

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

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

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

PREMESSA E CAMPO DI APPLICAZIONE.....	3
DEFINIZIONI.....	3
DISPOSIZIONI GENERALI.....	5
1. PRINCIPI GENERALI	5
2. I SOGGETTI PRIVACY	6
2.1 Il Titolare del Trattamento.....	7
2.2 Contitolarità del trattamento.....	7
2.3 Il referente privacy	8
2.4 I soggetti autorizzati	9
2.5 <i>Il Responsabile del trattamento (art. 28 GDPR)</i>	10
2.6 <i>Referente delle tecnologie informatiche</i>	10
2.7 <i>Il Responsabile della protezione dei dati (DPO)</i>	11
2.8 <i>Soggetti terzi (esterni)</i>	11
3. IL TRATTAMENTO DEI DATI.....	11
3.1 <i>Liceità del trattamento</i>	11
3.2 <i>Dati trattati e raccolta</i>	12
3.2.1 <i>Dati relativi alla salute – Esonero consenso</i>	13
3.2.2 <i>Dati relativi agli aspetti amministrativi</i>	13
3.2.3 <i>Tabella esemplificativa delle Finalità</i>	14
4. DIRITTI DEGLI INTERESSATI.....	15
4.1 <i>Esercizio dei diritti degli interessati</i>	15
4.2 <i>Accesso alla documentazione sanitaria</i>	16
4.3 <i>Trasparenza e pubblicità legale</i>	17
4.4 <i>Ulteriori misure operative sui diritti degli interessati</i>	18
DISPOSIZIONI SPECIFICHE	18
1. LIBERA PROFESSIONE	18
2. TRATTAMENTI PER RICERCA E SPERIMENTAZIONI CLINICHE.....	19
3. SISTEMI DI VIDEOSORVEGLIANZA	20
4. DATA BREACH O VIOLAZIONE DEI DATI PERSONALI	20
5. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO.....	20
DISPOSIZIONI FINALI	21
1. FORMAZIONE	21
2. VERIFICHE PERIODICHE	21
3. CONCLUSIONI.....	21

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

PREMESSA E CAMPO DI APPLICAZIONE

Le presenti Linee Guida disciplinano il sistema di gestione dei dati personali all'interno dell'Azienda Ospedaliero Universitaria Meyer, nel rispetto della normativa specifica, e riguardano tutti i trattamenti effettuati dalla stessa o per suo conto.

Richiamano al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (c.d. regolamento generale sulla protezione dei dati), e al Decreto Legislativo 30 giugno 2003 n.196, recante il "Codice in materia di protezione dei dati personali", così come modificato dal Decreto Legislativo n.101 del 10 agosto 2018, recante "Disposizioni per l'adeguamento della normativa nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

Il contenuto del presente documento è destinato a tutti gli interessati, referenti privacy e responsabili del trattamento nonché a tutti i soggetti autorizzati che effettuano operazioni di trattamento dati personali per conto dell'Azienda Meyer, allo scopo di garantire e proteggere i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei propri dati personali. A garanzia della conformità alla normativa si precisa che ciascuna area o settore dell'Azienda potrà dotarsi, in aggiunta e nel rispetto delle prescrizioni del seguente Regolamento, di proprie direttive specifiche per regolare casi particolari attinenti al trattamento dati personali.


DEFINIZIONI

Il dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato).

Il dato sensibile: qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Il dato relativo alla salute: qualsiasi dato personale attinente 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 (art. 4, n. 15, GDPR 679/2016).

Il dato genetico: qualsiasi dato personale relativo alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13, GDPR 679/2016).

Il dato biometrico: qualsiasi dato personale ottenuto da un trattamento tecnico specifico relativo 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 (art. 4, n. 14, GDPR 679/2016).

Il 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 (art. 4, n. 2, GDPR 679/2016).

Ambito sanitario: il contesto organizzativo, funzionale e professionale in cui soggetti specificamente autorizzati svolgono attività finalizzate alla tutela della salute, nelle quali e per le quali è essenziale il trattamento di dati idonei a rivelare lo stato di salute degli interessati.

