ISTRUZIONI PER IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI ex ART. 28 GDPR

OBBLIGHI DELLE PARTI

Il Responsabile del trattamento tratta i dati personali per conto del Titolare del trattamento soltanto su istruzione documentata del Titolare stesso ed esclusivamente ai fini specifici della esecuzione dei servizi oggetto del contratto/convenzione, nel rispetto della normativa vigente in materia di protezione dei dati personali, nonché delle istruzioni impartite dal Titolare nel presente Atto o in atti successivi.

Il Titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

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

Il Responsabile del trattamento informa immediatamente il Titolare del trattamento di ogni questione rilevante ai fini di legge; in particolare 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, le istruzioni del Titolare del trattamento violino il GDPR o le disposizioni applicabili, nazionali o dell'Unione, relative 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 dal Titolare e/o conformarsi alla normativa o a provvedimenti dell'Autorità di Controllo.

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

- ***persone preposte allo svolgimento di operazioni di trattamento sui dati personali:***

- sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, **designa** espressamente e per iscritto i dipendenti e i collaboratori autorizzati/incaricati allo svolgimento di operazioni di trattamento sui dati personali oggetto del contratto, attribuendo loro specifici compiti e funzioni ed impartendo adeguate informazioni ed istruzioni;
- al fine di garantire un trattamento corretto, lecito e sicuro **si adopera** per rendere effettive le suddette istruzioni, curando la formazione di tali soggetti - sia in tema di protezione dei dati personali che, ove occorra, di sicurezza informatica - vigilando sul loro operato, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento delle loro attività, anche successivamente alla cessazione del rapporto di lavoro/collaborazione con la Ditta stessa;
- **concede l'accesso** ai dati personali oggetto di trattamento a soggetti autorizzati/incaricati soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto;

- ***registro delle attività di trattamento:***

ove ne sia tenuto, **identifica e censisce** i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività oggetto del rapporto convenzionale, al fine di predisporre il registro delle attività di trattamento svolte per conto del Titolare da esibire in caso di ispezione della Autorità Garante, i cui contenuti devono corrispondere almeno a quanto indicato dall'art. 30 del GDPR;

- ***obblighi di sicurezza:***

- qualora faccia accesso ai sistemi informativi e ai dispositivi del Titolare, **mette in atto** le misure tecniche e organizzative specificate nell'Allegato 2;
- in ogni caso **adotta** le misure tecniche e organizzative indicate nel suddetto Allegato 2, per garantire la sicurezza, la riservatezza e l'integrità dei dati personali, tenendo conto dei rischi di varia probabilità e gravità (di distruzione o perdita, di modifica, di divulgazione non autorizzata o di accesso accidentale o illegale a dati trasmessi, conservati o comunque trattati), dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento;

In particolare:

- **definisce una politica di sicurezza** per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- **si impegna** ad utilizzare strumenti, applicazioni e/o servizi che rispettino i principi di protezione dei dati personali fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*).
- **assicura** la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- **definisce una procedura** per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
- **applica limitazioni specifiche e/o garanzie supplementari** se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati («c.d. categorie particolari di dati»);

- ***notifica di una violazione dei dati personali***

- in caso di violazione dei dati personali, **coopera** con il Titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;

- in caso di violazione riguardante dati trattati dal Titolare del trattamento, **assiste** il Titolare del trattamento:
  a) nel notificare la violazione dei dati personali all'Autorità Garante per la protezione dei dati personali, senza ingiustificato ritardo dopo che il Titolare del trattamento ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
  b) nell'ottenere le seguenti informazioni che, in conformità all'articolo 33, par. 3 del GDPR, devono essere indicate nella notifica del Titolare del trattamento e includere almeno:
     - la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
     - le probabili conseguenze della violazione dei dati personali;
     - le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
  c) nell'adempiere, in conformità all'articolo 34 del GDPR, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

