S O M M A R I O

STATO	DATA	FIRMA
Verificato	20/03/2024	Dott.ssa Maria Bonanno
Approvato	20/03/2024	Dott.ssa Federica Banorri
Approvato	20/03/2024	Dott.ssa Chiara Gibertoni
Applicato:	22/03/2024	

1. OGGETTO E SCOPO

Il presente documento dà attuazione alle disposizioni del Regolamento Europeo sulla protezione dei dati (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, c.d. GDPR) e del D.Lgs 30/06/2003, n. 196 e s.m.i., ed individua le misure organizzative atte a garantire che, nell'ambito delle diverse articolazioni aziendali, ogni trattamento di dati personali si svolga nel rispetto dei principi dei sopraccitati disposti.
Tale documento rappresenta il codice di comportamento generale che l'*IRCCS Azienda Ospedaliero-Universitaria di Bologna IRCCS Policlinico di S. Orsola* (d'ora in poi denominato *IRCCS AOU BO*) ha adottato in riferimento al trattamento e alla protezione dei dati personali, con l'obiettivo di assicurare che l'attività di tutti gli operatori sia svolta attraverso una corretta e scrupolosa applicazione delle norme poste a protezione dei dati personali.

2. CAMPO DI APPLICAZIONE

La presente istruzione operativa deve essere obbligatoriamente applicata da tutti i soggetti che, a qualunque titolo e livello, trattano dati personali per conto dell'IRCCS AOU BO. Il mancato rispetto delle indicazioni ivi presenti può determinare misure sanzionatorie di varia natura nei confronti di chi utilizza i dati personali in maniera non conforme alla normativa in materia di protezione dei dati personali.

3. RESPONSABILITA' E GRUPPO DI REDAZIONE

Il presente documento è stato riesaminato e revisionato dalla *Funzione Privacy*, condiviso con il Gruppo Aziendale Privacy (GAP), e *validato dal Data Protection Officer (DPO) dell'Azienda, al fine di garantire la coerenza con quanto definito in ambito AVEC*.
Gli aggiornamenti e le revisioni periodiche sono di responsabilità del Responsabile della Funzione Privacy, previo parere del DPO.

4. DOCUMENTI DI RIFERIMENTO

- L. n. 241 del 07/08/1990, "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e s.m.i.;
- D.Lgs n. 196 del 30/06/2003 "Codice in materia di protezione dei dati personali" e s.m.i. (*c.d. Codice Privacy*);
- D.Lgs n. 33 del 14/03/2013 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazione da parte delle pubbliche amministrazioni" *e s.m.i.;*
- D.P.C.M. del 08/08/2013 "Modalita' di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalita' digitali, nonche' di effettuazione del pagamento online delle prestazioni erogate, ai sensi dell'articolo 6, comma 2, lettera d), numeri 1) e 2) del decreto-legge 13 maggio 2011, n.70, convertito, con modificazioni, dalla legge 12 luglio 2011, n. 106, recante «Semestre europeo - prime disposizioni urgenti per l'economia»";
- Regolamento Regionale n. 1 del 30/05/2014, n. 1 "Regolamento per il trattamento dei dati sensibili e giudiziari di titolarità della Giunta Regionale e delle Agenzie, Istituti ed Enti che fanno riferimento all'Amministrazione Regionale";
- Regolamento (UE) 2016/679 del 27/04/2016 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);
- D.Lgs. n. 97 del 25/05/2016 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012 n. 190 e del Dlgs. 14 marzo 2013 n. 33, ai sensi dell'art. 7 della legge 7 agosto 2015 n. 124, in materia di riorganizzazione delle amministrazioni pubbliche" *e ss.mm.ii.*;

- Garante Privacy, Provvedimento del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuali con strumenti elettronici relativamente alle attribuzione delle funzioni di amministratori di sistema";
- *Garante Privacy, Delibera n. 25 del 16/07/2009 "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario";*
- Garante Privacy, *Provvedimento n. 331* del 04/06/2015 "Linee guida in materia di Dossier sanitario";
- Garante Privacy, Provvedimento n. 146 del 05/06/2019 "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.Lgs. 10/08/2018, n. 101*";
- *Garante Privacy, Provvedimento n. 256 dell'08/06/2023 "Parere sullo schema di decreto del Ministero della salute, da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sul Fascicolo Sanitario Elettronico (FSE)";*
- *Delibera n. 516 del 25/11/2015 "Approvazione del regolamento per la disciplina delle modalita' di esercizio e casi di esclusione del diritto ai accesso ai documenti amministrativi";*
- *Delibera Aziendale n. 265 del 19/12/2018 "Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali: ridefinizione dei profili di responsabilita' in tema di protezione dei dati personali e nuove modalita' di designazione dei soggetti autorizzati ad eseguire operazioni di trattamento dei dati personali (organigramma delle responsabilitá privacy aziendali)";*
- *Delibera Aziendale n. 167 del 09/06/2021 "Approvazione dell'accordo per l'istituzione della funzione di "Responsabile della protezione dei dati - Data Protection Officer" in ambito metropolitano - Provvedimenti conseguenti";*
- *Delibera Aziendale n. 194 del 30/06/2021 "Conferimento dell'incarico di responsabile della struttura semplice "Data Protection Officer Interaziendale";*
- *Delibera Aziendale n. 209 del 30/06/2021 "Riassetto organizzativo delle funzioni trasversali - provvedimenti riguardanti la struttura semplice "Attivita' Generali ed Istituzionali";*
- *Delibera Aziendale n. 310 del 20/10/2022 "Provvedimenti in merito alla definizione dei rapporti tra DPO e funzioni privacy/coordinatore/i del Gruppo Aziendale Privacy (GAP)";*
- *Delibera Aziendale n. 343 del 25/11/2022 "Nomina componenti Gruppo Aziendale Privacy (GAP)";*
- *Delibera Aziendale n. 207 del 12/07/2023 "Sistema deleghe aziendali relativamente alla nomina di responsabile del trattamento dei dati in caso di aggiudicazione/sottoscrizione di contratti/convenzioni: aggiornamento";*
- *Delibera Aziendale n. 27 del 24/01/2024 "Approvazione del Codice di Comportamento aziendale";*
- PA05 "Procedura aziendale di controllo dei documenti del sistema di gestione della qualità";
- PA36 "Procedura aziendale per la conservazione e rilascio della cartella clinica e di altra documentazione sanitaria";
- PA40 "Procedura aziendale per l'archiviazione, lo scarto e lo smaltimento della documentazione aziendale";
- PA46 "Procedura aziendale per la compilazione della cartella clinica";
- *PA104 "Procedura aziendale per la gestione delle sperimentazioni cliniche";*
- *PA122 "Procedura aziendale per l'esercizio dei diritti dell'interessato";*
- IOA44 "Istruzione Operativa Aziendale per l'utilizzo delle risorse informatiche, con particolare riferimento alla sicurezza e riservatezza";
- IOA87 "Istruzione Operativa Aziendale per il trattamento dei dati personali nell'ambito degli studi clinici";
- *IOA91 "Istruzione Operativa Aziendale gestione della videosorveglianza";*
- IOA95 "Istruzione Operativa Aziendale per la richiesta di estrazione di dati aziendali";
- IOA98 "Istruzione Operativa Aziendale per la gestione di un data breach";
- IOA99 "Istruzione Operativa Aziendale per l'utilizzo della posta elettronica e di internet";

– IOI83 "Istruzione Operativa Interservizi per la gestione della figura dell'amministratore di sistema"

5. DEFINIZIONI E ABBREVIAZIONI

Accountability*: il Regolamento Europeo pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Secondo tale principio viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento (es. criterio del data protection by default and by design).*

Amministratore di sistema: figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

CAD: *il Codice dell'Amministrazione Digitale (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese. Istituito con il decreto legislativo 7 marzo 2005, n. 82, è stato successivamente modificato e integrato prima con il decreto legislativo 22 agosto 2016 n. 179 e poi con il decreto legislativo 13 dicembre 2017 n. 217 per promuovere e rendere effettivi i diritti di cittadinanza digitale.*

Campione biologico: ogni campione di materiale biologico da cui possono essere estratti dati genetici caratteristici di un individuo.

Case report: *nell'ambito delle attività di pubblicazione scientifica, vengono generalmente redatti i c.d. case report (caso clinico e/o serie limitata di casi) trattasi della descrizione dei sintomi e dei segni di una malattia, degli effetti di trattamenti terapeutici, ecc. solitamente riscontrati in un singolo individuo e/o in una limitata serie di pazienti. Data la sua natura descrittiva il case report non rappresenta alcuna forma di sperimentazione clinica.*

Codice Privacy: è il D.Lgs. 30 giugno 2003 n. 196 e s.m.i. "Codice in materia di protezione dei dati personali".
Il documento è stato integrato con le modifiche introdotte dal Decreto Legislativo 10.08.2018 n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, 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)". Rappresenta il principale riferimento normativo nazionale in tema di privacy volto a garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Comunicazione: il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio *dell'Unione Europea*, dal responsabile o *dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile*, in qualunque forma, anche mediante la loro messa a disposizione, consultazione *o mediante interconnessione*.

Consenso al trattamento dei dati: qualsiasi manifestazione di volontà, libera, specifica ed informata con la quale la persona interessata o chi la rappresenta, accetta che i dati personali che la riguardano siano oggetto di un trattamento. Non va confuso con il consenso al trattamento sanitario regolamentato dai documenti aziendali PA24*A, PA24B e PA24C*.

Data protection by default and by design: *è uno dei criteri, definiti dal Regolamento Europeo, che il Titolare deve applicare nell'ambito dell'accountability. Esso esprime la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso)*

e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*il c.d. soggetto* interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati particolari (ex dati sensibili)*: dati rientranti in particolari categorie (costituiscono un sottoinsieme della più ampia categoria dei dati personali) che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale, dati genetici e dati biometrici*;

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

Dato anonimo: dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Dato pseudoanonimizzato: *dato che è stato sottoposto a trattamento di pseudonimizzazione.*

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Data Protection Officer (DPO): figura prevista dal Regolamento Europeo, quale supporto del Titolare con la finalità di facilitare l'attuazione della normativa (art. 37 e 38 del GDPR).