Dossier sanitario: banca dati elettronica comprendente dati e documenti sanitari in possesso di uno specifico Organismo, relativi ad uno o più percorsi di cura effettuati presso di esso da un certo assistito. Banca dati dinamica ed accessibile nel suo complesso da parte di soggetti incaricati facenti parte di una struttura che abbia in carico l'assistito.


La cartella clinica elettronica: collezione sistematica di informazioni sulla salute degli individui o di una popolazione in formato digitale.

La profilazione: qualsiasi forma di trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica, come ad esempio il rendimento professionale, la salute, le preferenze personali, l'ubicazione o gli spostamenti della stessa.

La pseudonimizzazione: il trattamento dei dati personali in modo che gli stessi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che queste ultime 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 (art. 4, n. 5, GDPR 679/16).

Il titolare del trattamento: 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.

Il 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;

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Il referente del trattamento: la persona fisica o giuridica, il servizio o altro organismo che, all'interno dell'azienda ed in relazione ad aree specifiche di competenza, tratta dati personali per conto del titolare del trattamento.

L'incaricato o autorizzato al trattamento: la persona fisica o giuridica, il servizio o altro organismo che ha accesso consentito al trattamento dei dati personali in un ambito di attività puntualmente individuato, sotto l'autorità diretta del referente o del titolare del trattamento.

L'interessato: persona fisica cui si riferiscono i dati personali trattati.

Il DPO (Data Protection Officer): la persona fisica o giuridica, il servizio o altro organismo nominato responsabile della protezione dei dati.

Il destinatario: la persona fisica o giuridica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di soggetti terzi.

Il 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.

L'informativa: informazione messa a disposizione dell'interessato attraverso la quale questi è edotto circa le modalità e le finalità del trattamento dei dati personali.


Violazione dei dati personali: 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.

La videosorveglianza: controllo ambientale effettuato nei locali o nelle pertinenze aziendali mediante apparecchi audiovisivi che rilevano immagini in una certa area, con possibilità o meno di registrazione degli eventi che vi accadono.

DISPOSIZIONI GENERALI

1. PRINCIPI GENERALI

Alla luce dell'entrata in vigore e dell'applicazione del nuovo Regolamento Europeo n. 679/2016 in materia di protezione delle persone fisiche con riguardo al trattamento di dati personali ed alla libera circolazione di tali dati, l'Azienda Ospedaliero-Universitaria Meyer (di seguito "Azienda" o "Meyer") si pone come obiettivo di adeguarsi alle nuove disposizioni in materia e garantisce che i trattamenti di dati personali effettuati per l'adempimento delle proprie attività istituzionali si svolgano nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

In particolare l'Azienda Meyer provvede al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 5 del Regolamento Europeo sulla protezione dei dati personali, in particolare dei principi di semplificazione, liceità, correttezza e trasparenza e adotta misure tecniche e organizzative volte a garantire un adeguato livello di sicurezza dei dati, configurando i propri sistemi informativi e i programmi informatici in modo da ridurre al minimo i rischi per i diritti e le libertà degli interessati ed attraverso un apposito processo di rendicontazione si impegna a dare conto ai diretti interessati di tutte le attività aventi ad oggetto uno o più trattamenti sui dati personali e ad assumersene le proprie responsabilità.

2. I SOGGETTI PRIVACY

Ai fini della corretta individuazione dei soggetti coinvolti nel trattamento dei dati personali, sarà utile una breve premessa funzionale all'inquadramento aziendale di queste categorie.

La nuova normativa europea, abrogando la disciplina previgente, prevede tre figure tipiche di soggetti che operano il trattamento di dati personali: il Titolare, il Responsabile e il soggetto autorizzato del trattamento; in questa ottica è bene precisare che il Responsabile è inteso come figura esterna, terza rispetto al titolare del trattamento.


Per qualificare la figura del responsabile del trattamento, qualora questo fosse invece interno all'Azienda Titolare, verrà sin da ora utilizzato il termine "referente".

È bene sin da ora precisare che L'Azienda Meyer quale Titolare del Trattamento definirà, attraverso una serie di nomine e deleghe ufficiali, i rapporti di tutti i soggetti che interverranno nel trattamento o in un processo di trattamenti di dati personali.

