SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO DELIBERAZIONE

AOO: DA

REGISTRO: Deliberazione

NUMERO: 0000320

DATA: 21/12/2018 18:04

OGGETTO: Adeguamenti al Regolamento (UE) n. 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e al D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal D.lgs. n. 101/2018: DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI E MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI - provvedimenti conseguenti di individuazione dei soggetti autorizzati al compimento delle operazioni di trattamento e dei referenti privacy del trattamento dati

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Cavalli Mario in qualità di Direttore Generale
Con il parere favorevole di Landini Maria Paola - Direttore Scientifico
Con il parere favorevole di Rolli Maurizia - Direttore Sanitario
Con il parere favorevole di Cilione Giampiero - Direttore Amministrativo

Su proposta di Laura Mandrioli - Affari Legali e Generali che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [06-04]

DESTINATARI:

- Collegio sindacale
- Servizio Unico Metropolitano Amministrazione del Personale (SUMAP)
- Affari Legali e Generali
- Accesso ai Servizi
- Amministrazione della Ricerca
- Programmazione, Controllo e Sistemi di Valutazione
- ICT
- Servizio Prevenzione e Protezione
- Dipartimento Patologie Complesse
- Dipartimento Patologie Specialistiche

- Struttura di Supporto Direzionale
- Patrimonio ed Attivita' Tecniche
- Direzione Servizio di Assistenza Infermieristica, Tecnica e della Riabilitazione (DAITER)
- Farmacia
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Servizio Unico Metropolitano Economato (SUME)
- Servizio Bilancio e Coordinamento Processi Economici
- Dipartimento Rizzoli - Sicilia
- Direzione Scientifica
- Comunicazione e Relazione con i Media
- Marketing Sociale
- Clinical Trial Center
- Dip. Rizzoli - RIT Research, Innovation & Technology

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000320_2018_delibera_firmata.pdf		7950FF37D7FEC5799268D4E4135FC7818DDFFD8B22789D4553CAB3735226413A
DELI0000320_2018_Allegato1.docx:		98A77842EEDA1A3C8EF14E1DEE913AC80433EA4B5D72E7FDB330505D52FDBE3A
DELI0000320_2018_Allegato2.docx:		F680B62E491507AA59CCE4ACD9D8BE7BBCE0A75FB313454E4C17AED59C2DB397
DELI0000320_2018_Allegato3.docx:		91E576F2FB642629032CD94C0D2E972F91D7AAFF32656D1FBED32D1DC742324A

DELIBERAZIONE

OGGETTO: Adeguamenti al Regolamento (UE) n. 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e al D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal D.lgs. n. 101/2018: DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI E MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI - provvedimenti conseguenti di individuazione dei soggetti autorizzati al compimento delle operazioni di trattamento e dei referenti privacy del trattamento dati

IL DIRETTORE GENERALE

Premesso che

- Il 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 (di seguito anche solo "Regolamento" o "GDPR"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- Le disposizioni del D.lgs. n. 196/2003 " *Codice in materia di protezione dei dati personali*" continuano a trovare applicazione, così come integrate e modificate dal D.lgs. n. 101/2018 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 (regolamento generale sulla protezione dei dati)*";
- Nelle more necessarie per il consolidamento della nuova normativa entrata in vigore i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante") e i principi ivi sanciti continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa sopra citata;

Considerato che

- Nel percorso di attuazione ai suddetti obblighi ed adempimenti, occorre aggiornare i provvedimenti a suo tempo assunti da questa Amministrazione, ad iniziare dai provvedimenti concernenti l'individuazione di coloro che – per motivi di servizio – trattano dati personali di cui è titolare IOR;
- Il GDPR individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

a) *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,

b) *il Responsabile (esterno) 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,

c) *il Responsabile della protezione dei dati* (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del Regolamento, che ne disciplinano compiti, funzioni e responsabilità,

d) ***persone autorizzate* al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (esterno):** figura che si desume implicitamente dalla definizione di " *terzo*" di cui al n. 10 del comma 1 art. 4 del Regolamento e dall'articolo 29 del Regolamento, che pone l'obbligo di dare istruzioni a chi abbia accesso a dati personali e agisca per conto del titolare o del responsabile (esterno) e che trova conferma nell'art. 2 quaterdecies del D.lgs. 196/2003 come modificato dal d.lgs. 101/2018;