DPIA: *Data Protection Impact Assessment, ovvvero Valutazione d'impatto sulla protezione dei dati. Trattasi di una particolare procedura, prevista dall'articolo 35 del GDPR, finalizzata a individuare, valutare e gestire i rischi legati a una specifica tipologia di trattamento. La DPIA consente al titolare del trattamento di analizzare in via preliminare l'impatto che possono avere sui diritti e le libertà degli interessati i nuovi trattamenti (legati ad esempio all'applicazione di una nuova tecnologia o di una nuova strategia aziendale), oppure modifiche sostanziali a un trattamento già in essere.*

EDPB *(European Data Protection Board): è il Comitato europeo per la protezione dei dati, ovvero un organismo indipendente con sede a Bruxell che assicura che il GDPR e e la direttiva sull'applicazione della legge sulla protezione dei dati siano applicati in modo coerente in tutti i paesi che ne sono coperti e che promuove la cooperazione fra le autorità nazionali preposte alla protezione dei dati.*

Funzione Privacy: *presidio aziendale* individuato dal Titolare a supporto dello stesso che, interagendo con tutte le strutture/articolazioni organizzative trasversali/di supporto, con i Dipartimenti ad Attività Integrata e con le strutture ad essi afferenti, ha la finalità di garantire e coordinare, *in qualità di principale interlocutore del Data Protection Officer (DPO),* le attività aziendali correlate alla normativa in materia di protezione dei dati personali.

GDPR: *General Data Protection Regulation ovvero il Regolamento Europeo Generale per la protezione dei dati personali.*

Gruppo Aziendale Privacy (GAP): gruppo di professionisti coordinato dal Responsabile *della Funzione* Privacy Aziendale, che 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.

Garante per la protezione dei dati personali: Autorità indipendente, con sede a Roma, istituita dalla Legge sulla privacy per assicurare la tutela dei diritti e delle libertà fondamentali ed il rispetto della dignità nel trattamento dei dati personali. É un organo collegiale, composto da quattro membri eletti dal Parlamento, i quali rimangono in carica per un mandato di sette anni non rinnovabile (www.garanteprivacy.it).

Informativa: rappresenta, assieme al consenso quando richiesto, uno dei requisiti fondamentali di legittimità del trattamento dei dati personali. E' lo strumento che rende esplicita e trasparente la gestione delle informazioni di carattere personale e/o sensibile degli interessati. Attraverso l'informativa l'interessato acquisce precise informazioni circa l'utilizzo dei suoi dati personali a garanzia del controllo delle proprie informazioni e dei relativi trattamenti.

Interessato: persona fisica cui si riferiscono i dati personali.

IRCCS AOU BO: Istituto di Ricovero e cura a carattere Scientifico - Azienda Ospedaliero Universitaria di Bologna

Misure adeguate: il complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di sicurezza in relazione ai rischi previsti nell'articolo 32 *del GDPR*.

***Profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.*

***Pseudonimizzazione**: è una tecnica che consiste "nel trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4 punto 5 del GDPR).*

Referente Aziendale Privacy: soggetti qualificati a cui il Titolare assegna compiti e funzioni connessi al trattamento di dati personali. *All'interno dell'IRCCS, i Referenti Privacy Aziendali sono i Direttori di Struttura Complessa, i Responsabili di Struttura Semplice Dipartimentale e i Responsabili di Programmi o altre strutture/articolazioni purchè con gestione di risorse*.

***Regolamento Europeo Generale per la protezione dei dati personali:** ovvero il Regolamento UE 2016/679, noto come **GDPR** (General Data Protection Regulation) o **RGPD** è la principale normativa europea in materia di protezione dei dati personali. Il GDPR è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018.*

***Registro delle attività di trattamento:** è un documento contenente le principali informazioni (specificatamente individuate dall'art. 30 del GDPR) relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento. Costituisce uno dei principali elementi di accountability del Titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. All'interno dell'IRCCS il Registro delle attività di trattamento viene gestito dalla Funzione Privacy e dall'ICT tramite l'applicativo informatico Privacy Manager.*

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.

***Sicurezza del trattamento**: tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza adeguato al rischio. Ad esempio: la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

Soggetto autorizzato: la persona fisica autorizzata dal Titolare o dal Referente Privacy a compiere operazioni di trattamento;

Soggetto incapace di agire: la capacità di agire, ai sensi dell'art. 2 del Codice Civile, consiste nell'attitudine di un soggetto di esprimere validamente la propria volontà ai fini giuridici. Soggetti incapaci di agire sono: i minorenni, gli interdetti (legali o giudiziali) e gli inabilitati.

Soggetto incapace di intendere o di volere: l'incapacità di intendere o di volere, cd. incapacità naturale, è uno status momentaneo, contingente e non abituale di incapacità che si determina per una qualsiasi causa che incide sulla sfera psichica e/o fisica di un soggetto. La stessa rileva solo nell'ipotesi in cui il soggetto agente abbia capacità legale di agire, ma sia privo, in un determinato momento, della capacità di intendere o di volere. In particolare, l'incapacità di intendere indica l'incapacità del soggetto a rendersi conto del significato delle proprie azioni; l'incapacità di volere, invece, indica l'incapacità di autodeterminarsi liberamente. In altri termini, si fa riferimento alla mancanza di quel minimo di attitudine psichica a rendersi conto delle conseguenze della propria condotta.
s.m.i.: successive modificazioni e integrazioni, formula che segue l'indicazione di un testo normativo, al fine di rappresentare che si ricomprendono anche gli aggiornamenti degli stesso.
Titolare del trattamento dei dati: *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.*
Trattamento dei dati: *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.*
Violazione dei dati personali (data breach): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

6. CONTENUTO

6.1 ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI[1]

Sulla base del Regolamento (UE) 2016/679, in vigore dal 25/05/2018, all'interno dell'*IRCCS AOU BO*, sono stati ridefiniti i profili di responsabilità in tema di protezione dei dati personali e le modalità di designazione dei soggetti autorizzati ad eseguire operazioni di trattamento.
La ridefinizione è stata formalizzata con l'adozione della Delibera n. 265 del 19/12/2018 che delinea l'ORGANIGRAMMA DELLE RESPONSABILITÁ PRIVACY AZIENDALI.
Si riportano di seguito i soggetti dell'organigramma privacy:

- ⇨ TITOLARE DEL TRATTAMENTO = l'*IRCCS AOU BO* nella persona del suo legale rappresentante pro tempore.

- ⇨ REFERENTI PRIVACY AZIENDALI = Direttori di Struttura Complessa, Responsabili di Struttura Semplice Dipartimentale, Responsabili di Programmi o altre strutture/articolazioni purchè con gestione di risorse, individuati dal Titolare quali soggetti che svolgono compiti e funzioni connessi al trattamento di dati personali.
  I Referenti Privacy sono stati nominati con Delibera n. 265 del 19/12/2018 del Direttore Generale.
  Relativamente all'assunzione/conferma degli incarichi di responsabilità o all'assegnazione della funzione "ad interim" o di "facente funzioni", come sopra specificati, successivi alla Delibera n. 265 del 19/12/2018, la designazione a Referenti Privacy viene formalizzata, a cura del *Servizio Unificato Metropolitano Amministrazione Giuridica del Personale (SUMAGP*), contestualmente alla sottoscrizione del contratto di incarico con specificazione circa i compiti/istruzioni assegnati.
  Il Titolare ha predisposto i compiti funzioni e poteri dei referenti privacy in specifiche istruzioni (T03/IOS01 "Compiti, funzioni e poteri dei referenti privacy").

[1] *Tutti i documenti e modelli/fac-simile citati nel presente paragrafo sono reperibili all'interno dell'area intranet privacy attraverso il seguente percorso: La privacy in Azienda>Documentazione di riferimento>Organigramma delle responsabilità privacy aziendali.*

⇨ RESPONSABILI DEL TRATTAMENTO = soggetti esterni all'*IRCCS AOU BO* che effettuano trattamenti di dati in outsourcing, nell'ambito di attività/servizi/funzioni correlate alle finalità istituzionali dell'*IRCCS AOU BO* (dietro stipula di convenzione, contratto, *accordo*, ecc.)
Il Titolare ha delegato ai Referenti Privacy Aziendali la nomina dei Responsabili del trattamento; tale delega è contenuta nella ***Delibera Aziendale n. 207 del 12/07/2023****.*
Tale nomina si formalizza tramite sottoscrizione del rapporto contrattuale o convenzionale in essere che deve a tal fine contenere uno specifico ***articolo privacy*** *ed i correlati allegati (****ALLEGATO 1****: Descrizione delle attività di trattamento e* ***ALLEGATO 2:*** *Istruzioni per il Responsabile del trattamento dei dati personali)*[2]*.*
Al fine di garantire, ai sensi dell'art. 30 del GDPR, la corretta implementazione del Registro delle attività di trattamento in relazione alla nomina di eventuali Responsabili del trattamento, è stata sviluppata, all'interno della piattaforma di gestione dei flussi documentali BABEL, una funzione che consente ai Referenti Privacy Aziendali di trasferire tempestivamente alla Funzione Privacy le informazioni indispensabili per l'implementazione del Registro delle attività di trattamento (Privacy Manager).
Le specifiche tecniche per l'utilizzo di tale funzionalità sono state diffuse tramite nota PG0003413 del 30/01/2023.

⇨ SOGGETTI AUTORIZZATI AL TRATTAMENTO
Attraverso la pubblicazione, nell'area privacy dedicata, della Delibera n. 265 del 19/12/2018, il Direttore Generale notifica l'autorizzazione al trattamento dei dati a tutte le **persone operanti stabilmente** all'interno dell'Azienda, ovvero:

- dipendenti/collaboratori/titolari di rapporto di lavoro autonomo
- soggetti operanti stabilmente ad altro titolo, compresi i medici in formazione specialistica, gli studenti di medicina e chirurgia nel periodo di tirocinio obbligatorio, i frequentatori volontari, i dottorandi e assegnisti di ricerca autorizzati all'attività di assistenza

A tal proposito si specifica che l'autorizzazione al trattamento dei dati personali per le persone, rientranti nelle categorie di cui sopra, che prenderanno servizio in data successiva alla adozione della Delibera opererà contestualmente alla sottoscrizione del relativo contratto di lavoro o alla accettazione del relativo incarico, atti che saranno integrati dal *SUMAGP* con specifica clausola.

Tutte le **persone operanti non stabilmente** all'interno dell'Azienda (ovvero, a titolo di esempio non esaustivo: lavoratori socialmente utili, volontari, tirocinanti diversi rispetto a quelli sopra indicati) dovranno invece essere nominate soggetti autorizzati al trattamento ad personam dal Referente Privacy *Aziendale* (ovvero dal responsabile della struttura a cui afferiscono) utilizzando *lo specifico report* R02/IOS01 *"ATTO DI DESIGNAZIONE DEL SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI"*che sarà da conservare agli atti del Referente Privacy *Aziendale*.