Sarà possibile dunque, di volta in volta, individuare il soggetto preposto al controllo della correttezza e liceità del trattamento, nonché tutti i soggetti singolarmente coinvolti nel trattamento stesso.

Nell'ambito delle proprie attività amministrative, L'Azienda avrà l'opportunità di redigere regolarmente apposito elenco dei suoi dipendenti e collaboratori, ai fini dell'individuazione della categoria professionale cui essi appartengono e delle mansioni che andranno a svolgere, con riferimento anche al trattamento dati.

Le direttive regionali in materia prevedono che ogni azienda sanitaria tenga ed aggiorni un censimento dei trattamenti dei dati personali eseguiti e dei soggetti preposti a tali attività, individuati in ragione delle loro funzioni anche di carattere organizzativo ed amministrativo.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

L' Azienda, pertanto, non consente il trattamento di dati da parte di personale non individuato, direttamente o indirettamente, a pena di incorrere in un trattamento illegittimo passibile di sanzioni.

Il Titolare del Trattamento

Il Titolare del trattamento è l'Azienda Meyer che esercita i poteri propri del titolare per mezzo del Legale Rappresentante, il quale può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati (DPO).

Il Titolare, cui competono le decisioni in ordine ai fini, alle modalità e ai mezzi del trattamento, ivi compreso il profilo della sicurezza, provvede alla corretta applicazione della normativa in materia di protezione dati, anche avvalendosi dell'Ufficio Privacy e del Comitato Privacy Aziendale.

Il Titolare provvede a nominare i delegati al trattamento e, al fine di adempiere all'obbligo di cui all'art. 28 del Regolamento UE, a designare quali Responsabili del trattamento – mediante apposito contratto - tutti i soggetti terzi che, in esecuzione di un contratto di fornitura o di una convenzione, effettuino un trattamento di dati personali per conto del Titolare stesso.


Si deve altresì chiarire che all'Azienda, quale Titolare del trattamento, e non alle sue singole articolazioni organizzative e di responsabilità, che spetta il compito di operare le scelte di fondo sulle finalità, modalità, strumenti, inerenti al trattamento dei dati.

Contitolarità del trattamento

Per un dato trattamento può essere configurata una situazione di contitolarità. Essa deve essere ricondotta ad una comunanza nella possibilità di determinare finalità e modalità del trattamento, derivante dalla compartecipazione finale agli interessi in vista dei quali il trattamento è predisposto (*Art. 26 GDPR*).

Sarà necessario esplicitare (anche a livello di informativa al paziente) questi ambiti di contitolarità in riferimento a percorsi sanitari che prevedano la compartecipazione paritaria e coordinata da parte di più enti.

Anche nei casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento, dovrà di volta in volta rappresentare una chiara ripartizione delle responsabilità al fine di proteggere i diritti e le libertà degli interessati (*Considerando n. 49 GDPR*).

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Il referente privacy


In applicazione di quanto disposto dal Regolamento UE e dal Codice Privacy in tema di profili di responsabilità e designazione dei soggetti autorizzati ad eseguire operazioni di trattamento di dati personali, avvalendosi dello strumento della delega, ha attribuito compiti e funzioni proprie del Titolare ai Direttori di Struttura Complessa e ai Responsabili di Struttura Semplice Dipartimentale, nonché a taluni dirigenti/funzionari individuati in virtù delle particolari attività svolte e/o della tipologia dei dati trattati, quali i Responsabili Scientifici di volta in volta individuati nell'ambito di ogni singolo progetto di ricerca/sperimentazione.

In virtù dell'atto di delega il Titolare impartisce a tali soggetti le istruzioni e gli adempimenti connessi

a una compiuta e corretta attività di protezione dei dati personali, tra i quali, secondo un elenco non

esaustivo:

- fare osservare le istruzioni e le direttive aziendali in materia di protezione dati, fornite dal Titolare del trattamento, anche per il tramite dell'Ufficio Privacy Aziendale e del Servizio ICT Aziendale;
- porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati;
- vigilare sulla conformità dell'operato dei propri preposti alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
- verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;
- attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento;
- compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- partecipare ai momenti formativi organizzati dalla Azienda ed assicurare la partecipazione dei propri preposti;
- fornire le informazioni richieste dall'Ufficio Privacy Aziendale, segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati;
- comunicare all'Ufficio Privacy Aziendale i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;

