REDATTO	
Luigi Rufo, Bruno Manno	
VERIFICATO	
Direttore Sanitario	Francesca Bellini
Direttore Amministrativo	Tito Berti
Qualità e accreditamento	Stefania Gianassi
APPROVATO	**Nome**
Direttore Generale	Alberto Zanobini

REGISTRO DELLE ATTIVITÀ

DI TRATTAMENTO DATI

INTRODUZIONE

1. Oggetto del documento

L'oggetto del presente documento consiste nella redazione di indicazioni operative che consentono di aver un quadro di insieme per consentire la corretta gestione e conservazione del registro delle attività di trattamento così come richiesto dal GDPR.

I contenuti del registro, come si vedrà meglio in seguito, sono contenuti all'art. 30 del GDPR.

2. Ambito di applicazione del documento

Le presenti indicazioni sono destinate alla corretta gestione del registro delle attività di trattamento dell'Azienda Ospedaliero Universitaria Meyer (da ora in avanti anche Azienda Meyer).

L'onere della tenuta del Registro è a carico del titolare o suo Referente e, se nominato, del responsabile del trattamento.
La tenuta del registro è utile per una completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio di tali trattamenti e a una corretta pianificazione degli stessi.

Il registro sarà tenuto in forma scritta, ma anche in formato elettronico, e sarà esibito all'autorità di controllo in caso di verifiche.

Si precisa che tutte le informazioni raccolte nel presente documento, ed i suoi allegati, sono volte a inquadrare lo stato dell'arte dei trattamenti svolti presso l'azienda Meyer e per prevenire violazioni della normativa sulla privacy ed a ridurre al minimo i rischi di accesso non autorizzato, di trattamento non conforme alle finalità istituzionali, di distruzione o perdita dei dati.

3. Revisione del Documento/monitoraggio efficacia misure adottate

E' previsto una verifica semestrale del presente documento, nonché un aggiornamento specifico ogniqualvolta si verifichino significative variazioni delle situazioni relative ai trattamenti di dati e ai sistemi informatici utilizzati, parimenti una volta all'anno o ogniqualvolta si verifichino tali significative variazioni, il Titolare, coadiuvato dal Coordinatore e dai Responsabili effettuerà un monitoraggio sull'efficacia delle misure tecniche e organizzative qui previste al fine di garantire la sicurezza dei trattamenti.

DEFINIZIONI

Anonimizzazione: tecnica di trattamento dei dati personali tramite la quale i dati personali non possano più essere attribuiti a un interessato specifico, nemmeno attraverso l'utilizzo di informazioni aggiuntive.
Archivio: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
Autorità di controllo: è l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

Cifratura: tecnica di trattamento dei dati personali tramite la quale i dati personali vengono resi non intellegibili a soggetti non autorizzati ad accedervi.
Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
Contitolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, insieme ad altri determina le finalità e i mezzi di trattamento dei dati personali;
Data Breach: è un incidente di sicurezza in cui i dati personali vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato o persi accidentalmente.
Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di Identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
DPIA: acronimo di Data Protection Impact Assessment (valutazione di impatto sulla protezione dei dati).
Interessato: persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
Misure di sicurezza: misure tecniche ed organizzative adeguate per garantire un livello di sicurezza dei dati trattati adeguato al rischio.
Nuovo trattamento: trattamento di dati personali che comporta l'utilizzo di nuove tecnologie o è di nuovo tipo e in relazione al quale il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.
Privacy by-design / by-default: l'incorporazione della privacy a partire dalla progettazione di un processo aziendale, con le relative applicazioni informatiche di supporto. La prima introduce la protezione dei dati fin dalla progettazione per caso specifico, la seconda per impostazione predefinita di una pluralità di casi tra loro omogenei.
Pseudonimizzazione: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
Rappresentante: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del regolamento;

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
Responsabile della Conservazione documentale: si tratta della figura preposta alla gestione e supervisione del processo di conservazione dei documenti (digitali o cartacei).
Sub responsabile: persona fisica o giuridica designata dal responsabile del trattamento previa autorizzazione scritta del titolare del trattamento;
Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare o suo delegato del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
Titolare del trattamento o suo delegato: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
Trattamento : qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
Violazione dei dati personali: la violazione di sicurezza che comporta 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.

