FRONTESPIZIO DELIBERAZIONE

AOO: ASL_BO

REGISTRO: Deliberazione

NUMERO: 0000375

DATA: 08/11/2023 14:25

OGGETTO: Convenzione tra AUSL BO e Villa Torri Hospital per l'erogazione di prestazioni di laboratorio ad opera del LUM - Laboratorio Unico Metropolitano. Presa d'atto di intervenuto rinnovo anni 2023/2025.

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Bordon Paolo in qualità di Direttore Generale
Con il parere favorevole di Roti Lorenzo - Direttore Sanitario
Con il parere favorevole di Ferro Giovanni - Direttore Amministrativo

Su proposta di Claudio Lazzari - UO Direzione Medica Ospedali Maggiore e Bellaria (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-01-03]

DESTINATARI:

- Collegio sindacale
- UO Servizi Amministrativi Ospedalieri (SC)
- UO Laboratorio Unico Metropolitano (SC)
- Funzione Amministrativa Economica (PO)
- UO Direzione Medica Ospedali Maggiore e Bellaria (SC)
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000375_2023_delibera_firmata.pdf	Bordon Paolo; Ferro Giovanni; Lazzari Claudio; Roti Lorenzo	696A1A7516EAB4832377FE6CD314DB82C429FF5C5546C413B889FE3A50F3F004
DELI0000375_2023_Allegato1.pdf:		134BBDEDA751DC5D475080BBEFE2DCCBE196EB02260AA99713578F9329F037CE
DELI0000375_2023_Allegato2.pdf:		B1E73B326B72FC31EFD27CFEED35E646EE08A71B2D51BA3C34CB5BF832EF19CC

DELIBERAZIONE

OGGETTO: Convenzione tra AUSL BO e Villa Torri Hospital per l'erogazione di prestazioni di laboratorio ad opera del LUM - Laboratorio Unico Metropolitano. Presa d'atto di intervenuto rinnovo anni 2023/2025.

IL DIRETTORE GENERALE

Su proposta del Direttore della UO Direzione Medica Ospedali Maggiore e Bellaria (SC), Dott. Claudio Lazzari, che esprime contestuale parere favorevole in ordine ai contenuti sostanziali, formali e dilegittimità del presente provvedimento;

Richiamati:

- il D.lgs 502/92 "Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421" e ss.mm.ii;
- la normativa generale in materia di incompatibilità di cui all'art. 4, comma 7, della legge 412/91;
- la L.R. 22/2019 e ss.mm.ii. in materia di autorizzazione e accreditamento sanitario e la relativa delibera di attuazione DGR 886/2022, in particolare nella parte che prevede la possibilità per le Strutture sanitarie accreditate di acquisire all'esterno prestazioni sanitarie complementari al processo diagnostico-assistenziale, ricorrendone i presupposti;

Richiamate - altresì - le precedenti Deliberazioni AUSL BO n. 254/2015, n. 158/2016 e n. 175/2016 con le quali è stato istituito il Laboratorio Unico Metropolitano (LUM) in capo alla stessa Azienda USL di Bologna, centro HUB cittadino di tutte le attività di patologia clinica, al quale sono confluite le attività di produzione svolte rispettivamente dall'Azienda Ospedaliero Universitaria di Bologna Policlinico S. Orsola Malpighi, dall' Istituto Ortopedico Rizzoli e dall'Azienda USL di Imola;

Precisato che l'Azienda USL di Bologna, per effetto dei suddetto trasferimento, è subentrata in tutti i rapporti attivi e passivi relativi all'attività ceduta instaurati in precedenza dalle rispettive Aziende, compresi gli accordi per la fornitura di prestazioni di laboratorio di patologia clinica in favore di terzi;

Premesso che Villa Torri Hospital:

- è società appartenente al Gruppo Villa Maria S.p.A. - GVM Care & Research, e gestisce l'omonima struttura ospedaliera, accreditata con il Servizio Sanitario Nazionale;
- in passato ha richiesto ed usufruito di prestazioni di laboratorio per analisi chimico-cliniche già rese da AOU BO, poi trasferite al suddetto Laboratorio Unico Metropolitano di AUSL BO;

Considerato che AUSL BO ha continuato a garantire in regime di attività istituzionale le prestazioni a favore dei pazienti della Struttura esclusivamente per le richieste in emergenza e urgenza, applicando le tariffe del Nomenclatore maggiorate del 10%, nell'ambito della convenzione approvata con Deliberazione n. 316/2016 , poi prorogata con Determinazione 2487/20;

Richiamata l'intercorsa conrrispondenza, mediante la quale Villa Torri H. ha chiesto ad AUSL BO di proseguire il rapporto anche per le future annualità;