Il Titolare ha predisposto delle **istruzioni di carattere generale** per tutti **i soggetti autorizzati al trattamento** *attraverso una specifca* tabella, *ovvero la* T04/IOS01 "ISTRUZIONI DI CARATTERE GENERALE IMPARTIRE DAL TITOLARE A TUTTI I SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI".

⇨ *FUNZIONE* PRIVACY AZIENDALE = *presidio aziendale, collocato all'interno dell'Ufficio Privacy afferente alla SS Attività Istituzionali, Comunicazione e URP* che, interagendo con tutte le strutture/articolazioni organizzative trasversali/di supporto, con i Dipartimenti ad Attività Integrata e con le strutture ad essi afferenti, ha la finalità di garantire e coordinare, *in qualità di principale*

[2] Per il recupero del modello articolo e relativi allegati vedasi nota 1.

interlocutore del Data Protection Officer (DPO), le attività aziendali correlate alla normativa in materia di protezione dei dati personali.
In particolare, all'interno dell'IRCCS, la Funzione Privacy svolge i seguenti compiti:

- *fornisce supporto all'interno dell'IRCCS in relazione ai pareri rilasciati dal DPO e in relazione all'applicazione delle policy aziendali e ne dà comunicazione al DPO;*
- *fornisce supporto giuridico nella predisposizione degli atti di attribuzione delle responsabilità in materia di trattamento dei dati personali (ad es. convenzioni, accordi, contratti) secondo le indicazioni fornite dal DPO, coinvolgendolo qualora il responsabile del trattamento avanzi richieste di modifiche sostanziali dei fac-simili predisposti dal DPO;*
- *individua e raccoglie le esigenze e i bisogni formativi in ambito aziendale e in collaborazione con il DPO progetta e pianifica le iniziative interne su specifiche tematiche su cui eseguire la formazione;*
- *fornisce supporto giuridico ai gruppi di lavoro delle singole Aziende o ai servizi aziendali competenti in relazione al trattamento oggetto di valutazione nella redazione della DPIA, in collaborazione con il Servizio ICT aziendale e le altre UUOO coinvolte;*
- *fornisce supporto ai servizi aziendali coinvolti nell'attività di audit espletata dall'UO interaziendale DPO; riceve dal DPO gli esiti della verifica e collabora per la messa in atto delle eventuali azioni correttive o comunque conseguenti;*
- *predispone e cura l'istruttoria della violazione secondo quanto definito negli specifici atti aziendali in collaborazione con i servizi coinvolti nell'incidente. Invia i risultati dell'istruttoria al DPO al fine di valutare la gravità e l'eventuale comunicazione all'Autorità Garante;*
- *collabora con il DPO nella fase di acquisizione degli elementi utili alla eventuale consultazione/richiesta di parere all'Autorità Garante;*
- *fornisce alle varie UUOO di riferimento (es. Ingegneria clinica, ICT, Controllo di gestione, URP, ALP, Dipartimento cure primarie, dipartimento amministrativo territoriale, DSP, Ricerca, ecc.) il supporto giuridico all'attività di popolamento, modifica, integrazione del registro delle attività di trattamento cooperando con il Servizio ICT. Ne condivide la tenuta con il Servizio ICT e con il DPO;*
- *predispone e cura la redazione dei documenti privacy di valenza aziendale (ad es. informativa per progetto realizzato all'interno di una UO). Recepisce e aggiorna le procedure, i fac-simili e i documenti privacy di valenza "trasversale" secondo le indicazioni fornite dal DPO;*
- *gestisce reclami e segnalazioni ordinarie in materia privacy, dalla ricezione al riscontro all'interessato (es. reclami in relazione alla mancata adozione di misure di sicurezza, ecc.) e ne dà comunicazione al DPO;*
- *supporta i professionisti aziendali in merito agli adempimenti da svolgere in ambito di studi e sperimentazioni nella presentazione di un progetto (ad es. supporto alla compilazione dei modelli e fac-simili, informativa, consenso, DPIA, modulistica varia predisposta dal DPO), in collaborazione con gli uffici ricerca aziendali.*

⇨ GRUPPO AZIENDALE PRIVACY (GAP): gruppo di professionsiti aziendali, *istituito con Delibera* (*l'attuale composizione è definita in particolare dalla Delibera n. 343 del 25/11/2022*), coordinato dal Responsabile *della Funzione* Privacy Aziendale, che 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.
In particolare, all'interno dell'IRCCS AOU BO, il GAP svolge i seguenti compiti:

- *sovraintendere all'applicazione delle procedure e degli atti inerenti il trattamento di dati personali, adottati all'interno dell'Azienda;*
- *rilevare eventuali problematiche privacy e proporre soluzioni tempestive;*
- *individuare e raccogliere le esigenze e i bisogni formativi in ambito aziendale, collaborando, congiuntamente al DPO, nella predisposizione della formazione interna;*

- *fornire supporto giuridico, tecnico e organizzativo ai vari servizi aziendali gestori dei dati;*
- *supportare l'Ufficio Privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo, nell'aggiornamento del Registro delle attività di trattamento di dati personali effettuati all'interno dell'Azienda, nonché nell'eventuale predisposizione della valutazione di impatto ai sensi dell'art. 35 del GDPR;*
- *collaborare con l'Ufficio Privacy nella fase di acquisizione degli elementi utili alla eventuale consultazione/richiesta di parere da parte del DPO all'Autorità Garante*

⇨ DATA PROTECTION OFFICER (DPO)

Il GDPR prevede l'obbligo per il Titolare o il Responsabile del trattamento di designare il DPO «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art. 37, paragrafo 1, lett a). A partire dall'anno 2018, in considerazione delle sinergie già esistenti in materia di privacy e al fine di agevolare omogeneità di azione da parte di Aziende dello stesso settore di attività e territorialmente contigue, i Direttori Generali dell'Azienda Ospedaliero-Universitaria di Bologna, dell'Azienda USL di Bologna, dell'Istituto Ortopedico Rizzoli, dell'Azienda USL di Imola e di Montecatone Rehabilitation Institute SPA hanno concordato di nominare un unico DPO. Successivamente, a giugno 2021, è stata istituita la struttura semplice Data Protection Officer Interaziendale collocata in staff al Direttore Generale dell'IRCCS Azienda ospedaliero-universitaria di Bologna (azienda capofila).
In particolare, all'interno dell'IRCCS AOU BO, il DPO svolge i seguenti compiti:

- *informa e fornisce consulenza ai Titolari del trattamento, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni normative nazionali, dell'Unione o degli Stati membri relative alla protezione dei dati;*
- *esprime pareri, anche su richiesta, su atti, documenti, tematiche di valenza trasversale, aziendale o innovativa e ne dà comunicazione alla Funzione Privacy di riferimento, o a tutte qualora la tematica sia di interesse comune/generale;*
- *sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali compresa l'attribuzione delle responsabilità in materia di trattamento dei dati personali, in particolare:*
  - *definisce e cura la predisposizione degli atti di attribuzione delle responsabilità per conto dei Titolari (organigramma privacy)*
  - *fornisce il necessario supporto alle funzioni privacy nell'individuazione dei ruoli privacy e delle responsabilità negli atti di nomina del Responsabile del trattamento ex art. 28 GDPR, nonché supporto nella predisposizione degli atti/convenzioni a carattere interaziendale*
- *promuove iniziative formative interaziendali, pianifica ed esegue la formazione in materia privacy, valutando l'eventuale coinvolgimento diretto delle funzioni privacy aziendali;*
- *fornisce pareri in merito alla necessità di redazione della valutazione d'impatto (DPIA) in relazione a un determinato trattamento, mette a disposizione il modello condiviso valida il documento finale (DPIA) prima dell'autorizzazione del titolare;*
- *definisce un piano annuale di audit interni e svolge attività di audit sul campo, al fine di verificare che la normativa vigente e le policy aziendali siano correttamente attuate e applicate;*
- *gestisce gli incidenti di sicurezza (data breach) nelle modalità previste dagli specifici atti aziendali, ne cura, su delega del titolare, l'eventuale notifica secondo le formalità e modalità tecniche impartite dall'Autorità Garante;*
- *coopera con l'Autorità Garante, fungendo da punto di contatto con la stessa su questioni connesse al trattamento (tra cui consultazione preventiva, audizioni, ecc.).Effettua eventuali consultazioni anche relative a pareri richiesti dal Titolare e/o dalla Funzione Privacy e in generale ne cura i rapporti. Informa il Titolare e la Funzione Privacy degli esiti dell'eventuale*

consultazione, richiesta parere, ecc. coinvolgendo, se ritenuto necessario, la Funzione Privacy già nella fase di contatto con Autorità Garante al fine di acquisire tutti gli elementi utili;

- *formula gli indirizzi per l'aggiornamento periodico o sulla base di provvedimenti normativi, del registro delle attività di trattamento dei titolari e del responsabile al fine di uniformarne la predisposizione in stretta collaborazione con le strutture informatiche (ICT) e le Funzioni Privacy aziendali. Coordina il gruppo di lavoro Privacy Manager relativamente alle attività di popolamento ed aggiornamento del registro delle attività di trattamento dei titolari e del responsabile. Funge da punto di riferimento con il fornitore in merito ad eventuali modifiche o integrazioni dei moduli dell'applicativo;*
- *predispone e cura la redazione di documenti privacy di valenza "trasversale" quali informative, fac-simili di accordi di contitolarità, procedure, ecc.;*
- *gestisce le richieste di esercizio dei diritti degli interessati (compresi dipendenti) e le richieste relative ad aspetti privacy su FSE in collaborazione con gli ICT e la RER e ne dà comunicazione alle Funzioni Privacy;*
- *formula pareri, in merito agli aspetti di protezione del dato personale nell'ambito di studi e sperimentazioni, alle richieste avanzate dal Titolare, dalla Segreteria del Comitato Etico AVEC e dalle Funzioni Privacy e gestisce l'eventuale attività di monitoraggio delle sperimentazioni cliniche come richiesto dalla Agenzia Italiana del farmaco (AIFA).*

⇨ AMMINISTRATORE DI SISTEMA = personale interno o esterno (in ipotesi di affidamento in outsourcing dei servizi di amministratore di sistema) all'*IRCCS AOU BO*, in possesso di competenze altamente specializzate dal punto di vista informatico, designato nominativamente dal Titolare del trattamento d'intesa con i Responsabili dei Servizi Interessati.
La nomina ad Amministratore di sistema viene effettuata in forma scritta con atto ad hoc.
L'elenco completo ed aggiornato degli Amministratori di sistema è tenuto dai Responsabili dei Servizi Interessati. Le regole di gestione degli amministratori di sistema sono definite nella Istruzione Operativa Interservizi IOI83 "ISTRUZIONE OPERATIVA INTERSERVIZI PER LA GESTIONE DELLA FIGURA DELL'AMMINISTRATORE DI SISTEMA".