INFORMAZIONI SCHEDA REGISTRO

La seguente sezione intende fornire una guida per definire le informazioni presenti nel registro trattamenti che sarà adottato dall'Azienda Meyer.

1. Informazioni generali

Dati generali del trattamento: insieme di informazioni che identificano il trattamento (Area specialistica, attività funzionale del trattamento, descrizione);
Soggetti: persone fisiche o giuridiche idonee ad individuare i soggetti attivi del trattamento ed i loro dati di riferimento/identificativi (Titolare/riferimento titolare, contitolare/riferimento contitolare), nonché i dati identificativi (nome proponente) della struttura quale punto di riferimento delegato dal titolare (ufficio/settore cui afferisce);
Responsabile esterno del trattamento: dati identificativi del soggetto nominato responsabile esterno ex art. 28 GDRP.

2. Dettaglio trattamento

Finalità: individuazione delle finalità di rilevante interesse pubblico perseguite relativamente all'attività istituzionale a cui è collegato il trattamento;
Categoria di soggetti associabili: macro categoria di soggetti interessati i cui dati rientrano in un'attività di trattamento del soggetto titolare/responsabile;
Modalità di trattamento: indicazione dell'ambito nel quale il trattamento viene posto in essere nonché indicazione del carattere automatizzato o meno del trattamento**;**
Natura dei dati personali: indicazione della tipologia di dati oggetto di trattamento;

Operazioni sui dati di cui si compone il trattamento: indicazione delle operazioni svolte sui dati; le operazioni possono essere di carattere standard oppure particolari;
Regolamento dei dati sensibili e giudiziari: annotare e citare eventuali codici di condotta o codici deontologici;
Consenso e trattamento di dati: indicazioni relative al consenso prestato al trattamento dei dati, all'informativa, al trasferimento ed all'eventuale comunicazione a terzi;
Strumenti utilizzati: banche dati, tecnologie cloud, strumenti IoT, ecc;
Dati relativi al rischio: indicazioni di sottomissione dell'eventuale trattamento alla Valutazione d'impatto.

TRATTAMENTO DEI DATI E CARATTERISTICHE

- ✓ *Premessa*

I dati che verranno censiti all'interno del registro vengono raccolti per finalità determinate, esplicite e legittime, ed il trattamento avviene nel rispetto delle disposizioni di legge e dei diritti e delle libertà fondamentali dell'interessato, secondo i principi di liceità, correttezza, trasparenza, minimizzazione (adeguatezza, pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi); i dati trattati sono essenziali per lo svolgimento delle attività istituzionali.

L'Azienda Meyer tratta dati personali relativi a:
- utenti, assistiti, pazienti e loro familiari e/o accompagnatori;
- personale sanitario, amministrativo, tecnico e professionale della dirigenza e del comparto con rapporto di dipendenza, convenzione o collaborazione;
- personale universitario che svolge attività assistenziale, di ricerca e di didattica all'interno dell'Azienda;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture dell'Azienda ed effettuano trattamento di dati personali, quali specializzandi, allievi tirocinanti, volontari, ecc;
- soggetti che intrattengono rapporti contrattuali con l'Azienda ai fini della fornitura di beni e servizi, attività di assistenza o consulenza, esecuzione di opere edilizie, interventi di manutenzione su software o dispositivi medici, ecc;
- soggetti e imprese partecipanti a bandi di gara o di pubblico concorso.

