NOMINA A PERSONA AUTORIZZATA AL TRATTAMENTO DI DATI PERSONALI

ai sensi del Regolamento UE 2016/679

Per il dott./dott.ssa _____

C.F._____

impiegato presso l'UCBM con la mansione di:_____Medico in formazione_____

("Incaricato")

Carlo Tosti, c.f. 97087620585 e p.IVA 04802051005, con sede in Via Alvaro del Portillo 21, 00128, quale titolare del trattamento

(**"Titolare"**),

PREMESSO CHE

- Il Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (**"Regolamento"**) abroga la Direttiva 95/46/CE e le implementazioni della stessa;

- l'art. 29 del Regolamento prevede che le operazioni di trattamento possono essere svolte solo da soggetti "autorizzati" che operano sotto la diretta autorità del titolare o del responsabile del trattamento; tali soggetti, devono attenersi, nell'effettuare le attività di trattamento, alle istruzioni loro impartite e la loro designazione, effettuata per iscritto, deve individuare l'ambito del trattamento consentito;

- l'art. 32 del Regolamento prevede che "il titolare del trattamento e il responsabile del trattamento fanno si che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

-i trattamenti di dati oggetto della presente autorizzazione vanno ricondotti al contesto emergenziale delineato dal decreto legge 9 marzo 2020 n. 14 "Disposizioni urgenti per il potenziamento del servizio sanitario nazionale in relazione all'emergenza Covid.19", e, in particolare dall'art. 14;

- ai sensi dell'art. 2 - quaterdecies del D.lgs. 196/2003 ("Codice Privacy") il titolare o il responsabile del trattamento possono (i) prevedere sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità; (ii) individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta;

- l'art. 28 del Regolamento richiede che le persone autorizzate al trattamento dei dati personali si impegnino alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

- nell'Intranet aziendale sono presenti e costantemente aggiornate le informazioni sulle sanzioni più rilevanti in materia di trattamento dei dati personali ex Art. 7 Statuto dei lavoratori (L. 20 maggio 1970, n.300), nonché sulle procedure aziendali rilevanti ai fini della corretta applicazione delle normative in materia di protezione dei dati da parte del titolare e delle persone autorizzate dal medesimo al trattamento dei dati, consultabili al seguente link: http://campusnet.unicampus-int.it/ucbm/1790;

- fanno parte integrale del presente atto il ***Regolamento per la richiesta e l'uso delle risorse informatiche*** nonché il ***Regolamento interno per la protezione dei dati personali*** presente sulla Intranet aziendale e consultabile al seguente indirizzo http://campusnet/ucbm/1101-regolamenti-comuni-a-tutta-listituzione e che la persona autorizzata li ha previamente esaminati e compresi;

NOMINA

persona **"autorizzata al trattamento dei dati"** Il/la Sig./Sig.ra_____(**"incaricato"**) in servizio presso Direzione/Area_____che, nello svolgimento della propria mansione di ed in virtù della stesse, tratterà dati personali per conto del Titolare come

specificato nell' allegato 1 (Perimetro funzionale di trattamento dei dati e profili di autorizzazione) che si considera parte integrante della presente lettera.

Il/la Sig./Sig.ra_____ sarà autorizzata/o ad accedere alle banche dati/archivi/documenti indicate/i nell'allegato Allegato 1 "Perimetro funzionale di trattamento dei dati e profili di autorizzazione" sui/sulle quali potrà effettuare solo le operazioni di trattamento strettamente necessarie alle funzioni esercitate.

OBBLIGHI

L'incaricato si impegna a mantenere il segreto professionale e l'assoluta riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti ad esso assegnati.