- non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- provvedere, qualora tra le attività istituzionali della struttura vi sia la stipula di contratti o convenzioni con soggetti esterni alla organizzazione che comporti il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula e sottoscrizione del relativo atto di designazione di tali soggetti esterni quali "Responsabili del trattamento" a norma dell'art. 28 del Regolamento UE e delle condizioni ivi indicate;
- comunicare tempestivamente all'Ufficio Privacy Aziendale i potenziali casi di *data breach* all'interno della propria struttura e collaborare alla istruttoria del caso;
- provvedere, di volta in volta, ad autorizzare al trattamento dei dati personali i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori).


I soggetti autorizzati

Ai fini dell'autorizzazione al trattamento, prevista dall'art.2-quaterdecies del D.lgs.n.196/2003 e s.m.i., si precisa che per "personale autorizzato al trattamento dei dati" (già «personale incaricato di trattamento dati») s'intende, in via generale, tutto il personale dipendente dell'Azienda Meyer, nonché tutti coloro che, pur in assenza di un rapporto di lavoro dipendente, siano, a vario titolo, inseriti stabilmente all'interno

dell'organizzazione ed effettuino operazioni di trattamento dei dati personali, ognuno per il proprio specifico ambito di competenza professionale, e che il personale già nominato incaricato di trattamento - alla data di adozione della citata deliberazione - sia da considerarsi personale autorizzato al trattamento.

La nomina dei dipendenti e di coloro che, a diverso titolo, trattano i dati personali nel contesto della singola articolazione aziendale costituisce atto autorizzativo al relativo trattamento ai sensi degli articoli 29 del Regolamento UE e 2-quaterdecies del Codice.

Spetta all'amministrazione del Personale nominare i soggetti autorizzati al trattamento al momento della sottoscrizione del contratto individuale di lavoro, del contratto di collaborazione coordinata e continuativa, del contratto libero professionale, del contratto di borsa di studio, del trasferimento e/o mutamento di mansioni. Contestualmente vengono fornite le istruzioni operative di carattere generale e particolare di cui sono invitati a prendere visione.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Il Responsabile del trattamento (art. 28 GDPR)

Il Responsabile del trattamento» (ex «Responsabile esterno») è la persona fisica o giuridica, autorità pubblica, servizio o altro organismo esterno rispetto all’Azienda Meyer, che, in virtù di rapporti contrattuali o convenzionali, previa designazione, tratta dati personali per conto del Titolare del trattamento.

L’atto di designazione viene predisposto secondo schema tipo, redatto secondo le disposizioni del Regolamento UE 2016/679, adottato dal Titolare del Trattamento e pubblicato sul sito web aziendale nell’apposita sezione Policy Privacy.

Nel rispetto delle istruzioni operative impartite dal Titolare, spetta al Direttore/dirigente responsabile del procedimento relativo al rapporto contrattuale o convenzionale con soggetti esterni provvedere alla designazione di tali soggetti contestualmente alla sottoscrizione del contratto/accordo/convenzione, quali “responsabili del trattamento” a norma dell’art.28 del Regolamento UE.


L’Ufficio Privacy e il DPO devono prendere evidenza di tale designazione, anche ai fini dell’aggiornamento del Registro delle attività di trattamento dei dati aziendale.

NOTA: *Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l’esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell’Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento. Qualora l’altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l’intera responsabilità dell’adempimento degli obblighi dell’altro responsabile (art. 28 comma 4 GDPR).*

Referente delle tecnologie informatiche

Al referente delle tecnologie informatiche, spettano i seguenti compiti:

- sovrintendere alle risorse del sistema informatico centralizzato (software dipartimentali e trasversali) e consentirne l'utilizzazione a tutti i Referenti e soggetti autorizzati, mediante l’adozione delle misure di sicurezza tecniche di cui all’art.32 del Regolamento UE;
- garantire la gestione e manutenzione degli strumenti elettronici aziendali;

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

- garantire la protezione dei dispositivi e dei programmi contro il rischio di intrusione e dell'azione di programmi di cui all'art.615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- garantire gli aggiornamenti periodici, almeno con cadenza annuale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti.