L'Azienda effettua il trattamento dei soli dati necessari per le finalità per le quali vengono raccolti o trattati tra cui:
- dati personali comuni quali: nome, cognome, residenza, cittadinanza, recapito telefonico, codice fiscale, ecc;
- categorie particolari di dati personali (art. 9 del GDPR);
- dati economici quali: retribuzione, compensi, benefici, agevolazioni, ecc;
- dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).
- dati relativi ai familiari, quando richiesti da un presupposto di legge o di regolamento.

I dati personali trattati dall'Azienda nelle forme e nei limiti di quanto previsto dalla vigente normativa sono raccolti:

- prioritariamente presso l'interessato o anche presso persone diverse nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
- presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

L'Azienda Meyer tratta i dati personali relativi alla salute ai sensi dell'art.9 paragrafo 2 lettere h) ed i) del GDPR e dunque, senza necessità di raccogliere il consenso (sempre che non siano trattati dati genetici e/o biometrici), per le seguenti finalità:

- tutela della salute e dell'incolumità fisica (ossia attività di prevenzione, diagnosi, cura, assistenza, terapia sanitaria o sociale, riabilitazione), anche nell'ambito di percorsi di cura integrati che coinvolgano altri soggetti/ strutture sanitarie pubbliche o private;
- medicina preventiva;
- tutela dell'incolumità fisica e della salute di terzi e della collettività;
- medicina del lavoro e valutazione della capacità lavorativa dei dipendenti;
- motivi di interesse pubblico nel settore della sanità pubblica.

Il trattamento disciplinato dal presente articolo è indispensabile per l'erogazione e la gestione delle prestazioni sanitarie richieste ed è effettuato, nel pieno rispetto del segreto professionale, del segreto d'ufficio e secondo i principi della normativa privacy, da personale dipendente o da altri soggetti che collaborano con l'Azienda Meyer (ad es. medici in formazione specialistica, tirocinanti...) tutti debitamente designati ed a ciò autorizzati.

I dati relativi allo stato di salute non sono oggetto di diffusione ma possono essere comunicati, nei casi previsti da norme di legge o di regolamento, a soggetti pubblici e privati, enti ed istituzioni, per il raggiungimento delle rispettive finalità.
L'Azienda Meyer tratta, altresì, i dati personali per fini amministrativi nel rispetto di quanto previsto dall'articolo 6, par.2, lettera e) del Regolamento UE, ovvero solo se necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita, e per le finalità di cui dell'articolo 9, par.2, lettera g) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

- ✓ *Trattamenti con l'ausilio di strumenti elettronici*

Le attività condotte nell'Azienda Meyer prevedono l'utilizzo di strumenti elettronici quali elaboratori o personal computer, anche portatili, connessi alla rete aziendale.
Grazie alla suddetta interconnessione da ogni postazione di lavoro sono usufruibili (in base ad una opportuna profilazione degli utenti interni) le informazioni presenti sulle banche dati attraverso i software gestionali dedicati alle varie attività.
I server aziendali in cui sono memorizzate le principali basi dati, sono collocati in una sala server principale.

Il sistema informatico è presidiato a livello centralizzato da un Referente informatico (c.d. Amministratore di Sistema) che – anche avvalendosi dei dipendenti facenti capo al Servizio Sistemi Informativi aziendale – ha il compito di sovrintendere alle risorse del sistema informatico in termini di hardware, sistemi operativi, sistemi per la gestione di basi di dati, applicazioni informatiche (cioè software di base e applicativo) e reti e di consentirne l'utilizzazione, come pure di a garantire, in relazione alle conoscenze informatiche acquisite in base al progresso tecnologico, lo sviluppo delle misure di sicurezza necessarie al fine di: a) ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati memorizzati su supporti magnetici e ottici gestiti, nonché delle banche dati e dei locali ove esse sono collocate; b) evitare l'accesso non autorizzato alle banche dati, alla rete e, in generale, ai servizi informatici dell'Azienda; c) prevenire trattamenti di dati non conformi alla legge od ai regolamenti; d) evitare la cessione o la distribuzione dei dati in caso di cessazione del trattamento.