Richiamata

- La DGR Regione Emilia Romagna n. 919 del 10/4/2018 " *Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018"* che prevede fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre la nomina del DPO l'adozione del registro delle attività di trattamento, la ri-definizione ed articolazione delle specifiche responsabilità privacy aziendali;

Richiamate inoltre:

- la Delibera n. 188 del 12/06/2018 dell'Azienda USL di Bologna di nomina del Data Protection Officer (DPO), ai sensi degli artt. 37, 38 e 39 del GDPR;
- **le delibere IOR n. 704 del 17/11/2004 e n. 503 del 9/6/2006 con le quali i dipendenti e tutti i soggetti (legati da altro** rapporto formalizzato con l'Ente, di carattere contrattuale, convenzionale, di collaborazione, ecc…), **che compiono operazioni di trattamento per conto di questo Istituto sono stati individuati quali incaricati** (ai sensi dell'abrogato art. 30 D.Lgs.196/2003) di tutti i trattamenti dei dati facenti capo all'Unità Operativa alla quale sono formalmente assegnati, nell'ambito delle funzioni e dei compiti specificatamente attribuiti;
- le delibere IOR n. 178 del 23/3/2004, n. 300 del 09/7/2013 e n. 239 del 30/10/2015;

Ritenuto

- che sia necessario, pur confermando la sostanza dei provvedimenti citati, provvedere ad un loro aggiornamento, nei termini che seguono, stante l'intervenuta diretta applicabilità del Regolamento (UE) n. 2016/679 e l'entrata in vigore del D.Lgs n. 101/2018;

Ritenuto altresì:

- che talune **prerogative o obblighi inerenti gli aspetti applicativi della normativa** Privacy, senza incidere sulla titolarità, possono essere demandati a un numero ristretto di figure aziendali in ragione degli incarichi ricoperti e delle aree di autonomia correlate;

- **che** per effetto dell'incarico ricoperto e senza necessità di nomina *ad personam* **per tali prerogative o obblighi si ritiene di individuare, le seguenti figure professionali**, in quanto possiedono le competenze necessarie al fine di garantire l'adozione delle misure tecniche ed organizzative per assicurare un trattamento conforme alla normativa vigente:
  - per l'area clinica e della ricerca nonché dell'assistenza:
  i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;
  - per l'area amministrativa:
  i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;

- **di stabilire che tali figure assumano la denominazione di "Referenti privacy"**;

- che la nomina ai singoli Referenti privacy verrà comunicata mediante lettera del Direttore Generale;

- che la designazione quali Referenti Privacy potrà rendersi necessaria in capo ad **altri soggetti** – ulteriori e diversi da quelli indicati sopra – anche non titolari di incarico di Struttura Complessa e/o di Struttura Semplice Dipartimentale (a titolo esemplificativo il *Responsabile Scientifico* e/o il *Principal Investigator* dei progetti di ricerca / sperimentazione clinica), i quali verranno **individuati di volta in volta e formalmente nominati** con separati atti in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

Dato atto ulteriormente:

- che l'elenco dei Referenti privacy potrà essere integrato o modificato, in ragione delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati e che, in caso di vacanza del ruolo, i compiti sono svolti dalla figura che ne assume le funzioni;

- che tale individuazione quale Referente privacy si esplica in particolare nello svolgimento dei **compi ti - di cui all'allegato 1 -** la cui elencazione non può comunque ritenersi esaustiva rispetto a tutti i compiti e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati;

Atteso inoltre che:

- coerentemente con quanto previsto dalla normativa citata, si ritiene ora di confermare l'autorizzazione al trattamento dei dati personali da parte di tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento;