Il Responsabile della protezione dei dati (DPO)

In applicazione dell'art. 37 del Regolamento UE, che prevede la nomina obbligatoria del Responsabile della Protezione dei Dati (DPO) per tutte le pubbliche amministrazioni, anche l'Azienda Meyer ha nominato il proprio DPO, attribuendogli il ruolo e i compiti previsti dagli artt. 38 e 39 del Regolamento UE.

Soggetti terzi (esterni)

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.

IL TRATTAMENTO DEI DATI

Liceità del trattamento

I trattamenti dei dati personali che avvengono all'interno dell'Azienda Meyer sono leciti e ricorre sempre almeno una delle seguenti condizioni (art. 6 del GDPR):

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

I Referenti Privacy e/o i soggetti autorizzati sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli artt.13 e 14 del Regolamento UE, predisposte nel rispetto delle indicazioni fornite dal Titolare del trattamento e/o dal Responsabile della Protezione dei Dati.


Dati trattati e raccolta

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.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

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.

Dati relativi alla salute – Esonero consenso


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.


Dati relativi agli aspetti amministrativi

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

L'Azienda Meyer tratta 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.

Tabella esemplificativa delle Finalità

Finalità del trattamento	Categorie di dati personali	Base giuridica del trattamento
Attività di didattica e formazione universitaria	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	Art. 9, par. 2, lett. g) del GDPR e art. 2-sexies, comma 2, lett. bb) D. Lgs. 196/2003)
Vigilanza sulle sperimentazioni, farmacovigilanza e vigilanza sui dispositivi medici	Dati personali, categorie particolari di dati personali (tra cui: dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)	Art. 9, par. 2, lett. g) e i) del GDPR e art. 2-sexies, comma 2, lett. z) D. Lgs. 196/2003) interesse pubblico rilev interesse pubblico nel settore della sanità pubblica
Instaurazione, gestione ed estinzione di rapporti di lavoro in ambito pubblico, anche non retribuito, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, pari opportunità, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici, dati biometrici, appartenenza sindacale, convinzioni religiose), dati giudiziari, relativi a carichi pendenti e condanne penali e civili per danno all'immagine o per responsabilità professionale e condanne per danno erariale nonché sanzioni disciplinari	Art. 6, par. 1, lett. b) GDPR "Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte" Art. 6, par. 1, lett. c) GDPR "Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" Art. 88 del GDPR Per i dati particolari: Art. 9, par. 2, lett. g) e h) del GDPR e art. 2-sexies, comma 2, lett. u) e dd) e D. Lgs. 196/2003 "Il trattamento è necessario per motivi di interesse pubblico rilevante" e per "finalità di medicina del lavoro, valutazione della capacità lavorativa del lavoratore"
Gestione del contenzioso	Dati personali, categorie particolari di dati personali (dati relativi alla salute, dati genetici e dati biometrici)	Art. 9, par. 2, lett. f) del GDPR "Il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria"
Fornitura di beni e servizi o esecuzione di opere edilizie e interventi di manutenzione necessari per il perseguimento delle finalità istituzionali dell'Azienda	Dati personali	Art. 6, par. 1, lett. b) del GDPR "Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte"

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Pubblicazione di atti e documenti per finalità di trasparenza	Dati personali	Art. 6, par. 1, lett. e) del GDPR „Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento” Art. 86 del GDPR
Tutela dei beni aziendali e del patrimonio, sicurezza e incolumità delle persone, accertamento dei reati	Dati personali (immagini di videosorveglianza)	Art. 6, par. 1, lett. e) del GDPR „Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui è investito il titolare del trattamento” Art. 6, par. 1, lett. f) del GDPR „Il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento, o di terzi”
Analisi di gradimento e valutazione della qualità dei servizi	Dati personali	Art. 6, par. 1, lett. a) del GDPR esplicito per una o più finalità specifiche

DIRITTI DEGLI INTERESSATI

Nella organizzazione delle prestazioni e dei servizi, l'Azienda adotta misure di tipo organizzativo volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

L'accesso agli archivi aziendali è controllato e sono identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura. La responsabilità della conservazione e della sicurezza degli archivi amministrativi contenenti dati personali e allocati in strutture aziendali ricade sul Responsabile del Servizio/Struttura che li produce e detiene, fino al loro conferimento all'archivio di deposito.