a. Autenticazione informatica

Tutti i trattamenti di dati personali in formato elettronico di cui l'Azienda Meyer è titolare sono accessibili soltanto attraverso una procedura di autenticazione.
Per poter accedere al trattamento dei dati i soggetti autorizzati devono essere in possesso di credenziali individuali di autenticazione rilasciate a seguito di apposita richiesta scritta del Referente privacy.
Come credenziali individuali l'Azienda Meyer si serve di password e codice dell'utente. In futuro potrà essere utilizzato qualunque altro strumento (ad esempio: badge, smartcard, ecc.) ritenuto idoneo all'identificazione nel rispetto della normativa sulla privacy.
Le credenziali di identificazione sono individuali e non possono essere rilasciate a più incaricati anche in tempi diversi. Ad ogni soggetto autorizzato possono essere assegnate più credenziali per accessi differenziati a diverse banche di dati o a software gestionali (vedi sistema informativo Accesso, protocollo informatico, posta elettronica, ecc.)
All'atto del rilascio il personale è istruito sulle cautele e precauzioni da adottare per mantenere la sicurezza e affidabilità delle credenziali.
Le credenziali non utilizzate da almeno tre mesi devono essere disattivate; sono, altresì, tempestivamente disattivate al venire meno delle condizioni per cui erano state rilasciate e comunque al verificarsi di qualunque evento che ne possa compromettere la segretezza e l'efficacia.
La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
Gli incaricati sono tenuti a conservare e custodire con cura le credenziali e i dispositivi di autenticazione; è vietato comunicare le proprie credenziali a terzi.

Altresì, secondo quanto stabilito dall'art. 32 del GDPR si è provveduto:

- a installare e mantenere aggiornati dispositivi antiintrusione per proteggere le reti informatiche da intrusioni dall'esterno con particolare attenzione alle reti collegate ad internet.
- A garantire che su tutti gli elaboratori siano presenti adeguati programmi di protezione da virus informatici e da tentativi di intrusione.
- Ad assicurarsi che su tutti i sistemi operativi installati negli elaboratori vengano installati gli aggiornamenti relativi alla sicurezza.
- Ad assicurarsi che tutte le disposizioni relative alle copie di sicurezza vengano osservate.

b. Analisi dei rischi che incombono sui dati

I Referenti privacy, con la collaborazione dei soggetti autorizzati o dei Responsabile del trattamento, devono verificare almeno annualmente il livello di sicurezza in cui vengono svolti i trattamenti.
La verifica dovrà, inoltre, riguardare l'affidabilità delle attrezzature elettroniche utilizzate, dei sistemi operativi installati e dei programmi utilizzati.
Anche a tal fine l'Azienda – in un'ottica informativa e formativa - può mettere a disposizione degli utenti interni, indicazioni, documenti, procedure operative di carattere generale e/o riguardo a specifici argomenti in materia.

A titolo esemplificativo, nella tabella che segue verranno indicate per alcuni rischi potenzialmente verificabili e alcune misure di mitigazione attuate dall'Azienda Meyer.