- per " **soggetti autorizzati"** si intendono tutti i dipendenti/collaboratori dell'Istituto, ognuno per il proprio specifico ambito di competenza professionale, i quali sono tenuti alla osservanza delle istruzioni – contenute nell' **allegato 2** al presente atto - impartite dal Titolare per il corretto trattamento dei dati personali, oltre ad ulteriori istruzioni che il Titolare del trattamento, anche per il tramite dei Referenti privacy, impartirà loro con riferimento a particolari trattamenti di dati;

- il personale in servizio presso l'Istituto (quale dipendente e/o collaboratore) alla data di adozione del presente Atto – e come tale già designato "incaricato del trattamento" ai sensi dell'abrogato art. 30 d.lgs. 196/2003 – deve considerarsi personale "autorizzato" al trattamento ai sensi dell'art. 29 del GDPR;

- il personale che, invece, entrerà in servizio successivamente alla data di adozione del presente Atto dovrà considerarsi designato quale "autorizzato" al trattamento dei dati contestualmente alla sottoscrizione del contratto di lavoro e/o di collaborazione;

- l'autorizzazione di cui sopra deve intendersi circoscritta esclusivamente ai trattamenti che afferiscono all'unità operativa a cui è assegnato il dipendente / collaboratore, così come indicati, oltre che nel registro dei trattamenti, nell'atto aziendale e suo regolamento attuativo, nelle assegnazioni funzionali del dipendente / collaboratore, nonché negli ulteriori atti ricognitivi dei processi e dei procedimenti e nelle eventuali ulteriori e specifiche indicazioni fornite dal Referente privacy al quale le singole unità operative fanno capo;

Ritenuto

- di comunicare tale autorizzazione al trattamento a tutti i dipendenti/collaboratori dell'Istituto tramite il portale del personale e apposita news sulla intranet;

Valutato inoltre

- con riferimento alle persone che prenderanno servizio in data successiva alla adozione del presente Atto, che l'autorizzazione al trattamento dei dati personali debba operare:

- per i dipendenti, mediante inserimento di idoneo riferimento e richiamo nel contratto di lavoro;

- per i soggetti che – in virtu' di un rapporto comunque formalizzato con l'Ente – debbano accedere e trattare dati personali, mediante la previsione, laddove possibile, di idoneo riferimento e richiamo anche nelle altre forme di contratto e/o di conferimento incarico variamente denominati (a titolo non esaustivo: legali, borsisti, tirocinanti, stagisti ecc.);

- per tutti gli altri soggetti per i quali non è prevista la sottoscrizione di un contratto/accordo individuale o comunque per i quali non è possibile la forma di designazione indicata al punto che precede (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, specializzandi ecc) sarà l'ufficio amministrativo che cura gli adempimenti finalizzati all'istaurazione del rapporto con l'Istituto a provvedere di volta in volta all'autorizzazione al trattamento dei dati attraverso l'atto di designazione **allegato sub 3)** alla presente delibera;

Atteso che

- con delibera n. 160 del 29.06.2018 l'Istituto ha provveduto a nominare il **Responsabile della protezione dei dati** (di seguito anche Data Protection Officer e/o DPO), nella persona della dott.ssa Federica Banorri (recapito mail: *dpo@ausl.bologna.it*), in condivisione con Azienda USL di Bologna, Azienda Ospedaliera Universitaria - Policlinico S. Orsola Malpighi, Azienda USL di Imola e Montecatone Rehabilitation Insitute S.p.A.;

- i compiti del nominato DPO, considerata la sua competenza riferita all'area metropolitana, sono i seguenti:
  - informare e fornire consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei referenti aziendali individuati dalle singole Aziende/Enti dovrà altresì assicurare attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di incaricati al trattamento, eseguono operazioni di trattamento dati;
  - sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti aziendali individuati dalle singole Aziende/Enti;
  - fornire, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
  - cooperare con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;
  - supportare le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti al fine di uniformarne la predisposizione;
  - garantire il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
  - promuovere iniziative congiunte tra le Aziende/Enti affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;
  - favorire il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