6.2 REGOLE GENERALI SUL TRATTAMENTO DEI DATI

Qualunque **trattamento** di dati personali da parte dell'*IRCCS AOU BO* è consentito soltanto per lo svolgimento delle funzioni istituzionali.
I dati personali devono essere trattati in modo lecito, secondo correttezza e trasparenza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le quali sono raccolti e trattati.
È compito dei Referenti Aziendali Privacy verificare periodicamente la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza, necessità, e nel caso dei dati relativi alla salute, l'indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati forniti dall'interessato di propria iniziativa.

6.3 TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO

6.3.1 PREMESSA

I dati personali trattati in ambito sanitario rientrano nella categoria dei **dati particolari** in quanto sono dati **idonei a rivelare lo stato di salute** (c.d. dati sanitari).
L'*IRCCS*, in qualità di organismo sanitario pubblico, ha l'**OBBLIGO** di fornire al paziente un'**informativa** sul trattamento dei dati personali che lo riguardano e, in **determinati contesti**, acquisire il consenso al loro uso.

6.3.2 OBBLIGO DI INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO

Il trattamento dei dati personali in ambito sanitario è subordinato, **sempre**, ad un obbligo di informativa da rendersi al paziente circa il contenuto del trattamento effettuato, **obbligo** che si considera assolto dall'*IRCCS* attraverso **l'affissione della specifica informativa** (**T01/IOA29** "INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI") **nei luoghi di attesa e di accettazione in cui staziona il paziente.** *Il contenuto dell'informativa di cui sopra evidenzia le attività istituzionali aziendali non soggette a specifico consenso.*
I trattamenti di dati relativi alla salute che non rientrano tra quelli presenti nella T01/IOA29 saranno effettuati mettendo a disposizione dell'interessato informazioni integrative e **richiedendo, se previsto, uno specifico ed esplicito consenso**. Si tratta ad esempio di trattamenti connessi:

- all'implementazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico;
- all'implementazione dei sistemi di sorveglianza/registri di patologia;
- a scopi di ricerca scientifica *in campo medico, biomedico, epidemiologico* (tranne alcuni casi specifici previsti dalla legge *ad es. l'art 110 bis, 4 comma del D.Lgs. 196/2003*);
- al trattamento dati genetici e/o biometrici;
- alla comunicazione di dati al medico di fiducia o ad altri soggetti (es. Rete SOLE);
- a servizi di refertazione on-line

Saranno altresì disponibili ulteriori e specifiche informative in relazione a particolari attività amministrative che comportano il trattamento di c.d. dati particolari (quali ad es. informativa relativa al trattamento delle segnalazioni, informativa relativa al contenzioso, ecc.).

Qualora, all'interno di una U.O. si presenti la necessità di effettuare una "particolare" raccolta di dati personali e/o sensibili, per finalità diversa da quelle sopradefinite, il relativo Referente Privacy Aziendale è tenuto a confrontarsi con *la Funzione* Privacy Aziendale al fine di adempiere ai necessari obblighi privacy (informativa e consenso).

6.3.3 *TRATTAMENTO DEI DATI PERSONALI IN AMBITO SANITARIO ATTRAVERSO STRUMENTI INFORMATICI (TELEMEDICINA, TELECONSULTO ECC.)*

L'IRCCS promuove e attua la Telemedicina quale modalità attraverso la quale erogare a distanza prestazioni sanitarie di routine svolte in presenza come la visita, il consulto, il monitoraggio di parametri e l'assistenza.
Attraverso tale modalità si erogano prestazioni di prevenzione, diagnosi, cura e riabilitazione inserite nei LEA e quindi riconosciute nel nomenclatore tariffario come prestazioni erogate in via telematica, in particolare per la presa in carico domiciliare secondo PDTA delle patologie croniche.
La telemedicina non sostituisce la medicina tradizionale, ma la affianca e la integra con nuovi canali di comunicazione e tecnologie innovative, con l'obiettivo di migliorare l'assistenza sanitaria e aiutare i cittadini ad accedere ed ottenere le migliori cure possibili.
Tale modalità può interessare tanto la pratica clinica diagnostica, assistenziale e riabilitativa quanto l'ambito dell'innovazione, ricerca scientifica e sviluppo.
L'IRCCS esegue il trattamento dei dati personali effettuato tramite gli applicativi che consentono la televisita, nella piena osservanza delle normative europee e nazionali e adottando misure tecniche ed organizzative adeguate quali:

- *la progettazione del trattamento secondo una analisi di privacy by design e by default (art. 25 GDPR);*
- *l'analisi del rischio e la valutazione di impatto (art. 35 GDPR);*
- *l'aggiornamento del registro dei trattamenti (art. 30 GDPR).*

L'IRCCS AOU BO ha predisposto su tale modalità di trattamento la seguente informativa: ***T29/IOA29*** *"INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI EROGAZIONE E GESTIONE DELLE PRESTAZIONI SANITARIE IN TELE MEDICINA".*

6.3.4 TRATTAMENTO DEI DATI NELL'AMBITO DELL'ATTIVITA' LIBERO PROFESSIONALE

Fermo restando la titolarità del trattamento dei dati personali per le prestazioni erogate in regime di libera professione in capo all'*IRCCS AOU BO*, il professionista che esercita attività libero professionale assume la qualifica di Referente Aziendale Privacy.
Valgono pertanto le stesse disposizioni aziendali in materia di rilascio dell'informativa e di acquisizione del consenso al trattamento dei dati personali. L'informativa specifica/locandina (T02/IOA29 "INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN RIFERIMENTO ALL'ATTIVITÀ LIBERO-PROFESSIONALE INTRAMURARIA") deve essere affissa nei locali in cui viene svolta attività libero professionale.

6.3.5 TRATTAMENTO DEI DATI GENETICI

Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti dall'art.9, par. 2 del GDPR e dalle misure di garanzia disposte dal Garante per la protezione dei dati personali in attuazione dell'art. 2-septies del Codice Privacy ed è subordinato alla raccolta di uno specifico consenso.
In considerazione della delicatezza dei dati genetici e delle specifiche prescrizioni del Garante Privacy (Autorizzazione Generale n. 8/2016 "Autorizzazione generale al trattamento dei dati genetici"), è necessario che nel trattamento di tale tipologia di dati siano adottate particolari misure organizzative e tecniche:

- *i dati genetici devono essere trattati esclusivamente all'interno di locali protetti e accessibili ai soli soggetti autorizzati al trattamento;*
- *il trasporto dei dati genetici all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti;*
- *il trasferimento dei dati genetici in formato elettronico deve essere cifrato o, comunque, può essere effettuato nel rispetto delle disposizioni date dal'ICT o dal DPO.*

L'*IRCCS AOU BO* ha predisposto, in conformità della normativa vigente, un'informativa specifica (T03/IOA29 "INFORMATIVA PER IL TRATTAMENTO DEI DATI GENETICI E L'UTILIZZO DEI CAMPIONI BIOLOGICI") ed il relativo consenso al trattamento dei suddetti dati (R08/IOA29 "CONSENSO AL TRATTAMENTO DEI DATI GENETICI E DEI CAMPIONI BIOLOGICI"), che deve essere obbligatoriamente sottoscrittto dal paziente e conservato agli atti dell'*IRCCS AOU BO* per il tempo in cui vengono utilizzati i dati stessi e/o il campione biologico.

6.3.6 TRATTAMENTO DEI DATI PERSONALI TRAMITE DOSSIER SANITARIO ELETTRONICO (DSE - applicativo GALILEO)

Il DSE è uno strumento facoltativo di raccolta e gestione di dati sanitari del paziente relativo ad eventi clinici presenti e trascorsi, originati da un unico Titolare del trattamento, ovvero verificatisi all'interno della stessa Azienda. È costituito per **finalità di prevenzione, diagnosi, cura e riabilitazione** quindi costituisce la storia clinica "aziendale" del paziente. Trattandosi di strumento facoltativo, i professionisti aziendali sono obbligati a raccogliere il consenso del paziente alla costituzione o meno del DSE.

Le modalità operative per la gestione del DSE sono riportate nei seguenti specifici documenti:

- Manuale operativo per la gestione del DSE
- Istruzioni per l'acquisizione del consenso al DSE nel dipartimentale Galileo (GSR, GSA, E-VISIT, Exprivia P.S.)
- T13/IOA29 "INFORMATIVA E CONSENSO PER IL DOSSIER SANITARIO ELETTRONICO (DSE)"
- R12/IOA29 "Dichiarazione sostitutiva di atto di notorietà per consenso al DSE"
- *R13/IOA29 "Notifica data breach relativo al DSE" (ad uso esclusivo della Funzione Privacy)*

I documenti sopra elencati sono reperibili all'interno dell'area intranet privacy attraverso il seguente percorso: La privacy in Azienda>Documentazione di riferimento>Dossier Sanitario Elettronico (DSE).

Nei luoghi di attesa e di accettazione in cui staziona il paziente dovrà essere affissa, oltre l'informativa base (**T01/IOA29**), anche l'informativa relativa al DSE (**T13/IOA29**).

6.3.7 TRATTAMENTO DEI DATI NELL'AMBITO DELLA RICERCA *SCIENTIFICA IN CAMPO* MEDICO, BIOMEDICO, ED EPIDEMIOLOGICO

Il trattamento di dati personali nell'ambito della ***ricerca scientifica*** *deve avvenire in conformità di quanto disposto dal GDPR, dal Codice Privacy, nonchè da specifici provvedimenti emessi dall'EDPB e dal Garante Privacy (tra i quali in particolare rilevano Autorizzazione n. 9/2016 "Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica" e le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101" 19 dicembre 2018).*
Per l'inquadramento degli accorgimenti e delle misure necessarie ed adeguate riguardo al trattamento dei dati personali in tale contesto si rinvia alla ***IOA87*** *"ISTRUZIONE OPERATIVA AZIENDALE PER IL TRATTAMENTO DEI DATI NELL'AMBITO DEGLI STUDI CLINICI".*

Il trattamento dei dati nell'ambito della redazione dei c.d. ***case report****, rilevanti nell'ambito dell'attività di pubblicazione scientifica e che non rappresentano alcuna forma di sperimentazione clinica data la natura prettamente descrittiva, è subordinato al rilascio di specifica informativa e alla raccolta del consenso (**T14/IOA29** "INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - UTILIZZO DEI DATI PERSONALI NELLA DESCRIZIONE DEL CASO CLINICO (CASE REPORT)").*
Il professionista che redige un case report dovrà obbligatoriamente rendere i dati personali utilizzati completamente anonimi, in modo da rendere impossibile l'identificazione del paziente per chiunque (ad esempio tramite accesso alla pubblicazione). I dati, pertanto, potranno essere diffusi solo in forma rigorosamente anonima.