L'Incaricato dovrà effettuare il trattamento dei dati nel rispetto della normativa vigente e delle misure di sicurezza indicate dal Titolare. L'incaricato dovrà svolgere il trattamento dei dati personali nell'ambito consentito così come individuato dal Titolare per le finalità e secondo le modalità da lui stabilite, anche in futuro. Il trattamento dei dati personali dovrà avvenire in modo lecito secondo correttezza e nel pieno rispetto della dignità dell'interessato; in particolare dovrà fare quanto di seguito precisato:

a) raccogliere e in qualsiasi modo trattare dati personali non oltre quanto necessario alle esigenze ed allo svolgimento delle proprie mansioni/attività lavorative;

b) non trattare i dati per finalità diverse da quelle per cui si è stati autorizzati;

c) sottoporsi agli interventi di formazione obbligatoria e aggiornamento sulla normativa in materia di trattamento dei dati personali che il Titolare fornisce attraverso le strutture, interne ed esterne, a ciò deputate;

d) comunicare e/o diffondere dati personali esclusivamente ai soggetti indicati dal Titolare e secondo le modalità stabilite dal medesimo;

e) non estrarre copia di banche dati o di singoli dati o creare nuove ed autonome banche dati al di fuori di quanto necessario alle mansioni lavorative;

f) Accertarsi che il device aziendale in dotazione sia protetto da una chiave di accesso composta da almeno otto caratteri alfanumerici e non contenga riferimenti agevolmente riconducibili all'incaricato;

g) Modificare il proprio codice d'accesso al primo utilizzo e, successivamente, ogni 3 mesi; in caso di dubbi, anche minimi, sulla possibilità che la segretezza della password sia stata compromessa dovrà immediatamente procedere alla sostituzione della stessa e darne comunicazione al Titolare;

h) non comunicare o rendere conoscibile a terzi il proprio codice di accesso e/o consentire a terzi di utilizzare il device aziendale e/o accedere ai dati per nessun motivo; senza previa autorizzazione del Titolare;

i) non salvare i dati in locale sul device aziendale;

j) il device aziendale è assegnato per utilizzo esclusivamente lavorativo; non utilizzarlo a scopo personale, non consultare internet e la posta elettronica a fini privati da tali dispositivi ovvero ascoltare o scaricare file audio o video, se non a fini prettamente lavorativi;

k) non modificare le configurazioni pre-impostate sul proprio device e/o scaricare ulteriori applicazioni o programmi senza previa espressa autorizzazione del Titolare;

l) non lasciare incustodito o accessibile a terzi il device aziendale;

m) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate senza mantenerne copia; quando tali atti e i documenti contengano speciali categorie didati personali e sono affidati all'Incaricato per lo svolgimento dei relativi compiti, quest'ultimo deve controllare e custodire i medesimi atti e documenti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e deve restituirli al termine delle operazioni affidate;

n) archiviare e custodire i documenti all'interno di armadi\mobili\cassetti muniti di

serratura. Conservare le chiavi con diligenza e restituirle al dipendente responsabile delle stesse; non lasciare le chiavi nella serratura o comunque in un luogo facilmente accessibile al termine della giornata lavorativa. Chiudere a chiave l'archivio (armadio, cassetto ecc.) o l'ufficio durante la giornata, in caso di allontanamento dall'ufficio (es. in occasione di pausa, riunioni, ecc.), al fine di impedire l'accesso da parte di persone non autorizzate.

o) prima di gettare nel cestino documenti cartacei contenenti eventuali dati personali, l'incaricato dovrà procedere alla loro distruzione, strappandoli o utilizzando un apposito distruggi documenti.