Ritenuto infine

- di costituire un **Gruppo Aziendale Privacy** (di seguito anche solo Gruppo o GAP) di cui faranno parte i seguenti componenti:
  - Il Coordinatore Aziendale sulle tematiche privacy e coordinatore del Gruppo (già Referente Aziendale privacy);
  - Il Responsabile ICT anche quale responsabile della transizione digitale (nominato con delibera n. 79 del 28/3/2018) e in particolare relativamente alle prerogative di cui all'art. 17 comma 1 lett. C e G del CAD (indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica di dati, sistemi e alle infrastrutture);
  - Il Responsabile della SSD Accesso ai Servizi;
  nonché
  - per l'area Direzione Sanitaria/ Area Clinica:
    Un **componente individuato dalla Direzione Sanitaria,** anche proveniente dall'area Clinica;
  - per l'area Direzione Scientifica:
    Un **componente individuato dal Direttore Scientifico nell'ambito dei Laboratori di Ricerca**;
  - per l'Area dell'Assistenza:
    Un **componente individuato dalla direzione DATER;**

- che il GAP, in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali;

- che, pertanto, il GAP, coordinato dalla Dott.ssa Laura Mandrioli, ha i seguenti compiti specifici:
  - supportare i Referenti privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Istituto, a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana,
  - supportare i Referenti privacy nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza e, con la collaborazione del DPO, nella eventuale valutazione di impatto,
  - fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO,
  - coordinare le richieste di parere al DPO da parte dei singoli Referenti Privacy;

- **che con il presente provvedimento vengono superati** tutti i provvedimenti adottati precedentemente e cioè, oltre a quelli citati, anche le delibere n. 674 del 8 ottobre 2001 e n. 643 del 15 ottobre 2003 con cui erano stati nominati i cosiddetti " responsabili interni";

- che sul presente provvedimento è stato acquisito il parere favorevole del DPO;

Delibera

1. di individuare, quali " **Referenti privacy**" :
   - per l'area clinica e della ricerca nonché dell'assistenza:
   i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali,
   - per l'area amministrativa:
   i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;

2. di stabilire che la designazione e nomina dei Referenti privacy è conseguente all'assunzione/conferma degli incarichi di responsabilità come sopra specificati o all'assegnazione della funzione "ad interim" e di "facente funzioni" e che, pertanto, tale atto reca in sè la nomina a Referente privacy, con specificazione circa i compiti/istruzioni assegnati (allegato 1);

3. di riservarsi di designare quali Referenti privacy del trattamento dati altri soggetti – ulteriori e diversi da quelli indicati ai punti che precedono – anche non titolari di incarico di Struttura Complessa e/o di Struttura Semplice Dipartimentale (a titolo esemplificativo, Responsabile di struttura semplice, Responsabile Scientifico e/o Principal Investigator di progetti e/o sperimentazioni), i quali verranno individuati e nominati di volta in volta in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

4. di disporre che **chiunque compie operazioni di trattamento dei dati personali per conto dell' Istituto Ortopedico Rizzoli è individuato come "autorizzato" di trattamento al quale, come tale, sono consentite le operazioni di cui all'art. 4 del GDPR,** ciascuno nell'ambito delle funzioni e dei compiti specificatamente attribuiti;

5. di dare atto che tale individuazione si concretizza, di norma e senza l'adozione di ulteriori atti, all'atto dell'instaurazione di qualsivoglia rapporto - purché formalizzato - con l'Istituto Scientifico anche tramite il SUMAP;

6. di dare atto che per tutti i soggetti per i quali non è prevista la formalizzazione di un contratto/accordo individuale e, comunque, per i quali non è possibile la forma di designazione indicata al punto 5) che precede (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, specializzandi ecc) sarà l'ufficio amministrativo che cura gli adempimenti finalizzati all'istaurazione del rapporto con l'Istituto a provvedere, di volta in volta, all'autorizzazione al trattamento dei dati attraverso l'atto di designazione di cui all'allegato 3) della presente delibera;