- in caso di violazione dei dati personali trattati dal Responsabile del trattamento, quest'ultimo ne dà notifica al Titolare del trattamento senza ingiustificato ritardo – comunque entro 24 ore - dopo esserne venuto a conoscenza. La notifica contiene almeno:
  a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
  b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
  c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

A tal fine il Responsabile può avvalersi della procedura predisposta dal Titolare del trattamento, prendendone visione nella sezione Privacy del sito internet del Titolare: https://www.aou.mo.it/privacy_dipendenti_responsabili_esterni. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

Le parti stabiliscono nell'Allegato 2 tutti gli altri elementi che il Responsabile del trattamento è tenuto a fornire quando assiste il Titolare del trattamento nell'adempimento degli obblighi che incombono sul Titolare del trattamento a norma degli articoli 33 e 34 del GDPR;

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

conformemente al Provvedimento della Autorità Garante del 27 novembre 2008 e s.i.m., in tema di amministratori di sistema, si impegna a:

- designare quali amministratori di sistema le figure professionali dedicate alla gestione e alla manutenzione di impianti di elaborazione o di loro componenti con cui vengono effettuati trattamenti di dati personali;
- predisporre e conservare l'elenco contenente gli estremi identificativi delle persone fisiche qualificate quali amministratori di sistema e le funzioni ad essi attribuite;
- verificare annualmente l'operato degli amministratori di sistema, informando il Titolare circa le risultanze di tale verifica;
- mantenere i file di log previsti in conformità a quanto previsto nel suddetto Provvedimento.

➢ ***assistenza al Titolare del trattamento***

- **notifica** prontamente al Titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal Titolare del trattamento.
- **assiste** il Titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere a tali obblighi il Responsabile del trattamento si attiene alle istruzioni del Titolare del trattamento;
- **collabora** con il Data Protection Officer (DPO) del Titolare del trattamento, provvedendo a fornire ogni informazione dal medesimo richiesta;
- solamente nell'ipotesi in cui il trattamento dei dati personali oggetto del rapporto convenzionale comporti la raccolta di dati personali da parte del Responsabile del trattamento, questi **provvede** al rilascio della relativa informativa ai soggetti interessati; inoltre, solamente qualora tale raccolta di dati personali avvenga in luoghi ad accesso pubblico, il Responsabile del trattamento **provvede ad affiggere** in tali luoghi i cartelli contenenti l'informativa, con la precisazione che l'informazione resa attraverso la cartellonistica integra, ma non sostituisce l'obbligo di informativa in forma orale o scritta.
- **provvede** ad informare immediatamente il Titolare del trattamento di ogni richiesta, ordine ovvero attività di controllo da parte dell'Autorità Garante per la protezione dei dati personali o dell'Autorità Giudiziaria e coadiuva il Titolare stesso nella difesa in caso di procedimenti dinanzi alle suddette Autorità che riguardino il trattamento dei dati oggetto della convenzione.

Inoltre, tenuto conto della natura del trattamento dei dati e delle informazioni a disposizione del Responsabile del trattamento, **assiste** il Titolare del trattamento nel garantire il rispetto dei seguenti obblighi:

- di effettuazione della valutazione di impatto sulla protezione dei dati qualora un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, fornendo al Titolare tutte le informazioni e tutti gli elementi a ciò utili;
- di consultazione dell'Autorità Garante, prima di procedere al trattamento, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;

- di garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare del trattamento qualora il Responsabile del trattamento venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti o obsoleti;
- di cui all'articolo 32 del GDPR (Sicurezza del trattamento);

Le parti stabiliscono nell'Allegato 2 le misure tecniche e organizzative adeguate con cui il Responsabile del trattamento è tenuto ad assistere il Titolare del trattamento nell'applicazione della presente clausola, nonché l'ambito di applicazione e la portata dell'assistenza richiesta.

