardante i dati personali ha avuto luogo. Non ogni evento relativo alla sicurezza delle informazioni avrà questo effetto, ma solo quello che causa un effettivo o significativamente probabile accesso non autorizzato ai dati personali o a una delle infrastrutture del Responsabile con le quali viene effettuato il trattamento o ad una delle strutture che contengono dati

personali e potrebbe includere, senza alcuna limitazione, ping o attacchi di rete su firewall o edge server, scan delle porte di comunicazione, tentativi di autenticazione non riusciti, attacchi DOS e sniffing di pacchetti.
Il Responsabile del Trattamento metterà inoltre a disposizione del Titolare ogni strumento informatico necessario o comunque utile a consentire l'accesso, la correzione e/o la cancellazione dei dati.
Il ***Responsabile*** è tenuto, in relazione ai soggetti autorizzati al trattamento che agiscono sotto la sua autorità, ad istruire quest'ultimi al rispetto delle seguenti misure, ove ritenute applicabili al trattamento di specie:

1) individuare per iscritto i soggetti autorizzati al trattamento dei dati personali (persone fisiche o gruppi omogenei);
2) impartire ai soggetti autorizzati al trattamento loro le istruzioni idonee alle attività da svolgere;
3) vigilare sull'operato dei soggetti autorizzati al trattamento all'accesso ai dati personali;
4) prevedere un piano di formazione destinato ai soggetti autorizzati al trattamento;
5) assicurarsi che ad ogni soggetto autorizzato al trattamento sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo del soggetto autorizzato al trattamento, eventualmente associato a un codice identificativo o a una parola chiave;
6) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo del soggetto autorizzato al trattamento;
7) assicurare che la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili al soggetto autorizzato al trattamento e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi;
8) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri soggetti autorizzati al trattamento, neppure in tempi diversi;
9) assicurare che sia operata la disattivazione delle credenziali di autenticazione del personale in caso venga a cessare la necessità di accesso da parte del soggetto autorizzato al trattamento o intervenga un'inattività per più di sei mesi.
10) le credenziali scadute o comunque disattivate non verranno in alcun modo messe a disposizione di altri soggetti.
11) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento del soggetto autorizzato al trattamento che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici. In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti autorizzati della loro custodia;
12) prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo soggetto autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;
13) verificare, ad intervalli almeno annuali, le autorizzazioni in essere;
14) redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e implementare le ulteriori misure di sicurezza, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i.;
15) installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque periodicamente ed in occasione di ogni versione disponibile dalla casa costruttrice;
16) provvedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un

congruo periodo di tempo, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;

17) prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi.

Il Responsabile garantisce che le persone coinvolte nel trattamento dei dati personali per conto del Titolare, in particolare i dipendenti del Responsabile ed eventuali ulteriori responsabili e loro dipendenti, tratteranno tali dati personali secondo le istruzioni impartite dal Titolare.

Il Responsabile garantisce che il personale impiegato è vincolato alla confidenzialità e che lo stesso è formalmente autorizzato al trattamento dei dati personali necessari per l'esecuzione delle attività di cui al Contratto e puntualmente istruito sulle modalità di esecuzione di tali attività.

In tema di sicurezza dei dati personali, ai sensi dell'art. 32 del Reg. UE 2016/679, il ***Responsabile*** del trattamento è tenuto a mettere in atto misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio. 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.

Inoltre, per il trattamento di categorie particolari di dati personali (c.d. dati particolari), cioè quelli di cui al art. 9, par. 1 del Reg. UE 2016/679, il ***Responsabile*** deve:

1) prevedere che il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui tutti i dati personali e i software precedentemente utilizzati siano stati rimossi o sovrascritti in maniera sicura, prima dell'eliminazione o del riutilizzo dei supporti stessi; In questo ambito risulta necessario procedere a:
   a) emanare adeguate istruzioni di comportamento a tutti i soggetti autorizzati al trattamento;
   b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili, sia essi di tipo asportabile che presenti in aree di memoria interne al sistema operativo od in programmi, ove possano trovarsi dati particolari;
   c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni ai soggetti autorizzati al trattamento.

2) assicurare che la memorizzazione dei dati particolari su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato (anche attraverso processi di pseudonimizzazione), ovvero che la memorizzazione dei dati particolari sia cifrata o in alternativa che vi sia separazione tra i dati particolari e gli altri dati personali che possano permettere l'identificazione dell'interessato;

3) assicurare che il trasferimento dei dati particolari in formato elettronico, avvenga attraverso "canali sicuri" o in maniera cifrata.

In merito al **trattamento dei dati personali con strumenti diversi da quelli elettronici**, il ***Responsabile*** è tenuto a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto i soggetti autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti.

Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio un registro e degli armadi separati e chiusi).

Il trattamento di dati particolari, dovrà infine prevedere l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.

È fatto comunque assoluto **divieto**, al ***Responsabile*** designato, della **diffusione** dei dati, della **comunicazione** non autorizzata a terzi e più in generale è fatto **divieto** di effettuare trattamenti non finalizzati all'esecuzione delle attività affidate, salvo a fronte di specifica autorizzazione da parte del ***Titolare***.

Le operazioni di trattamento devono essere gestite dal ***Responsabile*** del trattamento in aderenza alle attività svolte nell'ambito dei progetti assegnati e in considerazione di eventuali e successive modifiche alle operazioni e/o modalità di trattamento apportate dal Titolare.

Il ***Responsabile*** è chiamato ad assicurare, per conto del Titolare del trattamento, l'esercizio dei diritti eventualmente applicabili da parte degli Interessati (Capo III del Regolamento UE 2016/679), nel rispetto dei termini di legge, adottando ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali per l'esercizio degli stessi diritti.

Il ***Responsabile*** è tenuto a mettere a disposizione del ***Titolare*** tutte le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni, richieste dallo stesso Titolare del trattamento o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla normativa privacy.

Il ***Responsabile***, ai sensi dell'art. 30 del Regolamento UE 2016/679, è tenuto a fornire al ***Titolare*** le informazioni necessarie a quest'ultimo per la compilazione del proprio "Registro dei trattamenti". Il Responsabile si impegna – nei limiti previsti dalla normativa in materia di protezione dei dati personali – a conservare le registrazioni relative al trattamento dei dati personali svolto in qualità di Responsabile per conto del Titolare (art. 30, paragrafo 2, GDPR).

Qualora il ***Titolare*** intenda redigere la Valutazione di impatto prevista dall'art. 35 del Regolamento summenzionato, il ***Responsabile*** sarà tenuto a fornire anche le ulteriori informazioni che si rendessero necessarie alla redazione del documento.

Il ***Responsabile***, qualora in ottemperanza all'obbligo di Legge, fosse tenuto ad individuare all'interno della propria organizzazione la figura del "Responsabile per la protezione dei dati personali", quest'ultimo sarà tenuto a svolgere la propria attività in stretta collaborazione con il ***Titolare***.

Il ***Responsabile*** collaborerà attivamente con l'Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, al fine di consentire a queste ultime l'esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi ed ispezioni, relativamente ai trattamenti oggetto dell'Atto di nomina.