p) non effettuare copie di dati personali tantomeno su supporti elettronici rimovibili, a meno di espressa autorizzazione del Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;

q) conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

r) curare, in caso di utilizzo autorizzato di eventuali supporti di memorizzazione che i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori (devono essere utilizzati soltanto supporti vergini o vuoti);

s) dare immediata comunicazione, secondo quanto previsto nella procedura di gestione delle violazioni dei dati personali, al Referente Privacy di riferimento nel caso constati o sospetti un incidente di sicurezza, affinché quest'ultimo provveda a informare il Titolare e il Data Protection Officer;

t) rendere all'Interessato l'informativa appositamente redatta dal Titolare e visionata dal Data Protection Officer e, ove necessario, ottenere il consenso al trattamento dei dati; inoltre, non raccogliere dati relativi alla salute dei pazienti/interessati; a meno che sia strettamente necessario alla finalità del trattamento dei dati in oggetto (es. assistenza pazienti, cura ecc..), e previo consenso, adeguatamente informato dell'interessato, al

trattamento dei suoi dati sensibili;

u) dare seguito alle richieste ai sensi degli art. 15 e ss. del Regolamento, degli interessati (tra cui le richieste di opposizione al trattamento, di limitazione, di rettifica dei dati o di loro cancellazione, etc.) nei tempi e nei modi previsti nella "Procedura aziendale sull'esercizio dei diritti degli interessati" che si intende ivi integralmente richiamata e disponibile nella intranet aziendale, nella sezione privacy, al link http://campusnet.unicampus-int.it/ucbm/1790 .Qualora uno o più interessati denunci situazioni o fatti rilevanti di particolare gravità, informare tempestivamente il Referenti Privacy (o Referente interno), affinché a sua volta comunichi la richiesta al Titolare e al Data Protection Officer che adottano tutte le misure precauzionali e/o riparatorie necessarie;

v) prestare attenzione allo spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul pavimento (ove presente) ovvero, dietro le barriere o il paravento delimitanti lo spazio di riservatezza;

w) nel corso delle visite e/o interventi alla presenza di studenti autorizzati, adottare cautele specifiche volte a limitare il disagio dei pazienti, anche in relazione al grado di invasività del trattamento, circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie del paziente;

x) assicurarsi che la comunicazione di dati idonei a rivelare lo stato di salute sia sempre effettuata da personale medico o sanitario incaricato, salvo che tale comunicazione sia specificamente prevista nell'ambito delle mansioni svolte e nel rispetto della legge e dei regolamenti;

y) adottare idonee cautele in relazione allo svolgimento di colloqui con il paziente per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi; in particolare, la diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata (es. la comunicazione ad organi di informazione);

z) adottare idonee cautele per comunicare una prestazione di pronto soccorso a soggetti terzi, rispetto al paziente/interessato, al fine di accertarsi che siano legittimati ad

ottenere tali informazioni;

aa) dare, ai terzi legittimati, solo l'informazione della prestazione che è in atto o si è svolta una prestazione di pronto soccorso, e non anche ulteriori dettagli sullo stato di salute del paziente;

bb) fornire informazioni sullo stato di salute a soggetti diversi dall'interessato solo se lo stesso o altro soggetto a ciò legittimato ((in caso di impossibilità fisica, incapacità di agire o di intendere e/o volere del paziente/interessato) abbia manifestato un consenso esplicito e distinto al riguardo;

cc) nel fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato, dare solo la informazione della presenza nel reparto del paziente/interessato e non anche informazioni sul suo stato di salute;

dd) non deve affiggere le liste dei pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento operatorio;

ee) Adottare idonee cautele per evitare che siano resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'interessato (es. cartelle infermieristiche poste in prossimità del letto di degenza);

ff) Accertarsi di rendere la comunicazione degli esiti di esami clinici effettuati, accompagnata da un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta;

gg) consegnare i documenti contenenti referti diagnostici rilasciati dai laboratori di analisi, anche a persone diverse dai diretti interessati, previa verifica dell'identità del soggetto delegato e solo sulla base di una delega scritta e mediante la consegna in busta chiusa e sigillata; diversamente, i risultati di accertamenti diagnostici per infezione da HIV deve essere rilasciato esclusivamente, in busta chiusa e sigillata, alla persona che lo ha

effettuato.