- **ulteriori *obblighi:***

Fermo restando che entrambe le parti devono essere in grado di dimostrare il rispetto delle presenti clausole, il Responsabile:

- **risponde** prontamente e adeguatamente alle richieste di informazioni del Titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole;
- **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 contratto di designazione;
- su richiesta del Titolare del trattamento**, consente e contribuisce** alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del Responsabile del trattamento. Il Titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole. Su richiesta, le parti mettono a disposizione della Autorità Garante le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione. Resta inteso che qualsiasi verifica condotta ai sensi delle presenti clausole dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un preavviso di almeno sette giorni;
- **si impegna** altresì a:
  - **effettuare** a richiesta del Titolare un rendiconto in ordine all'esecuzione delle istruzioni ricevute dal Titolare stesso (e agli adempimenti eseguiti) ed alle conseguenti risultanze;
  - **collaborare**, se richiesto dal Titolare, con gli altri Responsabili del trattamento, al fine di armonizzare e coordinare l'intero processo di trattamento dei dati personali;
  - **realizzare** quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa in materia di protezione dei dati personali, nei limiti dei compiti affidati con il presente contratto di designazione;

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

- ***ricorso a sub-Responsabili del trattamento:***

- nell'ambito dell'esecuzione del presente contratto, il Responsabile del trattamento **è autorizzato sin da ora** alla designazione di altri responsabili del trattamento (d'ora in poi anche "sub-Responsabili"), fornendo al Titolare le informazioni necessarie per consentirgli di esercitare il diritto di opposizione. Il Responsabile del trattamento informa specificamente per iscritto il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta o la sostituzione di sub-Responsabili del trattamento con un anticipo di almeno 30 giorni, dando così al Titolare del trattamento tempo sufficiente per potersi opporre a tali modifiche prima del ricorso al o ai sub-Responsabili del trattamento in questione (indicati nell'Allegato 1);
- qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento (per conto del Responsabile del trattamento), stipula un contratto che impone al sub-Responsabile del trattamento, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al Responsabile del trattamento conformemente alle presenti clausole. Il Responsabile del trattamento si assicura che il sub-Responsabile del trattamento rispetti gli obblighi cui il Responsabile del trattamento è soggetto a norma delle presenti clausole e del GDPR;
- Su richiesta del Titolare del trattamento, il Responsabile del trattamento gli fornisce copia del contratto stipulato con il sub-Responsabile del trattamento e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile del trattamento può espungere informazioni dal contratto prima di trasmetterne una copia;
- Il Responsabile del trattamento rimane pienamente responsabile nei confronti del Titolare del trattamento dell'adempimento degli obblighi del sub-Responsabile del trattamento derivanti dal contratto che questi ha stipulato con il Responsabile del trattamento. Il Responsabile del trattamento notifica al Titolare del trattamento qualunque inadempimento, da parte del sub-Responsabile del trattamento, degli obblighi contrattuali;
- il Responsabile del trattamento concorda con il sub-Responsabile del trattamento una clausola del terzo beneficiario secondo la quale, qualora il Responsabile del trattamento sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare del trattamento ha diritto di risolvere il contratto con il sub-Responsabile del trattamento e di imporre a quest'ultimo di cancellare o restituire i dati personali;

- ***trasferimenti internazionali***

- qualunque trasferimento di dati verso un paese terzo o un'organizzazione internazionale da parte del Responsabile del trattamento è effettuato soltanto su istruzione documentata del Titolare del trattamento o per adempiere a un requisito specifico a norma del diritto dell'Unione o degli Stati membri cui è soggetto il Responsabile del trattamento e nel rispetto del Capo V del GDPR;
- il Titolare del trattamento conviene che, qualora il Responsabile del trattamento ricorra a un sub-Responsabile del trattamento conformemente alle clausole di cui al precedente paragrafo "*Ricorso a sub-Responsabili del trattamento"* per l'esecuzione di specifiche attività di trattamento (per conto del

Titolare del trattamento) e tali attività di trattamento comportino il trasferimento di dati personali ai sensi del Capo V del GDPR, il Responsabile del trattamento e il sub-Responsabile del trattamento possono garantire il rispetto del Capo V del Regolamento (UE) 2016/679 utilizzando le clausole contrattuali tipo adottate dalla Commissione conformemente all'articolo 46, par. 2, del GDPR, purché le condizioni per l'uso di tali clausole contrattuali tipo siano soddisfatte;

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

Il Responsabile del trattamento comunica al Titolare del trattamento i dati di contatto del proprio Responsabile della protezione dei dati (DPO), ove designato. Il nome del DPO del Responsabile del trattamento dei dati sarà comunicato al Titolare solo per uso tra le parti.