6.3.8 *TRATTAMENTI DI DATI PERSONALI NELL'AMBITO DEL RAPPORTO DI LAVORO DEI DIPENDENTI E DELLE ATTIVITÀ SVOLTE DA TERZI NON DIPENDENTI (LIBERI PROFESSIONISTI, CONSULENTI, DOCENTI, CONVENZIONATI, ECC.) E FORNITORI*

L'IRCCS AOU BO tratta i dati per i fini di cui all'articolo 6, par.1, lettera b) del GDPR, ovvero quando 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, nonché per i fini di cui all'art.9, par. 2, lettera b) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.
I Referenti Privacy sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del GDPR, nel rispetto delle indicazioni fornite dal Titolare.
In ogni caso le predette informazioni dovranno essere inserite nei relativi atti contrattuali e, laddove il rapporto sia soggetto a procedure concorsuali, le predette informazioni dovranno essere necessariamente contenute nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.
L'IRCCS AOU BO ha predisposto la seguente specifica informativa: ***T09*** *"INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI PER LA GESTIONE DEL RAPPORTO DI LAVORO DEI DIPENDENTI E DELLE ATTIVITÀ SVOLTE DA TERZI NON DIPENDENTI (LIBERI PROFESSIONISTI, CONSULENTI, DOCENTI, CONVENZIONATI, ECC.) E FORNITORI" pubblicata anche nel sistema di Gestione delle Risorse Umane – GRU e nella sezione privacy del sito web istituzionale: https://www.aosp.bo.it/it/content/privacy*

6.3.9 *TRATTAMENTO DEI DATI PERSONALI NEI DOCUMENTI SOGGETTI A PUBBLICAZIONE*

Gli atti dell'IRCCS AOU BO soggetti a pubblicazione contenenti dati particolari di cui agli articoli 9 e 10 del Regolamento UE, i provvedimenti disciplinari e gli atti concernenti i minori, non dovranno essere pubblicati in forma identificativa.

Sarà cura dei Referenti Privacy Aziendali valutare le modalità per pseudoanonimizzarli o anonimizzarli, eventualmente previa consultazione con l'Ufficio Privacy e con l'ICT, garantendo in ogni caso al diretto interessato la possibilità di identificarsi.

6.4 ISTRUZIONI PER GLI OPERATORI CHE TRATTANO I DATI DEI PAZIENTI: MISURE TECNICHE, ORGANIZZATIVE E PER IL RISPETTO DELLA DIGNITA' DEGLI INTERESSATI

La nuova disciplina impone al Titolare di **garantire il rispetto** dei principi in essa contenuti, ma anche di **essere in grado di comprovarlo** adottando una serie di **strumenti specifici.**

Il titolare tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto del contesto e delle finalità di trattamento come del rischio, deve adottare le **misure tecniche ed organizzative adeguate** a garantire un **livello di sicurezza adeguato al rischio**. Spetta inoltre al titolare individuare specificatamente i rischi legati al trattamento dei dati e valutare quali misure di sicurezza tecniche, organizzative procedurali adottare (accountability-responsabilizzazione del titolare).

Al titolare è richiesta un'analisi dell'organizzazione aziendale e dei sistemi che coinvolgono i trattamenti dei dati personali e la loro protezione deve essere garantita fin dalla progettazione (by design) ed in maniera predefinita (by default).
Diventa quindi fondamentale eseguire una attenta valutazione dei rischi e degli impatti al fine di pianificare da subito le attività da realizzare che possono comportare modifiche culturali, organizzative e tecnologiche.

L'IRCCS AOU BO, nell'organizzazione delle prestazioni e dei servizi, adotta inoltre le seguenti misure volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

6.4.1 INFORMAZIONI SULLO STATO DI SALUTE DELL'INTERESSATO NEL RISPETTO DEI SUOI DIRITTI

Le informazioni sullo stato di salute vanno rese esclusivamente al **diretto interessato** o, in ipotesi di soggetto incapace di agire, al suo **rappresentante legale**. È demandata esclusivamente a tali individui la facoltà di autorizzare tale comunicazione verso ulteriori soggetti, **familiari** o **terzi**. Ciò avviene solo previa autorizzazione scritta da acquisirsi su apposito modulo (**R04/IOA29** "Modulo per la comunicazione dei dati sullo stato di salute") che va conservato in cartella clinica, rappresentando l'unico strumento per i contatti autorizzati, e ad ogni aggiornamento dei contenuti, il report deve essere controfirmato dall'interessato.
Qualora il paziente versi in uno stato di incapacità naturale, attestato dal personale medico (trattasi dell'ipotesi in cui il **soggetto** è **temporaneamente impedito**, ovvero è incapace di intendere o di volere, ma non ha un rappresentante legale), le informazioni di cui sopra sono rese a chi dichiari, sotto la propria responsabilità, di essere prossimo congiunto, familiare, convivente o, assenza di questi, responsabile della struttura presso cui dimora l'interessato (**R05/IOA29** "Modulo per la comunicazione dei dati sullo stato di salute – paziente temporaneamente impedito").
I dati idonei a rivelare lo stato di salute possono essere resi noti all'interessato o al rappresentante legale (ovvero esercente la responsabilità genitoriale, tutore, curatore, amministratore di sostegno) o prossimo congiunto, familiare, convivente o, in loro assenza, responsabile della struttura presso cui dimora l'interessato **solo** per il tramite di un **medico** designato dall'interessato o dal Titolare.
Tuttavia, anche **altro personale sanitario** (diverso da quello medico), deputato ad intrattenere, nell'esercizio dei propri compiti, rapporti diretti con i pazienti, può essere autorizzato **per iscritto** dal Titolare o dal Referente Privacy Aziendale a tale comunicazione.
L'interessato ha diritto di conoscere la propria **collocazione** nelle **liste delle prestazioni** ambulatoriali, di diagnostica strumentale e di laboratorio, dei ricoveri ospedalieri e nelle altre liste di attesa, ma non può venire a conoscenza dei nominativi che lo precedono o lo seguono nell'elenco.

6.4.2 INFORMAZIONI SULLA DISLOCAZIONE DELL'INTERESSATO NELL'AMBITO DEI REPARTI NEL RISPETTO DEI SUOI DIRITTI

L'interessato o chi per lui che non volesse rilasciare notizie sulla dislocazione del ricovero dovrà esprimere tale volontà compilando l'apposito campo presente nel "Modulo per la comunicazione dei dati sullo stato di salute" (R04/IOA29 o R05/IOA29). In tal caso, il personale addetto all'accettazione provvederà a flaggare il campo "RISERBO" nella procedura informatizzata per i degenti.

6.4.3 DOCUMENTAZIONE CARTACEA CONTENENTE DATI PERSONALI

Per tutto il periodo in cui si effettuano operazioni di trattamento dei dati in modalità cartacea, non si deve mai perdere di vista i documenti oggetto di trattamento, per cui il Referente *Privacy Aziendale* e il Soggetto Autorizzato devono adempiere ad un preciso obbligo di custodia dei medesimi.

- ⇨ Modalità di trasporto interno della documentazione
  Quando la documentazione contenente dati *particolari* deve essere trasportata all'interno dell'ospedale, è necessario utilizzare le dovute cautele al fine di impedire un accesso non autorizzato (es. utilizzo di contenitori/buste sigillate, ecc.).

- ⇨ Modalità di consegna all'interessato della documentazione cartacea:
  Al momento della consegna dei documenti contenenti dati personali e/o sensibili all'interessato, è necessario adottare le garanzie minime di sicurezza di seguito indicate:
  - utilizzare buste chiuse
  - accertarsi dell'identità del diretto interessato
  - consegnare la documentazione all'interessato o a soggetti diversi dallo stesso solo se autorizzati dall'interessato e muniti di delega scritta.

- ⇨ Modalità di invio postale all'interessato della documentazione sanitaria:
  L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione scritta dello stesso (R11/IOA29 "Informativa e Consenso all'invio di *dati particolari* tramite fax, e-mail, posta").
  In tal caso *di invio postale* i documenti devono essere contenuti in plico sigillato, evitando di riportare sulla busta stessa i riferimenti a servizi/strutture specifici dell'*IRCCS* che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsiasivoglia di patologia.

- ⇨ Modalità di conservazione della documentazione cartacea
  L'accesso ai luoghi adibiti ad archivi "temporanei" di UO deve essere controllato e devono essere identificati i soggetti che vi accedono. In caso di abbandono, anche temporaneo, del luogo adibito ad archivio, l'operatore non deve lasciare incustoditi i documenti: è infatti necessario identificare un luogo sicuro di custodia che dia sufficiente garanzia di protezione da accessi non autorizzati (es. un armadio con casetti chiusi a chiave, una cassaforte, locale chiuso a chiave, ecc.). Occorre in particolare accertarsi che nessun visitatore o terzo estraneo possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti.
  I soggetti che devono accedere agli archivi di UO, dopo l'orario di chiusura della struttura, devono essere identificati e registrati su idoneo strumento predisposto dal Referente Aziendale Privacy dell'UO.
  Per quanto attiene alla conservazione delle cartelle cliniche e della documentazione sanitaria si rinvia allo specifico documento "Procedura aziendale per la richiesta e il rilascio di copia della cartella clinica e di altra documentazione sanitaria" PA36. La responsabilità della conservazione e della sicurezza degli archivi contenenti dati personali spetta al Referente Aziendale Privacy dell'UO di

afferenza, fatta salva la disciplina aziendale in materia di archiviazione e deposito della documentazione presso archivi generali dell'*IRCCS AOU BO*.