La responsabilità della conservazione e della sicurezza delle cartelle cliniche e della documentazione sanitaria è in capo ai Direttori delle rispettive unità operative di produzione, fino al loro conferimento all'archivio di deposito.

Della corretta gestione, conservazione e della sicurezza di tale archivio risponde il soggetto terzo a cui l'archivio è affidato in *outsourcing*.

Esercizio dei diritti degli interessati

L'Azienda agevola l'esercizio dei diritti degli interessati nel rispetto dei principi di semplificazione e trasparenza.

Nello specifico, sono state individuate le misure procedurali disposte dal Titolare del trattamento per permettere all'utente interessato di ottenere in qualsiasi momento informazioni sull'utilizzo dei propri dati ai sensi degli artt.15-21 del Regolamento UE,

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

esercitando i diritti:

- di accesso (art.15);
- di rettifica (art.16);
- alla cancellazione (art.17);
- di limitazione del trattamento (art.18);
- alla portabilità dei dati (art.20);
- di opposizione al trattamento (art.21).

A tal fine, le richieste di accesso ai propri dati personali, di rettifica, aggiornamento, cancellazione, integrazione dei dati, nonché di opposizione al trattamento possono essere presentate all'Azienda Meyer, utilizzando l'apposito modulo presente nella sezione Privacy del sito aziendale.


Accesso alla documentazione sanitaria

L'Azienda applica quanto contenuto nell'art. 59 del D. Lgs. 196/2003 in materia di accesso a documenti amministrativi contenenti dati personali, disciplinato dalla L. 241/90, e di accesso civico, disciplinato dal D. Lgs. 33/2013. In osservanza delle richiamate disposizioni l'Azienda valuta caso per caso, anche con riguardo ad altre regolamentazioni specifiche, la possibilità da parte di terzi di accedere a documenti contenenti dati di cui agli articoli 9 e 10 del GDPR.

Invece, ai sensi dell'art. 60 del D. Lgs. 196/2003, quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Così:

- Per quanto concerne la richiesta di copia di cartella clinica o di altra documentazione sanitaria riferita allo stesso richiedente, si rinvia alla procedura aziendale per l'accesso alla documentazione sanitaria.
- per le richieste di presa visione o di rilascio di copia della cartella clinica o in generale di documentazione sanitaria da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:
 - ✓ di esercitare o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

- ✓ di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.


In particolare, in caso di richiesta di cartella clinica e di altri documenti sanitari ai fini della difesa in giudizio o ai sensi dell'art. 391^{quater} c.p.p., ai fini della valutazione dell'ammissibilità e fondatezza della richiesta il difensore deve documentare la sua veste, anche mediante autocertificazione che individui gli estremi del procedimento nel quale svolga tale funzione e deve specificare le ragioni per le quali ritiene che le informazioni contenute nei documenti richiesti siano rilevanti per la finalità difensiva del proprio assistito, anche mediante esibizione di documenti che ritenga all'uopo giustificativi.

Trasparenza e pubblicità legale

Ai sensi dell'art. 2-septies, comma 8, del D. Lgs. n. 196/2003, e dell'art. 7-bis, comma 6, del D. Lgs. n. 33/2013 è sempre vietata la diffusione di dati genetici, biometrici e relativi alla salute e alla vita sessuale.

Salvo diversa disposizione di legge, i documenti da pubblicare sul sito istituzionale per finalità di trasparenza e/o pubblicità legale non devono contenere in forma intelligibile dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle finalità di trasparenza della pubblicazione.

Tra i dati da oscurare o rendere anonimi o da pseudonomizzare si citano, a titolo esemplificativo e non esaustivo: utenza telefonica e posta elettronica privati, indirizzi di residenza, codice fiscale, indicatore ISEE, carta d'identità o altra documentazione personale, numero di IBAN, dati relativi a condanne penali o reati, documentazione da cui si possa desumere, anche indirettamente, l'esistenza di patologie o condizioni di invalidità, disabilità, handicap fisici e/o psichici che riguardano l'interessato o familiari, documentazione da cui si evinca l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, politico o sindacale. In tutti questi casi l'ufficio competente alla redazione e conservazione del documento, con la consulenza ove necessario del Responsabile della protezione dei dati, verifica, caso per caso, se esistano i presupposti per oscurare od omettere determinate informazioni prima della trasmissione all'ufficio deputato alla pubblicazione sul sito web aziendale.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Ulteriori misure operative sui diritti degli interessati

È fatto divieto a chiunque di fornire indicazioni inerenti lo stato di salute degli interessati per via telefonica o telematica.