DURATA DEL TRATTAMENTO

Il presente contratto di designazione acquista efficacia dalla data di sottoscrizione ed è condizionato, per oggetto e per durata, al rapporto contrattuale/convenzionale in corso tra l'Azienda Ospedaliero-Universitaria di Modena e il Responsabile del trattamento e si intenderà revocato di diritto alla scadenza del rapporto o alla risoluzione, per qualsiasi causa, dello stesso; alla cessazione definitiva lo stesso decadrà con effetto immediato. Il trattamento, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato.

Salva diversa determinazione, in assenza di interventi di modifica della normativa, la presente designazione si intende estesa ad eventuali future proroghe e/o rinnovi di contratti, aventi ad oggetto le medesime o ulteriori attività che comportino un trattamento di dati personali analoghi da parte del Responsabile del trattamento in nome e per conto del Titolare.

RESTITUZIONE E CANCELLAZIONE DEI DATI

Al termine del periodo di conservazione o all'atto della conclusione o della revoca del contratto, su richiesta, o in qualsiasi altro momento per sopravvenute necessità, il Responsabile dovrà interrompere ogni operazione di trattamento dei dati personali e dovrà provvedere, a scelta del Titolare, alla cancellazione di tutti i dati personali trattati per conto del Titolare del trattamento, oppure alla restituzione al Titolare del trattamento di tutti i dati personali, cancellando le copie esistenti, a meno che il diritto dell'Unione o dello Stato membro non richieda la conservazione dei dati personali. In entrambi i casi il Responsabile rilascia attestazione scritta che presso di lui non ne esista alcuna copia. Finché i dati non sono cancellati o restituiti, il Responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

La restituzione ricomprende tutte le eventuali copie di backup e tutta la documentazione cartacea. Su richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

Resta fermo che, anche successivamente alla cessazione o alla revoca del contratto/convenzione, 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.

INOSSERVANZA DELLE CLAUSOLE E RISOLUZIONE

- Fatte salve le disposizioni del GDPR, qualora il Responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il Titolare del trattamento può dare istruzione al Responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il contratto. Il Responsabile del trattamento informa prontamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.
- Il Titolare del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:
  1) il trattamento dei dati personali da parte del Responsabile del trattamento sia stato sospeso dal Titolare del trattamento in caso di violazione degli obblighi derivanti dalle presenti clausole e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;
  2) il Responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del GDPR;
  3) il Responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o dell'Autorità Garante per la protezione dei dati personali per quanto riguarda i suoi obblighi in conformità alle presenti clausole o al GDPR;
- Il Responsabile del trattamento ha diritto di risolvere il contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il Titolare del trattamento che le sue istruzioni violano il GDPR o le disposizioni applicabili, nazionali o dell'Unione, relative alla protezione dei dati, il Titolare del trattamento insista sul rispetto delle istruzioni.

CONDIZIONI DELLA NOMINA

Chiunque subisca un danno materiale o immateriale causato da una violazione della normativa in materia di protezione dei dati personali ha il diritto di ottenere il risarcimento del danno dal Titolare o dal Responsabile. In particolare il Responsabile risponde per tale danno (anche per eventuali suoi Sub-responsabili) se non ha adempiuto agli obblighi che la normativa pone direttamente in capo ai responsabili o ha agito in modo difforme o contrario rispetto alle istruzioni impartite dal Titolare nel presente Atto o ad ulteriori istruzioni eventualmente trasmesse per iscritto dal Titolare.