⇨ Modalità di trattamento dei dati in reparto (elenchi pazienti presenti)

Non è giustificata l'affissione di liste di pazienti in locali aperti al pubblico, con o senza la descrizione della patologia sofferta. Tuttavia, l'elenco dei degenti presenti in reparto, per esigenze organizzative, può essere collocato in locali o aree riservate, dove solo il personale autorizzato può consultarle (ad esempio nella guardiola del Coordinatore Infermieristico).

Non è possibile apporre una targhetta identificativa riportante nome e cognome del paziente posizionata in testa o ai piedi del letto dell'interessato, poiché è vietata la diffusione dei dati idonei a rivelare lo stato di salute ai sensi dell'art. 2-septies, comma 8, del Codice Privacy novellato.

6.4.4 COMUNICAZIONI TELEFONICHE

In via generale, è preferibile non fornire indicazioni inerenti lo stato di salute degli interessati via telefono se non si è certi dell'identità dell'interlocutore e del fatto che egli sia autorizzato ad acquisire tali informazioni. Un suggerimento potrebbe essere quello di farsi comunicare dal chiamante, nominativo e numero di telefono; dopo di che, si può provvedere a ricontattare l'interlocutore, previa verifica dei dati forniti e dell'autorizzazione dello stesso soggetto ad acquisire tali informazioni.

⇨ Accorgimenti per fornire informazioni presso i Punti Informativi

È lecito comunicare la presenza del paziente all'interno dell'ospedale indicando a chi lo richiede il nome dell'Unità Operativa ed il nome e numero del Padiglione.

Se il paziente ha manifestato la volontà di non comunicare la presenza in ospedale (attraverso la compilazione del report R04/IOA29 o R05/IOA29), l'operatore addetto non avrà accesso ai dati in quanto non saranno visibili e dovrà comunicare per tanto al richiedente che a sistema non risultano presenze relative al nominativo richiesto. La conseguenza di ciò, da spiegare in modo chiaro al visitatore richiedente, è che o la persona non risulta ricoverata all'interno della struttura o se ricoverata, ha manifestato una volontà contraria a far conoscere a terzi la dislocazione all'interno della struttura medesima.

⇨ Modalità per fornire notizie o conferma, anche telefonica, a terzi legittimati di una prestazione di Pronto Soccorso

Al fine di dare correttamente notizia o conferma, anche telefonica, a terzi di una prestazione di Pronto Soccorso occorre:

- preliminarmente verificare che il paziente sia in grado di decidere se comunicare a terzi la sua presenza in Pronto Soccorso e ulteriori informazioni sul suo stato di salute;
- nel caso di accertata incapacità o impossibilità del paziente a decidere autonomamente, adottare una serie di accorgimenti *volti ad accertare* la sussistenza di un *reale* legame tra il chiamante ed il paziente (a titolo meramente esemplificativo, si potranno richiedere informazioni riguardanti caratteristiche fisiche – colore capelli, occhi – segni particolari o accessori indossati – barba, occhiali, tatuaggi – ovvero conferma di dati personali).

A seguito di queste verifiche si può confermare o meno la presenza del paziente in PS.

⇨ Modalità di contatto telefonico STRUTTURA SANITARIA-UTENTE

Nel caso in cui sia necessario contattare telefonicamente l'interessato (ad es. per lo spostamento di una visita, la risposta ad una segnalazione, ecc.) occorre verificare la presenza di un numero telefonico a cui contattarlo utilizzando, esclusivamente, la documentazione o gli applicativi informatici aziendali. Non è lecito, pertanto, andare a ricercare eventuali numeri di telefono presenti in elenchi o rubriche pubblici, al fine di poter ricontattare l'interessato il quale deve ritenersi che, ove non abbia fornito alcun numero di telefono, non voglia essere contattato.

Nel caso in cui l'interessato abbia fornito sia un numero telefonico di rete fissa che di rete mobile, è preferibile utilizzare quest'ultimo.
Qualora si utilizzi il numero di rete fissa occorre accertarsi di conferire direttamente con l'interessato. Nell'ipotesi in cui, in tale circostanza, risponda un soggetto diverso dall'interessato, bisogna, SENZA rilasciare specifiche informazioni (es. U.O. di appartenenza, motivo della chiamata, ecc.), chiedere di conferire direttamente con l'interessato e, qualora ciò non risulti possibile, bisogna terminare la conversazione provando a ricontattare l'interessato in un altro momento.

6.4.5 MODALITA' DI UTILIZZO DEL FAX/E-MAIL/*CLOUD AZIENDALE*/FOTOCOPIATRICE/STAMPANTE

Premesso che a monte di qualsiasi modalità di trasmissione di dati personali è necessario avere certezza che il destinatario sia soggetto legittimato alla ricezione degli stessi (ad es. in qualità di diretto interessato, o sulla base di un rapporto contrattuale/convenzionale in essere che espliciti la modalità di trasmissione di dati), si riportano di seguito gli strumenti utilizzabili all'interno dell'IRCCS.

⇨ FAX

Ai sensi dell'art. 47, comma 2, lett. c del CAD, le comunicazioni tra Pubbliche Amministrazione devono avvenire esclusivamente per via telematica ed è pertanto fatto assoluto divieto di usare il fax in tal senso.
Il fax può ancora essere utilizzato dall'IRCCS AOU BO:

- *per comunicazioni verso* ***soggetti privati*** *esclusivamente se espressamente richiesto da questi ultimi in quanto sprovvisti di diversi strumenti (es. e-mail, PEC)*
- *per comunicazioni operative esclusivamente* ***tra UUOO dell'IRCCS AOU BO***

L'utilizzo del fax deve avvenire sempre seguendo i seguenti accorgimenti:

a) prestare *sempre* attenzione alla corretta digitazione del numero cui inviare il documento;
b) nel caso *in cui* si debba procedere, tramite fax, alla comunicazione di dati *particolari*, è opportuno che lo strumento fax sia collocato in un'area protetta e presidiata, non accessibile a terzi non autorizzati e che i Referenti privacy *aziendali* e il personale autorizzato prestino attenzione alle fasi di invio e di ricevimento della documentazione contenente dati personali *particolari*;
c) nel caso in cui l'interessato chieda l'invio di propria documentazione *contenente dati particolari* (es. referti, prescrizioni specifiche, riscontro ad un'istanza di accesso, ecc.) ad un determinato numero di fax, dovrà preventivamente compilare il modulo predisposto (R11/IOA29 "INFORMATIVA E CONSENSO ALL'INVIO DI *DATI PARTICOLARI* TRAMITE FAX, E-MAIL, POSTA").

⇨ Posta Elettronica Certificata *(PEC)*, Posta Elettronica Ordinaria *(PEO)*, *Cloud aziendale*

Le regole per la gestione della posta elettronica sono definite nella IOA99 "Utilizzo della posta elettronia e internet".
Di seguito si riportano per comodità le indicazioni per l'invio di documentazione ***contenente dati particolari*** all'interno e all'esterno dell'*IRCCS tramite strumenti elettronici.*
Premesso che solamente l'uso della Posta Elettronica Certificata (PEC) garantisce la certificazione dell'invio e della consegna del messaggio e della sua integrità, l'IRCCS AOU BO, consapevole che l'uso della Posta Elettronica Ordinaria (PEO), c.d. e-mail, è divenuto il mezzo di comunicazione scritta più utilizzato, definisce le seguenti regole di utilizzo di tali strumenti nella trasmissione di documentazione contenente dati particolari all'interno e all'esterno dell'IRCCS AOU BO.

Trasmissione di documentazione contenente dati particolari all'ESTERNO dell'IRCCS	
*al **paziente***	*a **strutture esterne autorizzate** (es. altre Aziende Sanitarie, Case di Cura nell'ambito del proseguimento di cura del paziente ecc.)*
*è indispensabile raccogliere lo specifico consenso scritto dell'interessato utilizzando il modulo **R11/IOA29*** "INFORMATIVA E CONSENSO ALL'INVIO DI *DATI PARTICOLARI* TRAMITE FAX, E-MAIL, POSTA"	*lo scambio di documentazione contenente dati particolari deve essere preventivamente concordato e definito con la struttura esterna autorizzata nell'ambito del contratto/convenzione in essere o tramite nota scritta che definisca i criteri di trasmissione ordinariamente utilizzati.*

POSSIBILI MODALITA' DI TRASMISSIONE:

⇨ *da **Posta Elettronica Certificata (PEC) a PEC**: la documentazione trasmessa deve essere semplicemente allegata alla PEC trasmessa (es. referto specialistico in formato pdf non protetto)*

⇨ *da **Posta Elettronica Ordinaria (PEO) a PEO**: la documentazione trasmessa deve essere obbligatoriamente protetta attraverso crittografia del file* (es. referto specialistico in formato pdf protetto). La pw dovrà essere comunicata con diverso mezzo (ad es. telefonicamente, o con separata e-mail, o per iscritto o verbalmente all'atto della richiesta)

N.B. la crittografia di un file pdf è un'operazione semplice che viene effettuata attraverso il software PDF Creator, se non disponibile è possibile rivolgersi all'*UO Informations and Communications Technology (ICT)* per l'installazione dello stesso.

⇨ *utilizzando il sistema di **Cloud aziendale** disponibile all'indirizzo https://cloud.aosp.bo.it*
Tale sistema consente di salvare e condividere, anche con destinatari esterni all'IRCCS, file, anche di grosse dimensioni, in modalità protetta. La guida all'utilizzo di tale strumento è resa disponibile dall'UO Informations and Communications Technology nella sezione dedicata https://intranet.aosp.bo.it/content/dtsi/owncloud

Trasmissione di documentazione contenente dati particolari all'INTERNO dell'IRCCS
*i **professionisti sanitari** non possono utilizzare l'e-mail aziendale per scambiarsi documentazione contenente dati sanitari (es. referti).* *Qualora si presenti la necessità di cui sopra si consiglia di utilizzare una delle seguenti modalità:* ⇨ *consultazione del **DSE** aziendale utilizzando l'**accesso giustificato*** ⇨ *utilizzando il sistema di **Cloud aziendale** (cfr sopra)* ⇨ *trasmissione tramite **Posta Elettronica Ordinaria (PEO)** con file protetto (cfr sopra)*

⇨ Utilizzo della fotocopiatrice e della stampante

La fotocopiatura/stampa di documentazione contenente dati personali e *particolari* deve avvenire per opera di personale autorizzato, il quale deve provvedere altresì al ritiro tempestivo della documentazione dalla fotocopiatrice/stampante ed alla conservazione della stessa. Non deve essere riutilizzata, per esigenze di economia e risparmio, carta stampata da un lato, ove la stessa contenga informazioni personali e *particolari* presenti sull'altro lato del foglio e la copia sia destinata ad uso di terzi, diversi dal soggetto riproducente il testo. Nel caso in cui le fotocopie/stampe contenenti dati sensibili non siano più da conservare o non siano leggibili o conformi, prima di essere cestinate, devono essere trattate in modo da non rendere intelligibili le informazioni contenute a terzi non autorizzati.