Il Referente Privacy cura che:

- le fotocopiatrici ed i fax siano collocati in un'area protetta e presidiata e che il personale autorizzato presti attenzione alle fasi di invio e di ricevimento della documentazione contenente dati personali, non lasciandoli esposti alla visibilità di chiunque;
- nel caso si debba procedere alla comunicazione di dati particolari tramite fax con un ente esterno autorizzato per legge all'acquisizione di tale documentazione, laddove ne sia consentito l'utilizzo, si concordi un numero di fax non accessibile a terzi da utilizzare sempre e in modo esclusivo per tale comunicazione. Ciascuna comunicazione dovrà essere preceduta da una copertina nella quale non siano inclusi dati personali particolari né dati personali di soggetti diversi dal mittente e dal destinatario.


Il personale autorizzato al trattamento è tenuto al ritiro tempestivo della documentazione dalla stampante e dalla fotocopiatrice contenente dati personali ed alla conservazione della stessa. In tali casi è comunque fatto divieto di utilizzare supporti cartacei che contengano già informazioni personali e particolari sull'altro lato del foglio. Il personale autorizzato che proceda alla eliminazione di stampe e fotocopie è tenuto a distruggere fisicamente i supporti in modo da impedire la ricostruzione o comunque da renderla non facilmente accessibile a terzi non autorizzati. La trasmissione interna ed esterna di corrispondenza e di documentazione contenente dati particolari deve essere effettuata necessariamente in busta chiusa e sigillata che riporti il nominativo del destinatario.

L'accesso alle immagini registrate dai sistemi di videosorveglianza è consentito nel rispetto di quanto previsto dalle linee guida in materia di Videosorveglianza.

Laddove necessario per finalità di diagnosi e terapia o per la corretta alimentazione del paziente, le domande relative alla convinzione religiosa dell'interessato devono essere formulate in modo generico tale da non arrecare pregiudizio e disagio allo stesso.

DISPOSIZIONI SPECIFICHE

1 LIBERA PROFESSIONE

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

L'Azienda Meyer è Titolare del trattamento dei dati personali nell'ambito della attività libero professionale intramoenia erogata dai propri professionisti sanitari sia all'interno delle proprie strutture, sia in spazi sostitutivi.

Gli aspetti organizzativi, economici e di protezione dei dati sono definiti da apposito regolamento aziendale a cui si fa rinvio.

2 TRATTAMENTI PER RICERCA E SPERIMENTAZIONI CLINICHE


L'Azienda sostiene l'attività di ricerca e ne garantisce la gestione nel rispetto degli aspetti autorizzativi, normativo-regolatori e di protezione dei dati personali dei pazienti coinvolti. L'attività di ricerca si esplica previa specifica informativa da rendere agli interessati e previa raccolta del loro consenso, salve le deroghe sancite dall'Autorità Garante.

Infatti, ferma restando l'applicazione dell'art.104 e ss. del Codice, le informazioni di cui agli artt.13 e 14 del Regolamento UE devono essere fornite in modo tale da mettere in grado gli interessati di distinguere con le attività di ricerca da quelle di tutela della salute e, comunque, devono rendere edotto il paziente in modo chiaro ed inequivocabile che le informazioni contenute nella cartella clinica saranno utilizzate ed eventualmente comunicate ad una o più aziende farmaceutiche e/o produttrici di dispositivi medico sanitari e/o chirurgici o di altri Enti o altri committenti pubblici e privati, indicate nominativamente e se i dati comunicati lo rendono identificabile o sono resi anonimi.

E così, nello specifico agli interessati saranno sempre comunicate in maniera chiara e comprensibile tutte le informazioni riguardanti le modalità e i fini della ricerca.