Rischio	Misura	Possibili Ulteriori misure adottabili
Danneggiamento, distruzione o perdita del dato	✓ effettuazione di copie di sicurezza, salvataggio settimanale dei dati, backup centralizzato periodico, aggiornamento annuale dei programmi di protezione per elaboratore (semestrale per trattamento di dati sensibili o giudiziari); ✓ effettuazione di backup full dei database dei gestionali giornalieri conservando gli ultimi 7; ✓ effettuazione periodica di restore (dei dati di backup) del database del gestionale principale; ✓ dotazione di impianti antincendio; ✓ adozione di sistemi di ridondanza sui server; ✓ presenza di almeno due alimentatori su ogni server; ✓ utilizzo di dischi con RAID; ✓ utilizzo di infrastrutture servite da alimentazione privilegiata (gruppo elettrogeno) ed UPS per i sistemi di produzione.	✓ sistematizzare l'emanazione di indicazioni atte a responsabilizzare gli utenti interni sui rischi connessi all'utilizzo degli strumenti elettronici (ad esempio, rischi derivanti dalla tenuta ed archiviazione di dati sui rispettivi hard disk) e sui comportamenti, accorgimenti e misure da adottare per limitare/abolire danni correlati.
Accesso non autorizzato (ai locali, al sistema ed ai dati)	✓ server aziendali sono collocati in locali chiusi a chiave (porte blindate o tradizionali), di norma senza finestre e in taluni casi dotati di telecamera IP con	✓ sistema di tracciabilità degli eventuali accessi di personale non-CED; ✓ utilizzo di codici identificativi

	registrazione remota; ✓ i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persone diverse dalle autorizzate; ✓ assegnazione di credenziali di accesso alla rete differenziate per servizio/gestionale e di password personalizzate; ✓ adozione di sistema di gestione degli utenti che associa il data base degli stessi con le rispettive autorizzazioni, disponibile centralmente in rete al fine di un eventuale recupero su richiesta dei soggetti autorizzati al trattamento dei dati; ✓ utilizzo di salvaschermo protetti da password in caso di inattività tutti i PC fissi e mobili e gli elaboratori sono coperti da sistemi di rilevamento e di prevenzione delle intrusioni e anti-hackers, firewall di sistema, antivirus, antispyware la cui efficacia è periodicamente verificata ed aggiornata.	personali che non consentano l'accesso contemporaneo alla stessa applicazione da diverse stazioni di lavoro; ✓ definizione di istruzioni per l'uso, la custodia e la distruzione dei supporti rimovibili o del contenuto degli stessi, al fine di evitare accessi non autorizzati e trattamenti impropri; ✓ apposizione di clausole di sicurezza ai contratti di manutenzione software – ove non già esistenti - switch di rete per permettere un maggior controllo sugli accessi non autorizzati alla LAN.
Trattamento non autorizzato	✓ ogni incaricato del trattamento è munito di credenziali di autenticazione e/o parola chiave; è operativa la procedura che ne consente l'autonoma sostituzione periodica da parte del singolo operatore; ✓ di norma il codice identificativo personale fornito ad ogni operatore non viene assegnato a persone diverse; ✓ i supporti rimovibili e le copie di sicurezza vengono custoditi in luogo non accessibile a persona diversa dall'incaricato del trattamento; ✓ i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle	✓ disattivazione dei codici personali nel caso in cui vi sia perdita della qualità che permette l'accesso all'operatore o di mancato utilizzo superiore ai sei mesi

	proprie mansioni lavorative.	
Trattamento non conforme alla finalità della raccolta o illecito	✓ è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi; ✓ a tal fine, dati non più occorrenti vengono di norma cancellati o distrutti (anche facendone richiesta all'Amministratore di Sistema, ove il soggetto responsabile non fosse in possesso delle necessarie abilitazioni); qualora fossero conservati, non sono comunque utilizzabili.	✓ adozione di tecniche di cifratura o codici identificativi o di altre soluzioni che rendano temporaneamente inintelligibili i dati anche a chi è autorizzato ad accedervi, e permettano di identificare gli interessati solo in caso di necessità; ✓ trasferimento cifrato dei dati sensibili e giudiziari in formato elettronico ✓ conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale rispetto ad altri dati personali oggetto di trattamento.

c. Trattamenti affidati all'esterno

L'Azienda Meyer affida all'esterno anche il trattamento di alcuni dati.

I Gestori dei servizi affidati all'esterno sono informati della presenza di dati anche di natura sensibili negli archivi e non sono autorizzati ad accedere ai dati per altro titolo che non sia quello indicato nella lettera di affidamento dell'incarico o del servizio. L'accesso agli archivi da parte di alcuni gestori è consentito soltanto per operazioni di basso livello e per interventi tecnici (backup, aggiornamenti database, manutenzioni, ecc.); per il gestore che si occupa della configurazione dei server l'accesso è consentito anche da remoto per operazioni di medio/alto livello.