6.4.6 RAPPORTI DI FRONT OFFICE

Anche la gestione delle informazioni presso i front office richiede l'adozione di misure organizzative e comportamentali al fine di garantire il più ampio rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

- ⇨ Identificazione dell'interessato e controllo dell'esattezza dei dati

  Al momento della raccolta di dati anagrafici occorre fare attenzione alla digitazione e inserimento corretto dei dati identifcativi dell'interessato, verificando che le informazioni già disponbili siano aggiornate (es. indirizzo, n. telefono ecc.).

- ⇨ Distanza di cortesia

  Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato. Vanno in questa prospettiva prefigurate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli. Pertanto, è indispensabile che tutti i punti accettazione siano muniti di strumenti idonei a garantire tale distanza di cortesia per gli utenti individuando gli strumenti più idonei al contesto e alla struttura (es. una riga gialla di segnalazione a terra ed un cartello che indichi il rispetto della distanza di cortesia, o qualunque altro sistema garantisca il medesimo risultato).

- ⇨ Modalità di chiamata degli interessati

  All'interno dei locali di strutture sanitarie, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa, devono essere adottate **soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa** (ad es. attribuzione al momento della prenotazione o dell'accettazione di un codice numerico o alfanumerico o chiamata per nome di battesimo e prima lettera del cognome, ecc.).

  Si precisa che quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), possono essere utilizzati altri accorgimenti adeguati ed equivalenti (ad es. con un contatto diretto con il paziente).

6.4.7 COLLOQUIO CON L'INTERESSATO

É doveroso adottare idonee cautele in relazione allo svolgimento di **colloqui**, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

Il rispetto di questa garanzia non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell'intervento medico (ad es. alcuni trattamenti sanitari effettuati nei confronti di minori).

Il **dialogo-colloquio tra personale dell'*IRCCS AOU BO* e utenti**, qualora abbia ad oggetto informazioni inerenti lo stato di salute dell'interessato ed avvenga in spazi od in situazioni ove vi sia la presenza di altri soggetti, oltre all'utente interessato (ad esempio nelle stanze di degenza a più posti letto o nei punti ove vengono ritirati dagli interessati, esami, referti ecc., o presso le accettazioni e le segreterie delle Unità Operative), deve essere improntato ad un criterio di prudenza.
Stessa prudenza deve essere mantenuta nelle condizioni usuali di **colloquio tra operatori** nell'esercizio della professione: discussione di casi clinici durante il "giro-visita", supervisione di casi in luoghi aperti all'utenza, consulenze specialistiche effettuate al letto di degenza, passaggi di consegne tra personale, comunicazioni di servizio effettuate mediante apparecchi telefonici portatili o meno non posizionati in luoghi protetti, informazioni fornite a frequentatori medici, consulenti.
Una precisazione particolare merita il trattamento dei dati relativi alla **convinzione religiosa**, che rappresenta un dato sensibile non necessario ai fini della permanenza della persona in Azienda. Sono da preferire forme alternative e indirette, ad esempio, per stabilire le **preferenze alimentari** del paziente (ad es. evitare le portate a base di maiale). Per cui si consiglia di non formulare la domanda: "A quale religione appartiene?" o "E' di religione ebraica?", ma di utilizzare forme indirette del tipo "Ha delle preferenze alimentari?".
Al fine di limitare l'eventuale disagio dei pazienti, anche in relazione all'invasività del trattamento, oltre ad adottare specifiche cautele, qualora il paziente manifestasse la volontà di **limitare la presenza di personale sanitario in formazione** durante l'esecuzione della prestazione (ambulatoriale o di ricovero) è necessario soddisfare tale richiesta.

6.4.8 EFFETTUAZIONE DI IMMAGINI FOTOGRAFICHE E/O DI RIPRESE AUDIO/VIDEO

L'effettuazione di immagini fotografiche e/o di riprese audio/video su **pazienti** è possibile *esclusivamente* per *le* seguenti finalità:

a) *finalità clinica connessa al percorso di cura del paziente;*
b) *attività di ricerca scientifica;*
c) *attività didattiche e di formazione professionale;*
d) *divulgazione scientifica;*
e) *divulgazione e comunicazione, senza scopo di lucro, relative ad attività istituzionali dell'IRCCS AOU BO*

Il perseguimento

- *della **finalità a)** non implica la raccolta del consenso del soggetto interessato (ex art. 9 par. 2 lett. h), i) e j) del GDPR);*
- *delle **finalità b), c), d), e)** implica la raccolta di **espresso consenso** del soggetto interessato (ex art. 6, comma 1 lettera a) del GDPR) attraverso l'utilizzo dello specifico modulo **R15/IOA29** "TRATTAMENTO DI IMMAGINI PERSONALI PER LA REALIZZAZIONE DI FOTOGRAFIE/RIPRESE AUDIO/VIDEO - INFORMATIVA E LIBERATORIA".*

Il materiale prodotto per il perseguimento della

- ***finalità a)** e **b)** dovrà essere trattato come gli altri documenti sanitari (es. cartella di ricovero, referto ambulatoriale), ovvero non dovrà essere diffuso, cioè portato a conoscenza di soggetti indeterminati ed estranei al percorso di cura. Qualora le caratteristiche del supporto utilizzato non permettano una conservazione congiunta agli altri documenti sanitari collegati al paziente (es. cartella clinica), il professionista sanitario provvederà ad annotare l'avvenuta operazione nel documento principale. Il medesimo professionista sarà altresì responsabile della corretta conservazione del materiale.*
- ***finalità c)** e **d)** potrà essere pubblicato, in forma anonima, su riviste scientifiche, slide formative, piattaforme dedicate alla web-streaming dello specifico evento;*
- ***finalità e)** potrà essere pubblicato su brochures aziendali, articoli di stampa locale o nazionale, piattaforme dedicate alla web-streaming dello specifico evento, social network (Facebook/Instangram) e Youtube attraverso gli account ufficiali dell'IRCCS AOU BO.*

Il materiale prodotto dovrà essere archiviato e custodito in stretta osservanza della normativa vigente in tema di tutela della riservatezza dei dati personali e sensibili.

*Si precisa che l'utilizzo del modulo **R15/IOA29** copre l'effettuazione di immagini fotografiche e/o di riprese audio/video da parte di IRCCS AOU BO esclusivamente per il perseguimento di fini istituzionali come esplicitato in premessa.*

6.4.9 MISURE PER LA RICONOSCIBILITÀ DEL PERSONALE

L'IRCCS AOU BO svolge le proprie attività ispirandosi ad alcuni principi fondamentali per la realizzazione di un ospedale ad alto contenuto assistenziale in particolare:

- *l'umanizzazione in tutte le forme espressive che possono caratterizzarla sul piano strutturale, ambientale, funzionale, relazionale, sì da configurare un ospedale a misura d'uomo;*
- *l'affidabilità, intesa come capacità di generare fiducia nei cittadini con il decisivo contributo della professionalità degli operatori, del livello tecnologico, della "sicurezza" e della "tranquillità" indotte dall'intero assetto organizzativo ed ambientale.*

Da tali principi deriva un "modello etico" che richiama gli aspetti della trasparenza, della veridicità delle informazioni, anche e soprattutto nei rapporti tra gli operatori dell'IRCCS AOU BO e i cittadini, nell'intento di perseguire l'ottimizzazione dell'erogazione dei servizi, nonché il miglioramento delle relazioni con l'utenza, che si ritiene debba realizzarsi nel modo più congruo, tempestivo ed efficace.
Nell'ambito di tali principi, l'IRCCS AOU BO adotta, nel complesso dei mezzi per la tutela degli interessi degli utenti, strumenti che garantiscano la riconoscibilità del personale operante all'interno dell'Azienda, dipendente e non. In particolare, il tesserino di identificazione personale riporta, quali elementi essenziali, la fotografia, il nome e cognome e la qualifica. Qualsiasi altro strumento di identificazione personale diverso dal tesserino e nel quale non sia possibile inserire una fotografia (ad es. casacche e indumenti da lavoro) riporta comunque il nome e cognome e la qualifica.

6.4.10 MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI SU SUPPORTO INFORMATICO

Per le misure di sicurezza relative al trattamento dei dati su supporto informatico, si rinvia alla Istruzione operativa aziendale IOA44 "Regolamento aziendale in tema di sicurezza e riservatezza nell'uso delle risorse informatiche" *e alle specifiche indicazioni fornite dall'UO Information and Communication Technology (ICT).*

6.5 I DIRITTI DELL'INTERESSATO

Con riferimento alle misure procedurali disposte dal Titolare del trattamento per permettere all'utente interessato di ottenere in qualsiasi momento informazioni sull'utilizzo dei suoi dati ai sensi degli artt. 12-21 del GDPR, e precisamente il diritto:

- *di informazione, comunicazione e trasparenza (artt. 12, 13 e 14);*
- *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).*

si rinvia alla ***PA122*** *"Procedura aziendale per l'esercizio dei diritti dell'interessato".*

6.6. RELAZIONE TRA PRIVACY E DIRITTO DI ACCESSO

L'accesso ai documenti amministrativi, contenenti dati personali del diretto interessato o di soggetti terzi, formati o detenuti dall'*IRCCS AOU BO*, resta disciplinato dalle disposizioni contenute nel Regolamento *sul*

diritto di accesso a documenti amministrativi e diritto di accesso civico approvato con Delibera n. 516 del 25/11/2015.
L'*IRCCS* ha predisposto una specifica informativa *sul trattamento dei dati personali relativamente a richieste di accesso a documentazione sanitaria (T21/IOA29 "INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI RELATIVAMENTE A RICHIESTE DI ACCESSO A DOCUMENTAZIONE SANITARIA") ad integrazione di quanto contenuto nel Regolamento sopra citato.*
Qualora l'istanza di accesso riguardi documenti recanti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito nel rispetto del principio del pari rango (artt. 59 e 60 del Codice Privacy). Resta fermo, in capo al responsabile del procedimento, l'onere di consentire l'accesso ai soli dati pertinenti e non eccedenti rispetto alla finalità dell'istanza presentata, avvalendosi della consulenza del Responsabile Privacy Aziendale nella valutazione del caso.
L'istanza di "accesso generalizzato", c.d. FOIA, ex art. 5 D.Lgs. n. 33/2013, presentata dal cittadino viene gestita *dalle Articolazioni Aziendali che detengono le informazioni e/o i documenti e* che, a seconda del contenuto della richiesta, potranno avvalersi della consulenza del Responsabile Privacy Aziendale.