Tenuto conto che il LUM dell'Azienda USL di Bologna è articolato secondo un modello "Hub & Spoke", e che Villa Torri H. dovrà far pervenire le provette debitamente etichettate e consegnarle alla sede spoke del Laboratorio sito c/o l'Ospedale Sant'Orsola di Bologna, secondo le modalità indicate nell'art. 2 dell'accordo in oggetto;

Richiamata la nota PG 114900/23, mediante la quale le parti hanno sottoscritto il nuovo testo dell'accordo valido fino al 31 dicembre 2025 unitamente alla nomina del Responsabile del Trattamento dati personali;

Delibera

1. di dare atto dell'intervenuto rinnovo della Convenzione in oggetto, il cui testo si allega quale parte integrante e sostanziale del presente provvedimento;
2. di prevedere che la validità del citato accordo decorre dalla data dell'ultima sottoscrizione fino al 31 dicembre 2025, intendendo sanata e risconsocuta l'attività resa nelle more della formalizzazione degli atti;
3. di dare atto che le prestazioni erogate *ex* artt. 1 e 2 Conv. a favore dei pazienti di Villa Torri Hospital, sono richieste in emergenza e urgenza e rese da AUSL BO in regime di attività istituzionale applicando le tariffe del Nomenclatore regionale in vigore maggiorate del 10%;
4. di dare atto degli opportuni aggiornamenti al testo dell'accordo, anche in ragione delle intervenute modifiche legislative;
5. di prendere atto che Villa Torri H. è il Titolare del trattamento dati personali che ha nominato AUSL BO Responsabile del Trattamento ex art. 28 GDPR 679/2016 mediante sottoscrizione di apposito atto di designazione allegato;
6. di prevedere che i ricavi derivanti dal periodo di validità della Convenzione in oggetto saranno imputati annualmente sui Bilanci di competenza al Conto GAAC 0155700203 "Specialistica a privati paganti".

Responsabile del procedimento ai sensi della L. 241/90:
Vincenzo Grappone

ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO

Tra

Villa Torri Hospital S.r.l, con sede in Bologna, Viale Quirico Filopanti n. 12, Codice Fiscale e P. IVA 02383150394, in persona del proprio legale rappresentante *pro-tempore*, (di seguito, la "**Società**" o il "**Titolare**"),

e

Azienda USL di Bologna, con sede in Bologna, via Castiglione 29, Partita Iva e Codice fiscale 02406911202, nella persona del Direttore Generale e legale rappresentante *p.t*. Dott. Paolo Bordon (di seguito, il "**Fornitore**" o "**Responsabile**")

(di seguito, collettivamente, definite le "**Parti**")

PREMESSO CHE

a) il Fornitore o "Responsabile" e la Società hanno stipulato un contratto *(*di seguito, "**Contratto**"), avente ad oggetto l'erogazione, da parte del Fornitore stesso, di attività di service di esami di laboratorio e refertazione (di seguito: "**Servizi**"), valido dalla data dell'ultima sottoscrizione fino al 31 dicembre 2025;

b) lo svolgimento dei suddetti Servizi da parte del Fornitore o "Responsabile" comporta il trattamento, da parte di quest'ultimo, per conto della Società, dei dati personali di interessati di cui la Società stessa è Titolare (di seguito: "**Dati Personali**") indicati in Allegato (sezione 1), aventi gli impatti sui diritti e le libertà degli interessati riportati in Allegato (sezione 2);

c) il Fornitore o "Responsabile" dichiara di possedere esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate atte a garantire la conformità alla normativa in materia di tutela dei dati personali e la tutela degli interessati;

d) con il presente atto, le Parti intendono pertanto rinnovare e regolare i trattamenti dei Dati Personali da parte del Fornitore ai sensi dell'art. 28.3 del Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Regolamento Generale sulla Protezione dei Dati Personali, entrato in vigore il 24 maggio 2016 e applicabile dal 25 maggio 2018 (di seguito, "**GDPR**" o "**Regolamento**");

e) la Società ed il Fornitore sono qualificati anche, nel prosieguo, rispettivamente, quali "Titolare" e "Responsabile";

Tutto ciò premesso (e costituendo le premesse parte integrante e sostanziale del presente atto di designazione), fra le Parti si conviene e si stipula quanto segue

1. OGGETTO

Con il presente atto, il Fornitore è nominato dalla Società Responsabile del trattamento dei Dati Personali connesso all'erogazione dei Servizi.

2. OBBLIGHI DEL RESPONSABILE

Il Fornitore è tenuto a trattare i Dati Personali solo ed esclusivamente ai fini dell'esecuzione dei Servizi, nel rispetto di quanto disposto dalla normativa applicabile in materia di protezione dei dati personali, nonché delle istruzioni del Titolare riportate nei successivi articoli e nell'Allegato e di ogni altra indicazione scritta che potrà essergli dallo stesso fornita.