hh) accertarsi che l'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente sia sempre preceduto dall'autorizzazione dell'interessato e autorizzato dal titolare del trattamento e sempre contenuto in una busta sigillata evitando di riportare sulla stessa riferimenti a servizi/strutture specifici che possano in qualche modo essere idonei a rivelare lo stato di salute dell'interessato o creare una forma di associazione con qualsivoglia patologia;

ii) Informazioni e dati personali comuni e sensibili non possono essere trattati telefonicamente tranne che nel caso in cui l'interlocutore sia una persona autorizzata ad accedere ai dati richiesti e non vi sono dubbi circa la sua identità. Durante la conversazione non devono essere presenti persone non autorizzate a conoscere i dati eventualmente comunicati. In ogni caso in cui sia necessario trattare verbalmente dati personali, in particolare se di natura sensibile, in situazioni di promiscuità con terzi estranei al trattamento stesso, dovranno essere adottate cautele atte ad evitare l'indebito ascolto della conversazione, ad esempio usando toni di voce adeguati o evitando di ripetere a voce alta dati identificativi o relativi alla salute dell'interessato. Le medesime cautele devono essere adottate anche nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

L'incaricato dovrà segnalare al Referente di riferimento, affinché questi provveda ad informare il Titolare e il Data Protection Officer, eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

L'incaricato è tenuto a rispettare le procedure per la sicurezza dei dati che gli verranno indicate dal Titolare del trattamento dei dati personali.

L'incaricato dovrà informare tempestivamente al Referente Privacy di riferimento, affinché questi provveda ad informare il Titolare e il Data Protection Officer, quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può

determinare, ritenga vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati.

L'incaricato dovrà fornire al Titolare e/o al Data Protection Officer, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo; e, più in generale, prestare la più ampia e completa collaborazione al Titolare e/o al Data Protection Officer al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.
L'incaricato è autorizzato dal Titolare a comunicare all'interessato informazioni sul suo stato di salute.
Potranno essere registrate dalla Società, in appositi file log, gli accessi e tutte le operazioni compiute sui Dossier Sanitari e Fascicolo Sanitario Elettronico, comprese quelle di semplice consultazione. In particolare, potranno essere registrate automaticamente le seguenti informazioni: il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del soggetto a cui i dati, interessati dall'operazione di accesso, si riferiscono e la tipologia dell'operazione compiuta sui dati. Il Titolare verificherà i suddetti log per il controllo per verificare le anomalie nella frequenza degli accessi e nelle loro modalità, la legittimità degli accessi ai dati effettuati dagli incaricati, l'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento; nonché per riscontrare il diritto del paziente/interessato alla visione degli accessi nel proprio Dossier Sanitario Elettronico e/o Fascicolo Sanitario Elettronico.

Istruzioni ulteriori possono essere presenti nel ***Regolamento per la richiesta e l'uso delle risorse informatiche*** nonché il ***Regolamento interno per la protezione dei dati personali*** nella Intranet aziendale, e possono essere modificate in conformità con le modifiche della normativa vigente. L'incaricato si impegna a controllare periodicamente il contenuto dell'Intranet, che si considera parte integrante della presente lettera di nomina.

L'accesso all'account di posta elettronica aziendale dell'Incaricato (_____._____@unicampus.it) potrà essere effettuato dal Titolare, anche a mezzo dei Fiduciari nominati, secondo le modalità specificate ***Regolamento per la richiesta e l'uso delle risorse informatiche*** presente sulla Intranet aziendale e consultabile al seguente indirizzo: http://campusnet.unicampus-int.it/ucbm/1790

Ai fini appena esposti, e coerentemente con il ***Regolamento per la richiesta e l'uso delle risorse informatiche*** nonché il ***Regolamento interno per la protezione dei dati personali*** presenti sulla Intranet aziendale. l'Incaricato nomina due Fiduciari:

Nome e cognome del primo Fiduciario:

_____

Nome e cognome del secondo Fiduciario:

_____

L'Incaricato prende atto che opererà sotto la diretta autorità del Titolare il quale avrà facoltà di:

a) modificare di volta in volta il profilo di autorizzazione dell'Incaricato secondo le modalità di cui all'Allegato A della presente nomina.

b) revocare in ogni momento il presente incarico. Le revoche saranno effettuate con effetto immediato e senza obbligo di preavviso.