7. di dare atto che l'autorizzazione di cui sopra deve intendersi circoscritta esclusivamente ai trattamenti che afferiscono all'unità operativa a cui è assegnato il dipendente / collaboratore, così come indicati, oltre che nel registro dei trattamenti, nell'atto aziendale e suo regolamento attuativo,

nelle assegnazioni funzionali del dipendente / collaboratore, nonché negli ulteriori atti ricognitivi dei processi e dei procedimenti e nelle eventuali ulteriori e specifiche indicazioni fornite dal Referente privacy al quale le singole unità operative fanno capo;

8. di precisare che gli autorizzati al trattamento operano secondo le direttive dei Referenti privacy ai quali afferiscono attenendosi alle istruzioni operative impartite dagli stessi nonché a quelle di carattere generale ricevute dal titolare e contenute nella presente delibera e nel suo allegato 2);

9. di dare mandato al SUMAP di trasmettere la presente deliberazione ai Dirigenti attualmente titolari degli incarichi dirigenziali di cui al punto 1 e di procedere analogamente per il futuro, a seguito di ogni conferimento/rinnovo o comunque di variazioni soggettive nella titolarità degli incarichi come sopra individuati, integrando altresì il contratto individuale con apposita clausola;

10. di comunicare l'autorizzazione al trattamento a tutti i dipendenti e alle categoria di personale indicate al precedente punto 5 mediante messa a disposizione della presente deliberazione nel profilo personale del portale del dipendente (GRU), oltre che tramite pubblicazione nell'intranet aziendale e nel sito internet dell'Istituto all'indirizzo *http://www.ior.it/il-rizzoli/atti-amministrativi-generali*, dando mandato al SUMAP, secondo le rispettive competenze, di procedere analogamente nei confronti del personale di nuova "assunzione" integrando i (futuri) contratti di lavoro con apposita clausola;

11. di costituire il **Gruppo Aziendale Privacy** composto dai seguenti membri:
    - Il **Coordinatore Aziendale sulle tematiche privacy e coordinatore del Gruppo** (già Referente Aziendale privacy);
    - il Responsabile ICT anche quale responsabile della transizione digitale (nominato con delibera n. 79 del 28/3/2018) e in particolare relativamente alle prerogative di cui all'art. 17 comma 1 lett. C e G del CAD (indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica di dati, sistemi e alle infrastrutture);
    - Il Responsabile della SSD Accesso ai Servizi;
    nonché
    - per l'area Direzione Sanitaria/ Area Clinica:
      Un **componente individuato dalla Direzione Sanitaria,** anche proveniente dall'area Clinica;
    - per l'area Direzione Scientifica:
      Un **componente individuato dal Direttore Scientifico nell'ambito dei Laboratori di Ricerca**;
    - per l'Area dell'Assistenza:
      Un **componente individuato dalla direzione DATER;**

12. di allegare **(allegato 1) l'elenco dei compiti/obblighi dei Referenti privacy**;

13. di allegare **(allegato 2) le istruzioni operative per il trattamento dei dati da parte degli autorizzati** e, in generale, quale contenuto minimo dei compiti/obblighi applicabile alla generalità dei trattamenti a prescindere dai profili di incarico;

14. di allegare **(allegato 3) il fac simile dell'atto di designazione del soggetto autorizzato al trattamento dei dati personali** da utilizzare per le nomine previste al punto 6 della presente delibera;

15. di precisare che dall'adozione del presente provvedimento non derivano oneri economici a carico del Bilancio dell'Istituto Ortopedico Rizzoli;

16. di diffondere il presente atto attraverso la rete intranet aziendale e il portale del personale GRU.