3. MISURE DI SICUREZZA

3.1 Ai sensi dell'art. 32 del GDPR sia il titolare che il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.

3.2 Di conseguenza, le Parti concordano che:

i) il **Titolare** abbia la facoltà di richiedere al **Responsabile** una relazione sulle attività di trattamento oggetto del presente Atto di Nomina nonché delle misure di sicurezza adottate, evidenziando gli aspetti problematici, le difficoltà attuative, gli incidenti e/o i reclami riscontrati e segnalando alla Società l'eventuale necessità di revisione delle misure di sicurezza necessarie per dare corretta esecuzione al Contratto e non incorrere in violazioni di leggi e/o regolamenti.

ii) il **Titolare**, sulla base all'analisi fornita dal responsabile, potrà confermare il livello di rischio indicato in Allegato (Sezione 2) o individuare un diverso livello, comunicando al Responsabile la propria valutazione;

iii) Il **Responsabile** implementerà conseguentemente a proprie spese le misure di sicurezza, fra quelle riportate in Allegato (Sezione 3), che siano adeguate in relazione al livello d'impatto comunicato dal Titolare ai sensi della precedente lettera ii) entro 30 giorni dalla comunicazione.

3.3 Eventuali modifiche delle misure di sicurezza resesi necessarie a causa di modifiche e aggiornamenti della normativa in materia di protezione dei dati personali, nonché a causa di mutamenti delle tipologia, natura, contesto e finalità del trattamento, o variazioni del rischio o a seguito di evoluzioni tecnologiche delle applicazioni utilizzate dal Fornitore, saranno adottate ed implementate dal Fornitore e/o dei suoi eventuali subappaltatori a onere e spese del Fornitore stesso, previa in ogni caso effettuazione della procedura di cui al precedente art. 3.2

3.4 A prescindere dal livello di rischio/impatto, il Fornitore si impegna in ogni caso ad implementare le misure di sicurezza indicate in Allegato (Sezione 3).

3.5 Il **Responsabile** si impegna, altresì, ai sensi dell'art. 28.3, lett. f), ad assistere la Società in relazione all'obbligo del Titolare di mettere in atto proprie misure tecniche ed organizzative adeguate di cui all'art. 32 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore.

4. VIOLAZIONI DI DATI PERSONALI (CD. "DATA BREACH")

Il **Responsabile** si impegna ad informare senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza, il Titolare (inviando una comunicazione a mezzo PEC o all'indirizzo del medesimo) di ogni violazione della sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque trattati, ed, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

5. VALUTAZIONE D'IMPATTO (CD. "DATA PROTECTON IMPACT ASSESSMENT")

Il **Responsabile**, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.

6. SOGGETTI AUTORIZZATI AL TRATTAMENTO

6.1 Fatto salvo quanto previsto all'articolo 11 che segue, il **Fornitore** garantisce che l'accesso ai Dati Personali sarà limitato esclusivamente ai soli propri dipendenti e collaboratori il cui accesso sia necessario per l'esecuzione dei Servizi, previamente identificati per iscritto.

6.2 Il **Responsabile** si impegna a fornire ai propri dipendenti e collaboratori deputati a trattare i Dati Personali di cui è Titolare la Società le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, curarne la formazione, vigilare sul loro operato, vincolarli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività, anche per il periodo successivo alla cessazione

del rapporto di lavoro, e a comunicare al Titolare, su specifica richiesta, l'elenco aggiornato degli stessi.

7. AMMINISTRATORI DI SISTEMA

7.1 Qualora previsto, relativamente ai trattamenti eseguiti dai propri incaricati con il ruolo di 'amministratore di sistema' al fine di erogare il servizio oggetto dell'accordo, il **Fornitore** si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del Garante del 25 giugno 2009, e ad ogni altro pertinente provvedimento dell'Autorità.

7.2 Il Fornitore si impegna, in particolare, a:

i) designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di Dati personali, fornendo al Titolare, su richiesta, informazioni sulle valutazioni effettuate per le designazioni;
ii) effettuare un'elencazione analitica degli ambiti di operatività consentiti a ciascuno in base al relativo profilo di autorizzazione assegnato e fornendo, su richiesta, informazioni relative alle valutazioni alla base delle designazioni;
iii) predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
iv) comunicare periodicamente al Titolare l'elenco aggiornato degli amministratori di sistema, specificandone l'ambito di responsabilità (sistemi, database, reti, applicativi, etc.);
v) verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
vi) mantenere i file di log previsti in conformità a quanto previsto nel suddetto provvedimento;
vii) garantire una rigida separazione tra chi autorizza e/o assegna i privilegi di accesso e chi effettua le attività tecnico-sistemistiche (c.d. *Segregation Duty*).

8. RAPPORTI CON LE AUTORITÀ

Il **Responsabile**, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali.