In caso di richieste di risarcimento pervenute al Titolare, per violazioni compiute dal Responsabile, il Titolare si riserva il diritto di rivalsa nei confronti del Responsabile stesso.

Per quanto riguarda le sanzioni imputabili da parte dell'Autorità Garante, fanno fede gli art. 82, 83 e 84 del Regolamento.

Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.

Resta inteso inoltre che la presente designazione non comporta alcun diritto per il Responsabile a uno specifico compenso, indennità o rimborso per l'attività svolta in qualità di Responsabile, ulteriore rispetto a quanto già previsto nel contratto/convenzione stipulato con il Titolare, indicati al presente Atto.

ALLEGATI

Gli Allegati:

- 1. Descrizione e ambito del trattamento (art. 28, paragrafo 3, GDPR)
- 2. Misure di sicurezza tecniche e organizzative

costituiscono parte integrante del presente Atto di designazione

Per quanto non espressamente previsto nel presente contratto di designazione, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali, nonché alle disposizioni di cui al rapporto contrattuale stipulato tra le parti, indicato nelle premesse.

ALLEGATO 1 Descrizione e ambito del trattamento (art. 28, paragrafo 3, GDPR)

Finalità per le quali i dati personali sono trattati per conto del Titolare del trattamento
(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

- Erogazione di prestazioni sanitarie
- Finalità amministrative connesse alla cura dei pazienti (es.: accettazione, prenotazione, pagamento ticket..)
- Fornitura di beni e/o servizi
- Marketing
- Profilazione
- Erogazione di servizi di manutenzione IT
- Altro (specificare) _____
- Altro (specificare) _____
- Altro (specificare)_____

Categorie degli interessati

(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

- Pazienti
- Dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori
- Clienti
- Consulenti
- Fornitori
- Altro (specificare) _____
- Altro (specificare)_____

Categorie di Dati personali da trattare

(Il presente elenco è da considerarsi a titolo puramente esemplificativo e non esaustivo)

- dati anagrafici di pazienti
- dati anagrafici di dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori
- dati anagrafici dii familiari, se presenti detrazioni di figli/coniuge a carico e assegni nucleo familiare
- dati relativi allo stato di salute dei pazienti
- dati relativi allo stato di salute di dipendenti, specialisti convenzionati, universitari integrati, personale in formazione e altri collaboratori (disabilità, certificati medici, certificati di gravidanza)
- dati genetici
- dati biometrici
- permessi di soggiorno
- dati retributivi
- dati anagrafici dei fornitori
- abitudini di consumo
- Altri dati (specificare)
  _____

Natura del trattamento

_____

Durata del trattamento

_____

Per il trattamento da parte di **sub-Responsabili del trattamento**, specificare***:

1) estremi identificativi del/i Sub-responsabile/i (ragione sociale): _____
   _____
   materia disciplinata:_____
   natura del trattamento: _____
   durata del trattamento: _____

2) estremi identificativi del/i sub-Responsabile/i (ragione sociale): _____

_____
materia disciplinata:_____
natura del trattamento: _____
durata del trattamento: _____

3) estremi identificativi del/i sub-Responsabile/i (ragione sociale): _____
_____
materia disciplinata: _____
natura del trattamento: _____
durata del trattamento: _____

*** Il Responsabile del trattamento ha la facoltà di allegare al presente Atto di designazione un apposito elenco o link di collegamento contenente le informazioni richieste; ciò vale anche con riferimento alle misure tecniche e organizzative specifiche dettate al sub-Responsabile del trattamento.

ALLEGATO 2 Misure di sicurezza tecniche e organizzative

Il presente allegato descrive le misure tecniche e organizzative (comprese le eventuali certificazioni pertinenti) che il Responsabile deve adottare in modo concreto e non genericamente per garantire un adeguato livello di sicurezza, tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche.
Le misure descritte nel presente documento sono da intendersi integrative rispetto a quanto previsto dalle normative vigenti in merito al trattamento dei dati personali, che rimangono pertanto il riferimento normativo principale a cui attenersi.