Ai Gestori dei servizi potranno essere richieste ulteriori documentazioni relative alla sicurezza dei dati custoditi.

✓ *Trattamenti senza l'ausilio di strumenti elettronici*

Tale trattamento prevede che i dati siano conservati in archivi cartacei o su supporti di tipo magnetico e/o ottico.

La documentazione è conservata in luoghi non accessibili a personale non autorizzato e, laddove contenente dati sensibili, in armadi muniti di chiave.

Tutti i dati sono raccolti per perseguire finalità istituzionali e contrattuali, o in ottemperanza a disposizioni normative e regolamentari.

Tutti i trattamenti vengono conservati agli atti per il periodo obbligatorio per legge.

A titolo esemplificativo, nella tabella che segue verranno indicate per alcuni rischi potenzialmente verificabili e alcune misure di mitigazione attuate dall'Azienda Meyer.

Rischio	Misura
Accesso non autorizzato	✓ la conservazione dei documenti contenenti dati personali e/o sensibili avviene in archivi ad accesso selezionato e controllato chiusi a chiave; i locali in cui sono conservati tali documenti sono chiusi al termine dell'orario di lavoro i documenti contenenti dati sensibili, se affidati al soggetto autorizzato del trattamento, devono da questo essere conservati in modo tale da non garantire a terzi la consultabilità degli stessi fino alla restituzione all'archivio d'ufficio; ✓ l'accesso agli archivi non è consentito dopo l'orario di chiusura degli stessi, coincidente con l'orario di chiusura degli uffici o con l'effettivo termine delle attività lavorative. Peraltro, qualora si renda necessario consentire l'accesso agli archivi dopo l'orario di chiusura degli stessi, occorre prevedere procedure di controllo e di identificazione e registrazione dei soggetti ammessi, fatte salve preventive autorizzazioni; ✓ i documenti contenenti dati personali non rimangono incustoditi su scrivanie o tavoli di lavoro; ✓ si fanno attendere i soggetti estranei in luoghi in cui non siano presenti informazioni riservate o dati personali; se per ragioni di lavoro gli stessi possono accedere agli uffici, si ha cura di riporre eventuali documenti e se necessario di attivare il salvaschermo dei p.c..
trattamento non autorizzato	✓ i soggetti autorizzati al trattamento sono autorizzati al trattamento dei soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento dell'incarico affidato o per l'espletamento delle competenze attribuite alla struttura organizzativa di riferimento ✓ divieto di richiedere, raccogliere e/o conservare in fascicolo dati personali non pertinenti con le competenze e le attività svolte o eccedenti le necessità istruttorie delle attività assegnate i dati non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative; ✓ il trasporto di dati personali all'esterno dei locali ove si svolge il trattamento, ma comunque all'interno dell'Azienda avviene in modo da garantirne la riservatezza.
Trattamento non conforme alla finalità della raccolta o illecito	✓ i dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo ✓ è previsto da parte dei soggetti responsabili del trattamento l'aggiornamento periodico delle banche dati aziendali di rispettiva competenza, in particolare per

	quanto riguarda i dati sensibili e giudiziari, secondo i principi di pertinenza, non eccedenza, indispensabilità rispetto alle finalità perseguite nei singoli casi ✓ a tal fine, i documenti riportanti dati non più occorrenti - se non protocollati e/o allegati in fascicolo - vengono di norma distrutti (con modalità che ne garantiscano la non intelligibilità) e qualora fossero conservati, non sono comunque utilizzabili. ✓ i supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di un eventuale riutilizzo; se ciò non è possibile devono essere distrutti.