9. ISTANZE DEGLI INTERESSATI

Il **Responsabile** si obbliga ad assistere il Titolare con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, nell'adempimento degli obblighi gravanti su quest'ultimo di dar seguito ad eventuali istanze degli interessati di cui al capo III del GDPR ed a fornirgli ogni informazione e/o documento utile.

10. ULTERIORI OBBLIGHI

10.1 Il **Responsabile** mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni ragionevole collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto.

10.2Resta inteso che qualsiasi verifica condotta ai sensi del presente comma dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso.

10.3 Il **Responsabile** si impegna altresì a:

i) effettuare almeno annualmente un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare (e agli adempimenti eseguiti) ed alle conseguenti risultanze;

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

10.4 Fatto salvo quanto previsto nell'art. 12, resta inteso che qualora il Responsabile determini autonomamente le finalità e i mezzi di trattamento in violazione del GDPR, sarà considerato Titolare del trattamento, assumendo i conseguenti oneri, rischi e responsabilità.

11. ULTERIORI RESPONSABILI

11.1 Il **Responsabile** potrà ricorrere ad altri responsabili (di seguito, "**Sub-responsabili**") per l'esecuzione di specifiche attività di trattamento oggetto del presente atto, imponendo agli stessi i medesimi obblighi in materia di protezione dei dati cui è soggetto il Responsabile, in particolare in relazione alle misure di sicurezza.

11.2 Il **Responsabile** si impegna espressamente ad informare il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori Sub-responsabili; il Titolare avrà il diritto di opporsi a tali modifiche, comunicando la sua opposizione per iscritto entro 10 giorni dalla notifica da parte del Responsabile. Il Responsabile non ricorrerà ai Sub-responsabili nei cui confronti il Titolare abbia manifestato la sua opposizione.

11.3 Il **Responsabile**, nella scelta dei Sub-responsabili, garantisce altresì che i trattamenti effettuati da questi ultimi avvengano all'interno dell'Unione Europea e, qualora detti Sub-responsabili dovessero effettuare un trasferimento di dati verso paesi terzi o organizzazioni internazionali ai sensi degli artt. 44 ess GDPR, il **Responsabile** si obbliga a:

- verificare la sussistenza delle misure di garanzia adeguate ex artt. 44 e ss. GDPR;
- comunicare immediatamente al Responsabile il verificarsi di tale circostanza, specificando le misure di garanzia adeguate ex artt. 44 e ss. GDPR, fornendone una copia.

11.4 Resta espressamente inteso che il Responsabile rimarrà direttamente responsabile nei confronti della Società in ordine alle azioni e alle omissioni dei propri Sub-responsabili.

12. RESPONSABILITÀ

Il **Responsabile** si impegna a mantenere indenne la Società da ogni danno, costo od onere di qualsiasi genere e natura, nonché da ogni contestazione, azione o pretesa avanzate nei confronti del Titolare da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità derivanti da eventuali inadempimenti del presente atto da parte del Responsabile stesso (o di eventuali suoi Sub-responsabili) o inosservanze delle istruzioni di cui al presente atto o di ulteriori istruzioni eventualmente trasmesse per iscritto dalla Società.

13. DURATA

La presente designazione decorre dalla data in cui viene sottoscritta dalle Parti ed è valida fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del Contratto o dei Servizi o alla revoca, il Responsabile dovrà mantenere la massima

riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

14. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

14.1 Il **Responsabile**, all'atto della scadenza del Contratto e/o dei Servizi o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di designazione, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei Dati Personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del Titolare, all'immediata restituzione allo stesso dei Dati Personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia.

14.2 In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

15. DISPOSIZIONI FINALI

15.1 Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la Società.

15.2 L'Allegato alla presente designazione fa parte integrante della stessa.

15.3 Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei dati personali.

Bologna, data dell'ultima sottoscrizione

IL TITOLARE DEL TRATTAMENTO

……..

Lorenzo Venturini

Per accettazione

IL RESPONSABILE DEL TRATTAMENTO

……

Dott. Paolo Bordon

SEZIONE 1

AMBITO del TRATTAMENTO

Categorie di interessati

- Pazienti del Titolare, anche minori.

Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati)

- Dati personali comuni e dati di categorie particolari idonei a rilevare lo stato di salute.

Natura e finalità del trattamento

- Natura: il trattamento avviene mediante invio e scambio di documenti in formato digitale (trasmissione mediante applicativi informatici – in particolare tramite l'applicativo DNTerritorio messo a disposizione dal Fornitore - e posta elettronica).
- Finalità del trattamento: il trattamento avviene per finalità di cura connesse all'esecuzione di attività di prevenzione, diagnosi, cura e riabilitazione nell'ambito dell'erogazione del servizio di esami di laboratorio e refertazione in favore dei pazienti del Titolare.
- .....