Definizioni/acronimi:
- AOU: Azienda Ospedaliero-Universitaria di Modena/Titolare del trattamento
- RT: Responsabile del Trattamento
- STI: Servizio Tecnologie dell'informazione
- SUIC: Servizio Unico Ingegneria Clinica

2.A Misure di sicurezza tecniche per Responsabili del trattamento che facciano accesso ai sistemi informativi e ai dispositivi della Azienda Ospedaliero-Universitaria di Modena

INTRODUZIONE
Questa sezione descrive le misure tecniche e organizzative specifiche che l'Azienda Ospedaliero-Universitaria di Modena (AOU) richiede a soggetti che, a seguito di contratto di designazione a Responsabile del Trattamento (RT), siano abilitati all'accesso ai sistemi informativi della AOU stessa.

- ***Principi Generali***

Il RT si impegna a trattare i dati mantenendo una condotta orientata al rispetto dei principi generali sanciti dall'art. 5 del GDPR, in particolare di liceità, integrità, riservatezza, minimizzazione del trattamento, adottando ovunque possibile metodologie e soluzioni tecniche che privilegino il trattamento di dati con formati non riconducibili all'interessato (es. anonimizzati, pseudonimizzati, ecc.).
Il RT deve definire formalmente un regolamento sull'utilizzo degli strumenti IT oggetto del trattamento di dati di AOU. Tale regolamento deve essere conforme alla normativa vigente e garantire le misure minime organizzative atte a tutelare il dato di AOU. Tale regolamento deve essere, su richiesta, fornito ad AOU.

- ***Operatori del RT***

Il RT si impegna a informare delle presenti misure e delle normative applicabili tutti gli operatori che siano coinvolti nel trattamento dati (con qualsiasi tipo di rapporto).
Il RT si impegna a censire tutti gli operatori coinvolti nel trattamento e, su richiesta, a fornire l'elenco con descrizione dei ruoli al Titolare.
Qualora il RT, nell'ambito del trattamento, si avvalesse di credenziali con privilegi di amministrazione di sistema, è tenuto alla tenuta di un registro di tali operatori. Il RT si impegna a fornire l'elenco con descrizione dei ruoli ad AOU.

2.A.1 SERVIZI DI ASSISTENZA, MANUTENZIONE, SUPPORTO, COLLABORAZIONE, EROGAZIONE DI SERVIZI PER CONTO, CHE PREVEDANO ACCESSO AI SISTEMI DI AOU

Quanto descritto nella presente sezione si applica a RT che, in funzione della designazione da parte della AOU effettui trattamenti di dati personali mediante l'accesso ai sistemi informativi, per l'erogazione di servizi di assistenza, manutenzione, supporto, collaborazione e erogazione di qualsiasi di tipo per conto del Titolare del trattamento.

1. L'accesso ai sistemi AOU deve avvenire esclusivamente con modalità sicure, concordate con AOU. E' fatto divieto di adottare sistemi di collegamento e comunicazione non concordati con AOU.
2. L'accesso ai sistemi AOU deve avvenire a seguito di emissione di credenziali AOU, che sono personali e non condivisibili; la persona fisica associata alle credenziali sarà ritenuta responsabile, insieme al RT, di ogni azione svolta con tali credenziali e ritenuta responsabile di eventuali usi impropri (es. condivisione delle credenziali con colleghi).
   - Eccezioni all'abbinamento nominale delle credenziali aziendali possono essere valutate dal Servizio STI o SUIC solo in contesti tecnici che richiedessero tali modalità quale condizione non derogabile per

l'erogazione del servizio. Tale eccezione sarà regolata con apposito emendamento al contratto di nomina a RT.

- A seguito di cessazione del rapporto di operatori con il RT, questo è tenuto a comunicarlo al Servizio STI o SUIC entro 24h allo scopo di procedere all'immediata disabilitazione delle credenziali.