6.7 FORMAZIONE

L'*IRCCS AOU BO* individua nella specifica formazione del personale un elemento strategico della propria politica in materia di protezione dei dati personali.
Nell'ambito della programmazione degli interventi formativi del personale (corsi disponibili nell'ambito del Piano Aziendale di Formazione), sono garantiti a tutti i dipendenti, specifici corsi in materia di tutela della riservatezza e protezione dei dati finalizzati alla conoscenza della specifica normativa nonché degli strumenti aziendali predisposti a tutela della privacy, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza dei rischi e delle misure di sicurezza per prevenirli.
Alla formazione base, programmata annualmente, si affiancano momenti di approfondimento richiesti dalle strutture sanitarie rispetto a tematiche o problematiche specifiche.
Si ricorda che uno dei compiti attribuiti dal Titolare al Referente Privacy Aziendale è quello che partecipi sia in prima persona agli specifici momenti formativi organizzati dall'*IRCCS AOU BO* per i Referenti Privacy, e che assicuri la partecipazione dei propri collaboratori autorizzati ai corsi formativi dedicati al personale.

6.8 VERIFICHE INTERNE PRIVACY

Il DPO definisce, propone e concorda con il Titolare un piano annuale di audit interni e svolge attività di audit sul campo, al fine di verificare che la normativa vigente e le policy aziendali siano correttamente attuate e applicate.
La Funzione Privacy fornisce supporto ai servizi aziendali coinvolti nell'attività di audit espletata dall'UO interaziendale DPO, riceve dal DPO gli esiti della verifica e collabora per la messa in atto delle eventuali azioni correttive o comunque conseguenti.

6.9 VIDEOSORVEGLIANZA

L'*IRCCS AOU BO* ha approvato, nel rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone, con particolare riferimento alla riservatezza, all'identità e alla protezione dei dati personali, un *documento* aziendale sulla videosorveglianza che ne disciplina l'attività. A tal proposito, si rinvia allo specifico documento IOA91 "Istruzione Operativa Aziendale gestione della videosorveglianza" *e relativi allegati*.

6.10 PRIVACY POLICY AZIENDALE E AREA PRIVACY INTRANET

L'*IRCCS AOU BO* ha definito, con specifica informativa (T06/IOA29 "INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI ED UTILIZZO DEI COOKIE DEGLI UTENTI CHE CONSULTANO IL SITO WEB DEL L'AZIENDA OSPEDALIERO-UNIVERSITARIA DI BOLOGNA IRCCS POLICLINICO DI S. ORSOLA"), la propria Privacy Policy, ovvero le regole adottate nella gestione del sito web aziendale (disponbile nell'area internet aziendale).
Stante l'importanza sempre crescente e l'attenzione che deve essere riservata alle tematiche connesse alla tutela del dato, che impongono non soltanto l'adozione di misure di tipo tecnico, ma anche la condivisione e la conoscenza delle più importanti disposizioni e indirizzi adottati in materia, l'*IRCCS AOU BO* ha predisposto,

nell'area intranet aziendale, una specifica sezione, denominata "**La privacy in Azienda**", dedicata a tutti gli operatori dell'*IRCCS AOU BO*, nella quale si possono trovare le regole e gli strumenti per l'applicazione quotidiana della normativa privacy.

6.11 RINVIO

Per quanto non previsto dal presente documento trovano applicazione le disposizioni del *GDPR*, del D.Lgs n. 196/2003 "Codice in materia di protezione dei dati personali" s.m.i e quelle dei provvedimenti del Garante Privacy.

6.12 DISPOSIZIONI SPECIALI

Oltre a quanto sopra riportato, per particolari categorie di dati definiti "**ultra sensibili**", occorre soddisfare, nel loro trattamento, le disposizioni speciali emanate dal legislatore, *ponendo particolare attenzione ad eventuali provvedimenti emanati dal Garante Privacy*. In particolare:

- **Tossicodipendenze** (D.P.R. del 09/10/1990, n. 309 "Testo unico sugli stupefacienti")
- **Infezione da HIV** (Legge del 05/06/1990, n. 135 "Programma di interventi urgenti per la prevenzione e la lotta contro l'AIDS")
- **Interruzione della gravidanza** (Legge del 22.05.1978, n. 194 "Tutela sociale della maternità ed interruzione volontaria della gravidanza")
- **Parto in anonimato** (art 30 del Decreto del presidente della repubblica 03.11.2000, n. 396 "Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile, a norma dell'articolo 2, comma 12, della legge 15 maggio 1997, n. 127", art. 24 della Legge del28.03.2001, n. 149 "Modifiche alla legge 4 maggio 1983, n. 184, recante "Disciplina dell'adozione e dell'affidamento dei minori", nonche' al titolo VIII del libro primo del codice civile".
- **Violenza sessuale**, **abuso minorile** (Legge del 15.02.1996, n. 66 "Norme contro la violenza sessuale", Legge del 03.08.1998, n. 269 "Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitu", Legge del 05/04/2001, n. 154 "Misure contro la violenza nelle relazioni familiari")

7. ALLEGATI E MODULI UTILIZZATI

R04/IOA29	MODULO PER LA COMUNICAZIONE DEI DATI SULLO STATO DI SALUTE DEL PAZIENTE
R05/IOA29	MODULO PER LA COMUNICAZIONE DEI DATI SULLO STATO DI SALUTE DEL PAZIENTE TEMPORANEAMENTE IMPEDITO
R08/IOA29	CONSENSO AL TRATTAMENTO DEI DATI GENETICI E DEI CAMPIONI BIOLOGICI
R11/IOA29	INFORMATIVA E CONSENSO ALL'INVIO DI *DATI PARTICOLARI* TRAMITE FAX, E-MAIL, POSTA
R12/IOA29	DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETA' PER CONSENSO AL DOSSIER SANITARIO ELETTRONICO (DSE)
R13/IOA29	NOTIFICA DATA BREACH RELATIVA AL DOSSIER ELETTTRONICO SANITARIO (DSE)
R15/IOA29	TRATTAMENTO DI IMMAGINI PERSONALI PER LA REALIZZAZIONE DI FOTOGRAFIE / RIPRESE AUDIO / VIDEO - INFORMATIVA E LIBERATORIA
T01/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
T01/IOA29 CRT	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN MATERIA DI DONAZIONE E TRAPIANTO DI ORGANI, TESSUTI E CELLULE
T02/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI IN RIFERIMENTO ALL'ATTIVITÀ LIBERO-PROFESSIONALE INTRAMURARIA
T03/IOA29	INFORMATIVA PER IL TRATTAMENTO DEI DATI GENETICI E L'UTILIZZO DEI CAMPIONI BIOLOGICI
T06/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI ED UTILIZZO DEI COOKIE DEGLI UTENTI CHE CONSULTANO IL SITO WEB DEL POLICLINICO S. ORSOLA-MALPIGHI
T08/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI TRAMITE FORM

T09/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI PER LA GESTIONE DEL RAPPORTO DI LAVORO DEI DIPENDENTI E DELLE ATTIVITÀ SVOLTE DA TERZI NON DIPENDENTI (LIBERI PROFESSIONISTI, CONSULENTI, DOCENTI, CONVENZIONATI, ECC.) E FORNITORI
T12/IOA29	INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI REGISTRO PREVENZIONE INSUFFICIENZA RENALE PROGRESSIVA (P.I.R.P.) E DEL REGISTRO REGIONALE DIALISI E TRAPIANTO
T13/IOA29	INFORMATIVA E CONSENSO PER LA COSTITUZIONE FACOLTATIVA DEL DOSSIER SANITARIO ELETTRONICO (DSE)
T14/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - UTILIZZO DEI DATI PERSONALI NELLA DESCRIZIONE DEL CASO CLINICO (CASE REPORT)
T15/IOA29	INFORMATIVA PRIVACY NELL'AMBITO DELLA ATTIVITÀ DI RIVALSA DEL DATORE DI LAVORO
T16/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI PAGINA FACEBOOK E ISTAGRAM DELL'AZIENDA OSPEDALIERO-UNIVERSITARIA DI BOLOGNA IRCCS POLICLINICO DI S. ORSOLA
T19/IOA29	COMUNICAZIONE ALL'UTENZA: MISURE PER IL RISPETTO DEI DIRITTI DEGLI INTERESSATI
T21/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI RELATIVAMENTE A RICHIESTE DI ACCESSO A DOCUMENTAZIONE SANITARIA
T22/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI PER L'UTILIZZO DELLA FIRMA ELETTRONICA AVANZATA (FEA) NELL'AMBITO DEL PROCESSO DI SOTTOSCRIZIONE DEL DOCUMENTO DI CONSENSO INFORMATO AL TRATTAMENTO SANITARIO
T25/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 13 del Regolamento (UE) 2016/679 - Gestione dei dati personali nell'ambito della procedura di segnalazione condotte illecite (Whistleblowing) (art. 54-bis D.lgs. n. 165/2001 s.m.i.)
T26/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI - PROCEDURE CONCORSUALI E SELETTIVE
T27/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - Progetto Care4Today/APP Chirurgia Toracica IRCCS Bologna
T28/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - APP EASY HOSPITAL
T29/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI - EROGAZIONE E GESTIONE DELLE PRESTAZIONI SANITARIE IN TELE MEDICINA
T30/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI CONSEGNA ON-LINE DI REFERTI E IMMAGINI DIAGNOSTICHE ATTRAVERSO IL PORTALE WEB REGIONALE
T33/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI - Iscrizione alla Sezione "Anagrafe Ricercatori" del "Workflow della Ricerca" - Ministero della Salute
T34/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - Progetto PKU Connect
T35/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI - Applicazione MAppER (Mani App Emilia-Romagna)
T36/IOA29	INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER INDAGINI DI CUSTOMER SATISFACTION TRAMITE REDCap
T37/IOA29	INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI - Sistema di Segnalazione delle Malattie Infettive (PREMAL)
T38/IOA29	INFORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - Reti di riferimento europee (European Reference Networks, ERN) per le malattie rare

Tutta la modulistica è disponibile nell'area documentazione aziendale e nella specifica area Privacy (https://intranet.aosp.bo.it/content/la-privacy-azienda) del Portale Aziendale.