Durata del trattamento

- Pari alla durata del contratto stipulato tra Società e Fornitore.

SEZIONE 2

IMPATTI del TRATTAMENTO

In linea con il *risk-based approach* ed il principio di *accountability* di cui al Regolamento UE n. 679/2016, il Titolare ha individuato, per le operazioni di trattamento delegate al Responsabile (v. tabella), il livello di rischio sui diritti e le libertà degli interessati di seguito indicato:

Trattamento	**Impatto**	**Rischio**
Attività di laboratorio di analisi e refertazione	Medio Basso	Medio-Basso

I livelli di impatto sono i seguenti:

- Impatto basso: gli interessati dei dati personali coinvolti dal nuovo trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. ricezione di spam, perdita di tempo per ripetere formalità, etc.);
- Impatto medio: gli interessati dei dati personali coinvolti dal nuovo trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. multe imposte erroneamente, account servizi online bloccati, dati non aggiornati, etc.);
- Impatto alto: gli interessati dei dati personali coinvolti dal nuovo trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. perdita di lavoro, separazione o divorzio, perdita finanziaria a seguito di frode, etc.);
- Impatto molto alto: gli interessati dei dati personali coinvolti dal nuovo trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es. Perdita di prova nel contesto di contenzioso; Perdita di accesso a infrastrutture vitali, etc.).

SEZIONE 3

MISURE DI SICUREZZA

1. Premessa

A prescindere dal livello di rischio individuato, il Fornitore si impegna, per i trattamenti dallo stesso effettuati, a:

- adottare strumenti e implementare ed erogare servizi nel rispetto del principio della privacy by default;
- provvedere alla rimozione dei dati entro i termini definiti nell'art. 14 dell'atto di designazione fornendo opportuna evidenza dell'avvenuta rimozione. La rimozione dei dati dovrà essere tale da impedire il recupero degli stessi anche tramite attività di *computer forensic*;
- di recepire le policy in materia di Sicurezza informatica e di protezione dei dati della Società.

2. Ruoli e responsabilità

È responsabilità del Fornitore:

- verificare con continuità la correttezza, la completezza e la pertinenza dei dati personali e garantirne l'aggiornamento e la modifica;
- garantire la riservatezza dei dati personali dei clienti che tratta;
- garantire la sicurezza delle postazioni di lavoro e delle credenziali di accesso utilizzate per l'accesso ai sistemi della Società, nonché l'adeguatezza dei profili di accesso assegnati ad eventuali collaboratori.

È responsabilità della Società garantire la sicurezza dei sistemi utilizzati dai fornitori nonché dei dati trattati in particolare in termini di riservatezza, integrità, disponibilità.

3. Gestione delle violazioni di dati personali (Personal Data Breach)

Il Fornitore dovrà tempestivamente comunicare alla Società qualunque violazione dei dati relativa a riservatezza, integrità, disponibilità e qualità dei dati in conformità con termini e condizioni indicati nell'art. 4 dell'atto di designazione, garantendo il supporto al Titolare nelle attività di indagine e remediation.

Il fornitore è tenuto a concordare con il titolare le modalità più appropriate per la comunicazione, la gestione e le attività di escalation relative alle violazioni dei dati personali.

Inoltre, il fornitore deve garantire il presidio dei canali di comunicazione attivati, al fine di garantire una tempestiva presa in carico in caso di necessità.

Incident Report

Il Fornitore è tenuto a registrare i data breach insieme ai dettagli relativi all'evento e alle successive azioni correttive di contenimento eseguite, in particolare:

- le modalità di gestione e registrazione degli eventi di sicurezza che interessano l'infrastruttura e le successive azioni di attenuazione.
- le modalità di comunicazione di tutte le informazioni ed evidenze nel caso l'incidente interessi anche solo parzialmente le infrastrutture assegnate al Titolare
- le modalità di comunicazioni di eventuali remediation plan che possano interessare anche parzialmente le infrastrutture assegnate al Titolare
- la comunicazione degli esiti delle revisioni delle analisi dei rischi che incombono sulle infrastrutture di interesse del Titolare a seguito del verificarsi di un incidente

Incident Notification

Il Fornitore si impegna:

- ad effettuare una classificazione degli in termini di gravità;

- a rispettare le procedure di escalation previste per le varie tipologie di incidenti, come di seguito riportato:
    - il Responsabile fornisce una prima sommaria comunicazione dell'evento di sicurezza al titolare; la comunicazione deve essere inviata appena l'evento si verifica e/o il Responsabile ne viene a conoscenza, in particolare se questo coinvolge dati personali e/o sistemi critici per il Titolare.
    - le attività di gestione dell'incidente tra il personale del Titolare e del Fornitore prevedono:
        - l'attivazione di un Contingency Plan
        - la definizione di priorità di ripristino dei dati/sistemi
        - l'indicazione di dipendenze rilevanti rispetto al processo di ripristino (es. fornitori, partner, etc.)
    - il Responsabile fornisce una comunicazione dettagliata entro 48 ore dal verificarsi dell'evento in particolare se questo insiste su sistemi che trattano dati personali.
- a fornire supporto al Titolare in caso di notifica alle autorità competenti.