3. Qualsiasi accesso a dati deve essere motivato da esplicita richiesta da parte di AOU o da procedura operativa concordata tra RT e AOU. È obbligo del RT mantenere documentazione delle motivazioni degli accessi, che AOU si riserva di richiedere in fase di istruttoria relativa a specifici accessi.
4. In nessun caso è consentito il trasferimento di dati in copia unica dalla AOU verso sistemi informativi del RT (es. esportazione di dati storici verso i sistemi del RT con cancellazione dai sistemi di AOU). Anche quando si rendesse necessario trasferire copia di dati verso i sistemi del RT, una copia deve rimanere archiviata sui sistemi di titolarità della AOU o presso l'infrastruttura AOU con modalità concordate con AOU.
5. Eventuali copie di dati verso i sistemi del RT dovranno essere autorizzate (singolarmente o tramite definizione di procedure operative) da AOU e non potranno comunque eccedere l'insieme di dati oggetto del rapporto tra il RT e AOU.
6. Eventuali copie di dati verso i sistemi del RT dovranno essere archiviate e gestite secondo modalità conformi con la normativa vigente e su sistemi che rispettino le Misure Minime di Sicurezza ICT/SUIC definite da AGID come obbligatorie per le pubbliche amministrazioni. La durata dell'archiviazione deve essere limitata al soddisfacimento delle sole esigenze espresse da AOU.
7. Qualsiasi alterazione volontaria di dati (personali o non) da parte del RT sui sistemi di AOU dovrà essere preventivamente ed esplicitamente autorizzata da AOU.
8. Il RT deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità AOU da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da AOU.
9. E' obbligo del RT notificare alla AOU/Titolare del trattamento entro 24h qualsiasi evento che abbia comportato perdita, alterazione, diffusione o trasmissione non intenzionale verso terzi di dati di AOU. Questo include anche eventi non direttamente imputabili al RT, ma di cui il RT venga a conoscenza.

2.A.2. SERVIZI IN OUTSOURCING TOTALE

Quanto descritto nella presente sezione di applica a RT che, in funzione della designazione da parte della AOU, effettui trattamenti di dati personali nel corso della fornitura di servizi verso AOU, la cui infrastruttura tecnica sia totalmente in gestione al RT (es. soluzioni Cloud quali SAAS, IAAS, PAAS o gestione di sottoreti o sistemi informatici presso i locali di AOU ma a totale carico del RT).

1. Il RT è tenuto a fornire alla AOU una completa descrizione infrastrutturale e architetturale delle modalità di trattamento del dato (informatizzato), che riporti in particolare:
   - Collocazione geografica dei data center;
   - Modalità di gestione delle credenziali;
   - Modalità di gestione degli accessi;
   - Modalità di gestione dell'integrità (es. tecnologie di backup);
   - Modalità di gestione della confidenzialità (es. architettura di security di rete);
   - Modalità di gestione della continuità (es. tecnologie di business continuity).

   La AOU si riserva di chiedere approfondimenti tecnici e di rispondenza alle normative della documentazione fornita.
2. Le modalità di trattamento informatico del dato, oltre ad essere conformi alla normativa vigente, devono rispettare le Misure Minime di Sicurezza ICT definite da AGID come obbligatorie per le pubbliche amministrazioni.
3. La AOU si riserva, a titolo di monitoraggio ed ispettivo, di eseguire verifiche remote o sul posto delle modalità di trattamento. Il RT dovrà rendere possibili tali verifiche.
4. Il RT deve fornire una modalità di accesso massivo ai dati di titolarità AOU da parte di un insieme di utenti indicato da AOU. Tale accesso deve consentire in qualsiasi momento una verifica della integrità dei dati, ed essere reso disponibile alla conclusione del rapporto tra RT e AOU per il recupero dei dati e il loro trasferimento su sistemi di gestione AOU o di altri RT. Tali dati devono essere disponibili in formato leggibile, con strutturazione e codifica documentate e coerenti con le modalità di fruizione e archiviazione applicative (es. non è considerato accesso massivo accettabile il riversamento in formati solo testuali destrutturati, PDF, immagini o comunque non riconducibile a dati strutturati e codificati)
5. Il RT deve garantire l'accesso ai log di sistema (operazioni di accesso e modifica) relativi ai trattamenti dei dati di AOU. Tale accesso deve essere reso disponibile in tempo reale ad un insieme concordato di utenti AOU, o comunque reso disponibile entro 24h dalla richiesta.