La presente nomina si intenderà automaticamente revocata nel caso di cessazione, per qualsivoglia motivo, del rapporto di lavoro/consulenza/collaborazione con la Società.

L'Incaricato sottoscritto prende atto e accetta quanto previsto nella presente nomina e dalla normativa vigente ed assume la qualifica di Incaricato.

Allegati
1. Perimetro funzionale di trattamento dei dati e profili di autorizzazione

Data e luogo

Per il Titolare il legale rappresentante *pro tempore*

Per accettazione

l'Incaricato

X

INFORMATIVA RILASCIATA AI SENSI DELL'ART. 13 DEL REGOLAMENTO 679/2016

Fatto salvo quanto già indicato nell'informativa ex art. 13 del GDPR rilasciata in sede di assunzione, ed a integrazione della stessa, che ivi si intende integralmente richiamata, La informiamo, anche con riferimento alle tutele di cui all'art. 4 della L. n. 300/70 (Statuto dei Lavoratori che potranno essere registrate dalla Società, in appositi file log, come indicato nell'incarico, in ottemperanza a quanto prescritto nei provvedimenti "Linee guida in materia di Dossier sanitario" del 4 giugno 2015 – G.U. n. 164 del 17 luglio 2015; "Prescrizioni in tema di Fascicolo sanitario elettronico (Fse)" del 16 luglio 2009 - G.U. n. 178 del 3 agosto 2009, per cui la base di legittimità del trattamento è da rinvenirsi nell'art. 6.1.c) del GDPR; gli accessi e le operazioni compiute sui sistemi contenenti dati idonei a rivelare lo stato di salute degli interessati. I dati identificativi e i dati sugli accessi (il codice identificativo del soggetto incaricato che ha posto in essere l'operazione di accesso; la data e l'ora di esecuzione; il codice della postazione di lavoro utilizzata; l'identificativo del soggetto a cui i dati, interessati dall'operazione di accesso, si riferiscono e la tipologia dell'operazione compiuta sui dati) saranno, dunque, trattati dalla Società per il controllo sulla legittimità degli accessi oltre che per finalità di sicurezza informatica, in particolare, per verificare anomalie nella frequenza degli accessi e nelle loro modalità, la legittimità degli accessi ai dati effettuati dagli incaricati, l'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento e per riscontrare al diritto di visione degli accessi da parte dei pazienti/interessati a cui vengono, su richiesta, comunicati. Tali trattamenti avverranno solo con strumenti elettronici e sono obbligatori e non facoltativi, non potendo essere rifiutati da lei se non cambiando funzione. Il Titolare conserva i log per un periodo di 24 mesi dalla data di registrazione dell'operazione per cui, successivamente, vengono cancellati in maniera permanente.

Lei ha diritto di chiedere alla Società, in qualunque momento, l'accesso ai suoi Dati Personali, la rettifica o la cancellazione degli stessi o di opporsi al loro Trattamento, ha diritto di richiedere la limitazione del Trattamento nei casi previsti dall'art. 18 del Regolamento UE 2016/679, nonché di ottenere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati che la riguardano, nei casi previsti dall'art. 20 del Regolamento.

La informiamo, infine, che Lei ha diritto di opposi al trattamento dei suoi dati ai sensi dell'art. 21 del Regolamento.

In ogni caso ha sempre diritto di proporre reclamo all'Autorità di Controllo competente (Garante per la Protezione dei Dati Personali), ai sensi dell'art. 77 del Regolamento, qualora ritenga che il Trattamento dei Suoi Dati Personali sia contrario alla normativa in vigore.