Responsabile del procedimento ai sensi della L. 241/90:
Marina Cioni

Allegato 1

COMPITI FUNZIONI E POTERI DEI REFERENTI PRIVACY

- Trattare i dati personali solo su istruzione del Titolare del trattamento e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs.101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali;
- Osservare e fare osservare:
    a) le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, anche per il tramite del Gruppo Aziendale Privacy e del Servizio ICT Aziendale (a titolo esemplificativo: regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli approvato con delibera n. 225/2017 e informativa per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*); linee guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario consultabili sulla rete intranet (all'indirizzo *http://intranet.internal.ior.it/documentazione/normativa/linee-guida-del-garante-protezione-dei-dati-personali-tema-di-fascicolo-san*), indicazioni sulla acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy assunte con il protocollo n. 6054 del 19.02.2015, linee guida in materia di Dossier Sanitario – provvedimento 04.06.2015 del Garante per la protezione dei dati personali pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n.164 del 17.07.2015 assunte con protocollo n. 26344 del 24.07.2015, procedura di *data breach* assunta con protocollo n. 5968 del 25.05.2018 e consultabile nella cartella di Fileserver2020 denominata *Condivisioni\RegolamentoUE.679.2016* ed ulteriori regolamenti e disposizioni consultabili sulla rete intranet aziendale)
    b) le istruzioni di carattere generale impartire dal Titolare a tutti i soggetti autorizzati al trattamento (di cui all'**allegato 2**);
    c) eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- Porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori ecc.) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del GDPR;
- Provvedere alla designazione dei soggetti autorizzati al trattamento dei dati personali per 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 volontari, lavoratori socialmente utili ecc.), attraverso la predisposizione dell'apposito modello di cui l'**allegato 3**;
- Vigilare sulla conformità dell'operato dei soggetti autorizzati ad essi afferenti 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 e 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 dall'Istituto ed assicurare la partecipazione dei propri autorizzati;
- Fornire le informazioni richieste dal Gruppo Aziendale Privacy e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
- Comunicare al Gruppo Aziendale Privacy i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;
- Collaborare con il Gruppo Aziendale Privacy e il Servizio ICT Aziendale per la predisposizione del documento della valutazione di impatto sulla protezione dei dati qualora ne ricorrano i presupposti in base all'art. 35 del GDPR;
- 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/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale Privacy, attraverso l'invio della predetta documentazione agli *Affari Legali e Generali* tramite BABEL, con nota a protocollo che indichi gli estremi cronologici della nomina stessa (decorrenza e periodo di validità), anche ai fini dell'aggiornamento del registro dei trattamenti;
- Comunicare tempestivamente al Gruppo Aziendale Privacy i potenziali casi di *data breach* all'interno della propria struttura e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito.

Allegato 2

ISTRUZIONI di CARATTERE GENERALE impartite dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente aziendale privacy garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;

- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Istituto che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento.
- email e uso della rete internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*);
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii.
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerà porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli;*
2. *Informativa per gli utenti sull'utilizzo dei servizi informatici IOR;*
3. *Linee guida in tema di fascicolo sanitario elettronico (FSE) e di Dossier Sanitario;*
4. *Indicazioni sull'acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy;*
5. *Procedura di data breach;*

a cui si rinvia, reperibili sempre sulle pagine intranet dedicate.

Allegato 3

ATTO DI DESIGNAZIONE
DEL SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, così come modificato dal D.Lgs. n. 101/2018

Il sottoscritto_____

(indicare il nome del Referente Privacy di afferenza)

in qualità di Referente Privacy dell' UO/UOC/……_____

DESIGNA

(indicare NOME e COGNOME)

in qualità di ……

(indicare funzione, ruolo,…)

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI relativi

AMBITO DEL TRATTAMENTO (sede/i di assegnazione) DESCRIZIONE DEL TRATTAMENTO ARCHIVI BANCHE DATI

A seguito della suddetta designazione Lei è autorizzato a svolgere operazioni di trattamento, per il proprio ambito di competenza, secondo i principi generali di trattamento, le prescrizioni, le istruzioni operative generali impartite dal Titolare e le ulteriori eventuali istruzioni specifiche dal sottoscritto impartite.