6. Il RT deve garantire ad AOU di potere, qualora fossero necessarie operazioni massive sui dati (es. rettifica di dati per prevenire o riparare a malfunzionamenti o errati inserimenti di dati), di poter accedere in modifica con modalità massive ai dati ospitati sui sistemi del RT.
7. Qualsiasi alterazione volontaria di dati (personali o non) da parte del RT sui dati di AOU dovrà essere preventivamente ed esplicitamente autorizzata dalla AOU.
8. Il RT deve garantire ad AOU di poter oscurare volontariamente e in modo tracciato i dati (pur mantenendo l'oscuramento dell'operazione di oscuramento).
9. Il RT deve garantire, a conclusione del rapporto, la completa rimozione dei dati di titolarità AOU da ogni supporto o collocazione. Questa dovrà avvenire dopo avere eseguito e documentato con verbale di collaudo il trasferimento dei dati verso destinazione indicata da AOU.
10. E' obbligo del RT notificare alla AOU/Titolare del trattamento entro 24h qualsiasi evento che abbia comportato perdita, alterazione, diffusione o trasmissione non intenzionale verso terzi di dati di AOU. Questo include anche eventi non direttamente imputabili al RT, ma di cui il RT venga a conoscenza.

2.B Misure di sicurezza organizzative per i Responsabili del trattamento

INTRODUZIONE

Questa sezione descrive le misure organizzative specifiche che l'Azienda Ospedaliero-Universitaria di Modena (AOU) richiede a RT che, a seguito di contratto di designazione a Responsabile del Trattamento (RT), effettuino trattamenti di dati personali mediante erogazione di servizi di assistenza, manutenzione, supporto, collaborazione di qualsiasi di tipo per conto del Titolare, senza accedere ai sistemi informativi della AOU stessa. Tali misure si applicano, ove ricorrano le condizioni, anche a RT indicati nelle sezioni 2A del presente Allegato.

- ***Principi Generali***

Il RT si impegna a trattare i dati mantenendo una condotta orientata al rispetto dei principi generali sanciti dall'art. 5 del GDPR, in particolare di liceità, integrità, riservatezza, minimizzazione del trattamento, adottando ovunque possibile soluzioni organizzative che garantiscano:

1. La adozione di una policy in materia di protezione dei dati personali, per la corretta gestione e conservazione in ambienti protetti, durante tutto il ciclo di trattamento.
2. La diffusione di tale policy mediante formazione di tutti gli operatori che siano coinvolti nel trattamento dati (con qualsiasi tipo di rapporto), impartendo istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.
3. La protezione dei dati in caso di loro trasmissione (sia telematica che con modalità cartacea).
4. La sicurezza fisica dei luoghi in cui i dati personali sono trattati (uffici, archivi…).
5. La conservazione limitata dei dati, in applicazione delle regole contenute nel massimario di scarto aziendale.
6. In caso di trattamento dei dati personali e di natura particolare di pazienti/assistiti, il rispetto delle prescrizioni di natura organizzativa dettate dall'Autorità Garante per la protezione dei dati personali con Provvedimento denominato "Strutture sanitarie: rispetto della dignità - 9 novembre 2005".
7. La notifica alla AOU/Titolare del trattamento entro 24h di qualsiasi evento che abbia comportato perdita, alterazione, diffusione o trasmissione non intenzionale verso terzi di dati di AOU, pur se l'evento non sia avvenuto mediante l'utilizzo di sistemi informatici/telematici. Questo include anche eventi non direttamente imputabili al RT, ma di cui il RT venga a conoscenza.