Le richieste vanno rivolte per iscritto alla Società al seguente indirizzo: Via Alvaro del Portillo 21 ,00128 ovvero al Privacy officer "DPO" contattabile al seguente indirizzo e-mail dpo@unicampus.it.

ALLEGATO A

ai sensi del Regolamento

Il Titolare,

AGGIORNA

la Nomina a persona autorizzata al trattamento di dati personali stabilendo che l'Incaricato apparterrà al seguente ufficio/area di appartenenza:_____.

L'Incaricato conferma l'impegno a controllare periodicamente il contenuto dell'Intranet dove troverà ulteriori istruzioni aggiornate alla normativa vigente.

L'Incaricato sottoscritto prende atto e accetta quanto previsto nel presente Allegato A.

Data e luogo

Per il Titolare il legale rappresentante *pro tempore*

_____ _____

Per accettazione
L'Incaricato

X_____

Allegato 1

1. Perimetro funzionale di trattamento dei dati e profili di autorizzazione

In virtù della presente nomina, a Lei è consentito:

Svolgere operazioni di trattamento relative alle seguenti tipologie di dati personali:

Tipologia del dato	SI	NO
Dati anagrafici dei pazienti del Policlinico	☒	☐
Dati sanitari dei pazienti del Policlinico ivi comprese le immagini idonee a rilevarne lo stato di salute	☒	☐
Dati anagrafici relativi agli studenti dell'Università	☐	☒
Dati relativi alla carriera accademica degli studenti dell'Università	☐	☒
Dati anagrafici relativi ai dipendenti e collaboratori dell'Università	☐	☒
Dati relativi al rapporto di lavoro e alla carriera dei dipendenti e collaboratori dell'Università	☐	☒
Dati anagrafici relativi a personale non dipendente ma comunque operativo presso l'Università o in relazione con essa (volontari, amici del Campus, ecc.)	☐	☒
Dati personali relativi ai Fornitori dell'Università	☐	☒
Dati relativi alla gestione del contenzioso e del sistema di videosorveglianza	☐	☒
Altro (specificare)_____	☐	☒

Svolgere operazioni di trattamento relative alle seguenti categorie di interessati:

Categorie di interessati	SI	NO
Pazienti visitati negli ambulatori afferenti all'U.O. di appartenenza	☒	☐
Pazienti ricoverati presso l'U.O. di appartenenza	☒	☐
Studenti dell'Università	☐	☒
Dipendenti e collaboratori dell'Università	☐	☒

Categorie di interessati	SI	NO
Personale non dipendente ma comunque operativo presso l'Università o in relazione con essa	☐	☒
Fornitori	☐	☒
Visitatori	☐	☒
Altro (specificare)_____	☐	☒

Svolgere operazioni di trattamento sui dati per il perseguimento delle seguenti finalità:

Finalità delle operazioni di trattamento	SI	NO
Erogazione della prestazione assistenziale medica	☒	☐
Erogazione della prestazione assistenziale infermieristica	☐	☒
Compilazione di cartelle cliniche, di certificati e di altri documenti di tipo sanitario	☒	☐
Amministrazione del personale dipendente o collaboratore dell'Università	☐	☒
Amministrazione degli studenti dell'Università	☐	☒
Formazione del personale e degli studenti dell'Università	☐	☒
Gestione dei fornitori	☐	☒
Sicurezza	☐	☒
Altro (specificare) _____	☐	☒

Svolgere operazioni di trattamento sui dati con l'ausilio dei seguenti strumenti:

Strumenti	SI	NO
Archivio cartaceo	☒	☐
Strumenti informatici	☒	☐
Strumenti o apparecchiature biomediche	☒	☐

Sistemi di videosorveglianza	☐	☒
Altro (specificare) _____	☐	☒