Principi di carattere generale:

- ✓ trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
- ✓ trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
- ✓ verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- ✓ conservarli nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare (**allegate alla presente**) e sempre consultabili nella sezione Privacy della rete intranet aziendale, dalle prescrizioni e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto in qualità di Referente Privacy di Sua afferenza.

Prescrizioni:

a. Rispettare l'obbligo di riservatezza e segretezza, mantenendo la segretezza delle informazioni di cui venga a conoscenza mediante accesso ai sistemi informativi aziendali, secondo il profilo di autorizzazione assegnato alle proprie credenziali di autenticazione (user e password), corrispondente alla classe di autorizzato di appartenenza;
b. trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
c. trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
d. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;

e. conservare i dati nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione Privacy della rete intranet aziendale, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
f. utilizzare le informazioni e i dati, con cui si entra in contatto per ragioni di lavoro, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza, secondo quanto definito dalle regole aziendali, per tutta la durata dell'incarico ed anche successivamente al termine di esso, astenendosi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
g. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su tutti dispositivi in dotazione ad altri operatori e/o di lasciare, in caso di allontanamento anche temporaneo dalla postazione di lavoro il sistema operativo avviato con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
h. conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate mettendo in atto tutte le misure di sicurezza previste dal Regolamento Europeo in materia di protezione dei dati n. 2016/679, dalla normativa nazionale, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione sopra indicata, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
i. astenersi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
j. segnalare al sottoscritto eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
k. informare senza ingiustificato ritardo il soggetto delegato al trattamento di qualunque fatto o circostanza, anche accidentale, che abbia causato perdita, distruzione dei dati, accesso non consentito o comunque non conforme ai principi sopradetti.

La S.V. prende atto di quanto previsto nella presente designazione ed assume la qualifica di soggetto autorizzato al trattamento dei dati personali impegnandosi a:

- ✓ rispettare i principi e le prescrizioni sopraripportate, le istruzioni di carattere generale impartite dal Titolare, allegate al presente atto di designazione e disponibili nella sezione Privacy della rete intranet aziendale, e le eventuali istruzioni che Le verranno eventualmente impartite per l'ambito di competenza e del profilo professionale di appartenenza.

E' fatto obbligo a ciascun professionista autorizzato al trattamento consultare gli aggiornamenti della documentazione aziendale in materia sul sito intranet aziendale nella sezione sopra citata.

Ciò premesso, il presente atto costituisce pertanto conferimento formale dell'autorizzazione al trattamento dei dati connessi allo svolgimento dell'attività lavorativa connessa all'ambito del trattamento sopra individuato, secondo le istruzioni allegate e secondo le prescrizioni sopra riportate. Tale DESIGNAZIONE:

- ha validità per l'intera durata del rapporto di lavoro con l'Istituto;
- viene a cessare al modificarsi del rapporto di lavoro o con esplicita revoca dello stesso.

DICHIARAZIONE DI RICEVIMENTO DELL'ATTO DI DESIGNAZIONE E DI IMPEGNO ALL'OSSERVANZA DELLE ISTRUZIONI ALLEGATE

Il sottoscritto _____

(indicare NOME e COGNOME)

DICHIARA

1. di aver ricevuto la designazione ad autorizzato al trattamento;
2. di aver attentamente letto e compreso il contenuto del presente atto e del suo allegato, e di impegnarsi ad osservare tutte e specifiche istruzioni impartite;
3. di obbligarsi ad osservare le ulteriori direttive/regolamentazioni aziendali reperibili alla sezione intranet dedicata.
4. di dare atto che l'obbligo di riservatezza correlato all'incarico va osservato anche successivamente alla conclusione dello stesso

Data_____

Firma_____

Allegato

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*);
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo

quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..

- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda/Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli;*
2. *Informativa per gli utenti sull'utilizzo dei servizi informatici IOR;*
3. *Linee guida in tema di fascicolo sanitario elettronico (FSE) e di Dossier Sanitario;*
4. *Indicazioni sull'acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy;*
5. *Procedura di data breach;*

a cui si rinvia, reperibili sempre sulle pagine intranet dedicate.