Accesso ai locali ed ai sistemi

Fermo restando quanto indicato nell'art. 10 dell'atto di designazione, nel caso di data breach, il Fornitore deve garantire al Titolare o alle figure da esso ingaggiate, per la verifica e/o l'accertamento di eventuali data breach, l'accesso ai locali e ai sistemi, nonché l'adeguato supporto durante tutta la fase di analisi dell'incidente.

4. Misure di sicurezza in funzione del rischio

Nella tabella di seguito riportata vengono descritti gli obiettivi di controllo che il fornitore deve garantire, individuati sulla base della metodologia ISO/IEC 27001:2013. In particolare, i controlli sono stati individuati previa valutazione della tipologia di trattamento esternalizzata, oltre che sulla complessità e capacità organizzativa del fornitore.

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**	Le modalità di gestione dei dati personali tramite strumenti informatici e le misure di sicurezza adottate sono descritte in un documento di sicurezza che è riesaminato e riveduta periodicamente e a fronte di eventi significativi (es: incidenti informatici, cambiamenti organizzativi, etc..). Il documento di sicurezza per l'elaborazione dei dati personali è comunicato a tutti i dipendenti, collaboratori e alle parti esterne pertinenti, e come minimo riporta: i ruoli e le responsabilità, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, i responsabili dei dati e altre terze parti coinvolte nel trattamento di dati personali.
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**	Devono essere individuati i ruoli coinvolti nel trattamento dei dati personali. 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. Il documento/politica di sicurezza deve descrivere e documentate le regole di controllo accesso ai sistemi informatici che trattano dati personali.
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 essere aggiornato periodicamente.
A. 12.1	**Operational procedures and responsibilities**	I progetti che determinano dei cambiamenti significativi alle procedure informatiche, ai sistemi informatici, comprese le iniziative di affidamento dei servizi informatici all'esterno, devono essere corredati di adeguata documentazione che descrive gli obiettivi, i requisiti, i principali rischi di sicurezza e le misure che sono state individuate per mitigarli. I dati personali reali non devono essere utilizzati per effettuare lo sviluppo e test di applicativi.
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**	E' definita e documentata una procedura per la risposta agli incidenti relativi ai dati personali. La procedura deve assicurare che 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**	Devono essere definiti i livelli di servizio (disponibilità) dei servizi oggetto della fornitura, nonchè dei tempi di ripristino dei dati E DEI SERVIZI in caso di incidenti e problemi

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.7.2.2	**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.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.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	**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 considerate soluzioni di cifratura, adottandole dove possibile
A. 12		Deve essere considerata la cifratura delle unità d'archiviazione sulle quali sono presenti dati personali, quali dischi rigidi (HD), dischi e chiavette USB, DVD ecc., adottandola dove possibile
A. 12		Per i file, record o campi più critici devono essere considerate 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. 14.1	**Security requirements of information systems**	Gli utenti non devono essere in grado di disattivare o aggirare le impostazioni di sicurezza. Le applicazioni anti-virus 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		Le policy adottate non devono consentire agli utenti di installare applicazioni senza autorizzazione
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.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. 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 pre-registrati 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.12.6 & A.14.2	**Technical vulnerability management & Security in development and support processes**	Devono essere ottenute informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati.
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 sottioposti 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.11	**Physical and environmental security**	I sistemi server non devono essere fisicamente collocati in aree accessibili al pubblico

CONVENZIONE PER FORNITURA DI PRESTAZIONI SPECIALISTICHE DI LABORATORIO ANALISI

Tra

L'Azienda USL di Bologna (di seguito AUSL di Bologna), con sede in Bologna, via Castiglione 29, Partita Iva e Codice fiscale 02406911202, nella persona del Direttore Generale e legale rappresentante *p.t*. Dott. Paolo Bordon;

e

Villa Torri Hospital S.r.l. (di seguito Villa Torri), con sede in Bologna, Viale Quirico Filopanti 12, Codice Fiscale e P.Iva 02383150394, nella persona dell'Amministratore Delegato e legale rappresentante Dott. Lorenzo Venturini;