In tale ambito l'Azienda/Titolare si avvale dello strumento della delega di funzioni, per attribuire le competenze e le responsabilità in materia di protezione dei dati personali e i relativi compiti, oltre a quelli ulteriori legati alla specifica attività, a ciascun Responsabile Scientifico volta per volta individuato nel provvedimento autorizzatorio per ciascun progetto di ricerca/sperimentazione clinica. Gli aspetti procedurali, amministrativi ed economici per la conduzione di ricerche e sperimentazioni cliniche sono definiti da apposito documento aziendale a cui si fa rinvio.

Il trattamento dei dati genetici è consentito nei soli casi previsti dall'art. 9, par. 2 del Regolamento UE, nonché nel rispetto delle relative prescrizioni approvate dall'Autorità Garante nel Provvedimento del 5/6/2019 n. 146 che ha aggiornato, adeguandole al Regolamento UE, le prescrizioni di cui alla previgente n.8/2016 e delle misure di garanzia approvate dall'Autorità.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

3 SISTEMI DI VIDEOSORVEGLIANZA

L'installazione di apparecchiature di videosorveglianza è autorizzata dall'Azienda nel rispetto delle disposizioni vigenti, solo quando ciò sia strettamente indispensabile per garantire la sicurezza del patrimonio aziendale e delle persone che, a vario titolo, accedano alle strutture aziendali.

Il trattamento dei dati personali effettuato attraverso i sistemi di videosorveglianza avviene nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori (art. 4 L. 300/1970 s.m.i.) e dei Provvedimenti in materia emessi dall'Autorità Garante per la protezione dei dati personali.

Per la procedura di installazione degli impianti di videosorveglianza e per le misure di sicurezza da osservare si fa rinvio ad apposito regolamento aziendale.

4 DATA BREACH O VIOLAZIONE DEI DATI PERSONALI

In caso di violazione dei dati personali (c.d. *data breach*), anche potenziale, si applica la procedura adottata dall'Azienda Meyer, in conformità agli artt.33 e 34 del Regolamento UE, al fine di tutelare le persone, i dati e le informazioni e di documentare i flussi per la gestione delle violazioni dei dati personali.


La procedura definisce i ruoli e le funzioni dei soggetti coinvolti nella valutazione e graduazione del rischio della eventuale violazione e le fasi istruttorie conseguenti.

L'intero iter di gestione della segnalazione viene documentato dal DPO nel Registro Aziendale delle Violazioni.

5 REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, contenente le informazioni di cui all'art. 30, paragrafo 1, del GDPR:

- a) il nome e i dati di contatto del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

	Regolamento Aziendale Privacy	CODICE
	MEYER	All.1 AZI056 rev.0 Data 13/05/2020

Ogni responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare, contenente le informazioni di cui all'art. 30, paragrafo 2, del GDPR.

DISPOSIZIONI FINALI

6 FORMAZIONE

L'Azienda Meyer individua nella formazione del personale un elemento strategico della propria politica in materia di protezione dei dati personali.

La formazione, individuata quale formazione obbligatoria sarà erogata, attraverso il Laboratorio Formas di Regione Toscana, in modalità di e-learning.

7 VERIFICHE PERIODICHE

Il Titolare, tramite verifiche periodiche affidate al Responsabile per la Protezione dei Dati (DPO) e/o ad altro soggetto in possesso di comprovate capacità professionali, effettua attività di audit, intesa come attività di controllo interno volta a verificare la conoscenza delle procedure aziendali, e i controlli opportuni per vigilare sulla puntuale osservanza della normativa vigente.

8 CONCLUSIONI

Ne caso emergano dubbi sulla applicazione della normativa in materia di protezione dei dati personali e delle presenti linee guida il personale autorizzato è tenuto ad attenersi al criterio della tutela e del massimo rispetto della riservatezza nei confronti dell'interessato, pur garantendo allo stesso tempo il normale espletamento delle attività.

In ogni caso, il personale autorizzato è tenuto a rivolgersi al Referente Privacy di afferenza, il quale può avvalersi del supporto del Responsabile della Protezione dei dati – DPO.

Per tutto quanto non espressamente previsto dalle presenti Linee Guida si rinvia alle disposizioni europee, nazionali, regionali ed aziendali in materia.