a. Ulteriori misure organizzative

Con riguardo alle problematiche di tutela della privacy nell'**esercizio della professione sanitaria e delle attività correlate**, in Azienda si ha cura di adottare, tra le altre, anche le seguenti misure organizzative:

- ✓ chiamata degli interessati prescindendo dall'individuazione nominativa degli stessi in caso di prenotazione e attesa;
- ✓ accorgimenti utili al rispetto delle distanze di cortesia;
- ✓ soluzioni atte a garantire la riservatezza dei colloqui;
- ✓ cautele volte ad evitare che la prestazione, ivi compresa l'anamnesi, avvengano in condizioni di promiscuità;
- ✓ garanzie di informativa ai soli terzi legittimati in ordine alle prestazioni eseguite e sulla dislocazione degli ospiti nell'ambito dei reparti, previo consenso degli interessati;
- ✓ procedure atte a prevenire esplicite correlazioni fra l'interessato e reparti/strutture indicative di un particolare stato di salute;
- ✓ tutela della dignità della persona, anche adottando – se del caso – accorgimenti provvisori per delimitare la visibilità dell'interessato durante l'orario di visita, ai soli familiari e conoscenti;
- ✓ divieto di affissione di liste di ospiti/utenti in locali aperti al pubblico;
- ✓ evitare la visibilità ad estranei di documenti sulle condizioni cliniche dell'interessato;
- ✓ rilasciare informazioni sullo stato di salute a persone diverse dall'interessato solo dietro acquisizione di specifico consenso (anche rilasciato da persone legittimate a farlo in caso di impossibilità o incapacità dell'interessato) e solo per il tramite di un medico designato dall'interessato, o dal responsabile del trattamento dei dati (individuato – per i dati di carattere sanitario e per le cartelle cliniche - nel Direttore Medico e nel Direttore del Laboratorio di Analisi, per quanto di rispettiva competenza): quest'ultimo può autorizzare a ciò per iscritto operatori sanitari diversi dai medici che, nell'esercizio dei propri compiti, intrattengano rapporti diretti con i pazienti, individuando nell'atto di incarico appropriate modalità e cautele;

- ✓ consentire il ritiro di referti diagnostici, risultati di analisi e certificazioni solo a terzi muniti di delega e con consegna in busta chiusa.

b. Soggetti terzi

I soggetti terzi che accedono alla struttura (compresi i volontari) devono rispettare, in materia di privacy e di approccio agli ospiti, tutte le regole e le garanzie previste per il personale.

In ogni caso, è previsto per i soggetti esterni il divieto di effettuare fotografie e/o riprese video di persone ed ambienti senza preventivo formale assenso rispettivamente da parte degli interessati e dei responsabili di struttura.

CONCLUSIONI

È cura del Titolare e dei Responsabili regolamentare l'accesso a tutte le apparecchiature elettroniche e/o alla documentazione cartacea presente nei locali dell'Azienda Meyer, anche se non adibite nello specifico a trattamenti di dati.

I soggetti autorizzati al trattamento dei dati sono destinatari di istruzioni in ordine al trattamento dei dati, alle sue finalità, al controllo ed alla custodia degli atti e dei documenti contenenti dati personali, alla gestione in sicurezza delle banche dati e degli archivi di riferimento.

Vengono, inoltre, in particolare formati sui rischi relativi ai dati e sulle correlate misure di sicurezza, sugli accorgimenti operativi da adottare per la protezione degli stessi, sulle responsabilità derivanti dal processo di trattamento dei dati.
Tale formazione è prevista al momento dell'ingresso in servizio dell'operatore destinato ad operazioni di trattamento dei dati, e -se del caso - in occasione di cambiamento di mansioni o di introduzione di nuovi strumenti o procedure rilevanti rispetto al trattamento dei dati personali.

ALLEGATI

1. Allegato – Scheda registro del Trattamento.
2. Allegato – Strumenti Hardware e Software
3. Allegato – Elenco ricerche scientifiche mediche