- Richiamati il D.lgs. 502/92 e ss.mm.ii. e - da ultimo - la L.R. 22/2019 e ss.mm.ii. in materia di autorizzazione e accreditamento sanitario e la relativa delibera di attuazione DGR 886/2022, in particolare nella parte che prevede la possibilità per le Strutture sanitarie accreditate di acquisire all'esterno prestazioni sanitarie complementari al processo diagnostico-assistenziale, ricorrendone i presupposti;
- Richiamata inoltre la normativa generale in materia di incompatibilità di cui all'art. 4, comma 7, della legge 412/91;
- Premesso che Villa Torri Hospital è società appartenente al Gruppo Villa Maria S.p.A. - GVM Care & Research, e gestisce l'omonima struttura ospedaliera, accreditata con il Servizio Sanitario Nazionale;
- Premesso che Villa Torri Hospital ha chiesto all'Azienda USL di Bologna di poter usufruire di prestazioni urgenti di laboratorio a favore di propri pazienti ricoverati, prestazioni che, in condizione di urgenza, possono essere erogate dall'Azienda USL anche se la struttura privata è accreditata per questa attività;

Tutto quanto sopra premesso, si conviene e stipula quanto segue:

Art 1 Oggetto

L'AUSL di Bologna si rende disponibile a garantire a Villa Torri, nell'ambito dell'attività istituzionale, prestazioni specialistiche di laboratorio richieste in emergenza e urgenza a favore di pazienti ricoverati presso la propria struttura. L'AUSL di Bologna assicura le prestazioni attraverso il LUM – Laboratorio Unico Metropolitano presso il laboratorio spoke sito c/o l'Ospedale Sant'Orsola indicativamente stimate per tipologia e volume annuo di attività, in circa 2000 richieste/anno.

Art 2 Modalità di esecuzione

Villa Torri si impegna a inviare la richiesta in formato informatico inserita per il mezzo dell'applicativo DNTerritorio. Le provette dovranno pervenire debitamente etichettate e consegnate presso il Laboratorio spoke sito c/o l'Ospedale Sant'Orsola di Bologna, come da prassi consolidata.

I contenitori necessari all'esecuzione dei prelievi possono essere richiesti mezzo mail all'indirizzo segreterialum@ausl.bologna.it; tali contenitori saranno depositati in giacenza presso il locale Accettazione Materiale dell'Ospedale Maggiore, Edificio LUM - Piano terra, ove potrà essere ritirato dal personale di Villa Torri dal Lunedì al Venerdì dalle ore 8,00 alle ore 15,00 e il sabato dalle ore 8,00 alle ore 12,00. Il costo dei contenitori deve considerarsi incluso nella tariffa delle prestazioni.

Villa Torri inoltre assume gli oneri relativi al trasporto del materiale biologico da analizzare, nonché delle responsabilità che ne derivano.

L'AUSL di Bologna, attraverso il Laboratorio Unico Metropolitano, si impegna ad effettuare le prestazioni richieste nell'ambito dell'attività istituzionale.

L'utilizzo dell'applicativo informatico DNTerritorio consente la visualizzazione del referto al momento della sua conclusione rendendo superflua la stampa cartacea e la consegna che si considerano effettuate in tempo reale mediante la procedura informatica.

Direttore del Laboratorio Unico Metropolitano è la d.ssa Rita Mancini.

Art 3 Compensi

Per le prestazioni eseguite dal Laboratorio Unico Metropolitano, l'AUSL di Bologna provvederà ad emettere fattura con cadenza trimestrale. Le parti concordano che, in considerazione del fatto che l'attività di cui trattasi viene svolta in urgenza, alle prestazioni viene applicata la tariffa prevista dal Nomenclatore Tariffario della Regione Emilia Romagna in vigore, maggiorata del 10%.

Villa Torri si impegna a corrispondere alla AUSL di Bologna gli importi dovuti nei termini e con le modalità indicate nella fattura stessa.

Art. 4 – Inadempimenti

In caso di inadempimento, la parte creditrice della prestazione inadempiuta, può intimare per iscritto all'altra parte, mediante comunicazione inoltrata tramite PEC, di adempiere entro un congruo termine, comunque non inferiore a 15 giorni.

Decorso inutilmente detto termine, la convenzione si intenderà risolta.

Art 5 Privacy

Le Parti si impegnano, per quanto di rispettiva competenza, ad adempiere alle disposizioni del Regolamento Europeo 2016/679 ("GDPR") e, per quanto applicabile, del D.Lgs. n. 196/2003, Codice in materia di protezione dei dati personali e successive modifiche e integrazioni ("Codice Privacy"), nonché, in

generale, ai provvedimenti e linee guida emanati dal Garante per la Protezione dei Dati Personali e alla normativa, nazionale e non, di tempo in tempo vigenti ed applicabili in materia di tutela dei dati personali.
Le Parti riconoscono e si danno reciprocamente atto che, ai sensi di quanto previsto dagli artt. 13 e 14 del Regolamento (UE) 2016/679 ("GDPR"), i dati personali, relativi ai rispettivi dipendenti, collaboratori, agenti, amministratori e, in generale, del personale aziendale (di seguito anche "Referenti"), eventualmente comunicati tra le Parti, direttamente e/o accidentalmente, nell'ambito dell'esecuzione del rapporto contrattuale, saranno trattati dall'altra Parte in qualità di autonomo Titolare del Trattamento.
Fermo restando quanto precede, le Parti prendono atto che, in occasione ed in funzione dell'esecuzione del presente contratto, l'AUSL di Bologna viene a conoscenza di dati personali ulteriori rispetto a quelli dei Referenti, relativi ai pazienti (tra cui dati comuni e dati idonei a rivelare lo stato di salute dell'interessato), in relazione ai quali Villa Torri Hospital si qualifica quale Titolare del Trattamento.
Le Parti, dunque, concordano che, in conformità con le disposizioni del GDPR, AUSL di Bologna viene nominato da Villa Torri Hospital, ai sensi e per gli effetti dell'art. 28 del GDPR, quale "Responsabile del Trattamento" di tali dati, a mezzo di sottoscrizione di separato atto, a cui le Parti fin da ora rimandano e che dovrà ritenersi parte integrante ed essenziale della presente convenzione.

Art 6 Divieto di "pantouflage"
Con la sottoscrizione del presente atto, Villa Torri dichiara, per quanto in sua conoscenza, di non aver concluso nei tre anni successivi alla loro cessazione dal rapporto di lavoro, contratti di lavoro subordinato o autonomo e, comunque, di non aver attribuito incarichi ad ex dipendenti e/o lavoratori autonomi che hanno esercitato poteri autoritativi o negoziali per conto dell'Azienda USL di Bologna nel triennio antecendente alla cessazione stessa e di essere consapevole che, ai sensi dell' art. 53, comma 16-ter D.lgs. 165/2001, i contratti conclusi e gli incarichi conferiti in violazione del divieto previsto da tale disposizione sono nulli e che è fatto divieto ai soggetti privati che li hanno conclusi o conferiti di contrattare con le pubbliche amministrazioni per i successivi tre anni, con l'obbligo di restituzione dei compensi eventualmente percepiti.

Art 7 Responsabilità
Le parti convengono che Villa Torri rimarrà, ad ogni effetto di legge, unica titolare e responsabile nei confronti dei terzi in genere dell'attività di laboratorio intesa nel suo complesso, dalla fase del prelievo sino alla consegna del referto.
L'AUSL Bologna risponderà del proprio operato esclusivamente nei confronti di Villa Torri, impegnandosi pertanto a tenerla completamente indenne e manlevata da qualsiasi conseguenza, onere, danno o nocumento che derivasse esclusivamente dalla propria specifica attività o da fatti imputabili alla stessa nell'esecuzione delle prestazioni di cui al presente contratto.

Art 8 Foro competente

Per ogni eventuale controversia relativa all'interpretazione o esecuzione della presente convenzione si individua quale foro competente il Tribunale di Bologna.

Art 9 Durata

La validità della presente convenzione decorre dalla data dell'ultima sottoscrizione fino al 31 dicembre 2025, facendo salva e riconoscendo l'eventuale attività resa antecedentemente, nelle more della formalizzazione degli atti.

Il rinnovo dovrà essere chiesto preventivamente per iscritto a mezzo PEC.

La presente convenzione può essere disdetta anche prima della scadenza, previa comunicazione scritta di una delle parti un mese prima della data di cessazione.

Art 10 Registrazione e imposta di bollo

La presente convenzione è soggetta a registrazione solo in caso d'uso ai sensi dell'art. 10 del DPR 26/4/1986 N. 131. TARIFFE - parte seconda. Le spese di registrazione saranno a carico della parte che con proprio comportamento ne avrà resa obbligatoria la registrazione.

La presente convenzione è altresì soggetta all'imposta di bollo ai sensi dell'art. 2, Tariffa, parte prima - allegata al D.P.R 642/72, così come disposto dalla Risoluzione 86/E del 13/3/2002 dell'Agenzia delle Entrate - Direzione Centrale Normativa e Contenzioso. Le spese di bollo sono a carico di Villa Torri in quanto soggetto beneficiario delle prestazioni.

Si allega: atto di nomina a responsabile del trattamento dati personali.

Letto, approvato e sottoscritto in modalità digitale, in difetto di contestualità spazio/temporale, secondo il combinato disposto dell'art. 15, co. 2 bis, della L. 241/1990 e ss.mm.ii. e dell'art. 24 del D.lgs. 82/2005.

Bologna, data dell'ultima sottoscrizione.

Per l'Azienda USL di Bologna	**Per Villa Torri Hospital S.r.l.**
Il Direttore Generale	L'Amministratore Delegato
Dott. Paolo Bordon	Dott. Lorenzo Venturini