

REGOLAMENTO UNICO PER IL TRATTAMENTO DEI DATI PERSONALI NELLE AZIENDE SANITARIE DELLA PROVINCIA DI FERRARA

Sommario

Art. 1. Principi generali e ambito di applicazione.....	1
Art. 2. Definizioni e principi generali del trattamento dei dati.	2
Art. 3. Titolare e responsabili del trattamento.....	2
Art. 4. Referenti Interni del trattamento.....	3
Art. 5. Referente dell'U.O. ICT.	5
Art. 6. Referente dell'U.O.C. Ingegneria Clinica.	6
Art. 7. Autorizzazione al trattamento.....	7
Art. 8. Modalità di raccolta e requisiti dei dati.....	8
Art. 9. I diritti dell'interessato.....	9
Art. 10. Informazioni agli interessati.....	9
Art. 11. Ricerca medica, biomedica, epidemiologia e sperimentazioni cliniche.....	10
Art. 12. Cartelle cliniche.....	11
Art. 13. Dati genetici.....	12
Art. 14. Telemedicina.....	12
Art. 15. Misure di sicurezza.....	13
Art. 16. Misure di sicurezza particolari.....	15
Art. 17. Misure per la riconoscibilità del personale.	16
Art. 18. Comunicazione dei dati sanitari.	16
Art. 19. Diffusione dei dati particolari o giudiziari.....	17
Art. 20. Registro delle attività di trattamento.	17
Art. 21. Violazione dei dati personali.....	17
Art. 22. Attività di monitoraggio.....	17
Art. 23. Consulenza del Responsabile della Protezione di Dati.....	18

Art. 1. Principi generali e ambito di applicazione.

1. Alla luce dell'assetto dipartimentale dell'organizzazione sanitaria provinciale, di cui alle deliberazioni AUSL n. 68 del 16/03/2023 e OSPFE n. 84 del 16/03/2023, integrate dalle deliberazioni AUSL n. 212 del 4/11/2025 e OSPFE n. 196 del 4/11/2025, le **Azienda Ospedaliero-Universitaria Arcispedale Sant'Anna di Ferrara** (di seguito, "OspFE") e **Azienda USL di Ferrara** (di seguito, "AusIFE") sono Contitolari dei trattamenti di dati svolti dalle Aziende stesse.

2. I predetti Contitolari sono i soggetti che, secondo le ripartizioni di cui all'Accordo di contitolarità stipulato ai sensi dell'art. 26 del Regolamento UE 679/2016 (di seguito, "RGPD") garantiscono che i trattamenti di dati personali svolti nelle Aziende si svolgano 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.

3. Le Aziende perseguono altresì i principi di semplificazione, armonizzazione ed efficacia delle modalità previste per l'esercizio dei diritti richiamati al comma 2, nonché per l'adempimento degli obblighi imposti sul titolare del trattamento dal RGPD e dal d.lgs. 30 giugno 2003 n. 196 (di seguito, "Codice").

4. Il presente Regolamento disciplina il sistema di gestione dei dati personali all'interno delle Aziende e rappresenta lo strumento con il quale le stesse specificano i compiti e le regole alle quali devono attenersi le strutture aziendali in materia di trattamento dei dati, fermo

restando quanto dispongono il RGPD, il Codice e le altre norme in materia di protezione dei dati, e si applica a tutti i trattamenti ivi effettuati.

5. Le Aziende, singolarmente o congiuntamente, anche su proposta del DPO, possono adottare Linee Guida, Disciplinari e/o Istruzioni Operative che dovranno essere inserite nella sezione Privacy del sito internet istituzionale, e che i Referenti Interni, i Responsabili del trattamento designati e tutti i soggetti autorizzati al trattamento sono tenuti a rispettare.

Art. 2. Definizioni e principi generali del trattamento dei dati.

1. Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 4 del RGPD, di cui all'art. 2-ter del Codice e, comunque, si intende per:

- a) **"RGPD"**: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- b) **"Codice"**: il decreto legislativo 30 giugno 2003 n. 196 rubricato *"Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE"*;
- c) **"DPO"**: il Responsabile della Protezione dei Dati designato dall'Azienda ai sensi degli articoli 37, 38 e 39 del Regolamento UE, contattabile all'indirizzo PEO dpo@ausl.fe.it;
- d) **Referente Interno**: il soggetto indicato nell'articolo 4, comma 1, del presente regolamento;
- e) **Soggetti Autorizzati al trattamento**: i dipendenti, i collaboratori, e qualsiasi soggetto di cui all'art. 2-*quaterdecies* del Codice autorizzato al trattamento dei dati ai sensi dell'art. 7 del presente regolamento;
- f) **"Garante"**: il Garante per la protezione dei dati personali di cui all'art. 2-*bis* del Codice

2. L'Azienda procede al trattamento dei dati personali nel rispetto delle disposizioni previste dall'articolo 5 del RGPD, anche tramite la formazione dei soggetti autorizzati al trattamento.

3. I sistemi informatici, i sistemi informativi, i programmi per elaboratore e, in genere, gli applicativi e i dispositivi in genere in uso presso le Aziende devono essere configurati riducendo al minimo l'utilizzo di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi, dati non aventi natura particolare od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 3. Titolare e responsabili del trattamento.

1. I titolari del trattamento, anche relativamente al trattamento dei dati svolto nel contesto dell'attività libero-professionale intramuraria, sono, rispettivamente, l'**Azienda Ospedaliero-universitaria Arcispedale Sant'Anna di Ferrara** e l'**Azienda USL di Ferrara**, che esercitano i poteri propri del titolare per mezzo del Legale Rappresentante dell'Ente, il quale può agire d'ufficio o su impulso e/o proposta dei singoli Referenti Privacy e/o del DPO.

2. Al titolare competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza e, comunque, fermi gli altri obblighi derivanti dall'applicazione del RGPD e dal Codice, designa i responsabili del trattamento e ha, altresì, l'obbligo di vigilare sulla puntuale osservanza da parte dei responsabili e dei soggetti autorizzati delle disposizioni in materia di trattamento dei dati personali.

3. L'Azienda, singolarmente o congiuntamente all'altra, con delibera del Direttore Generale, fermo restando la delega generale di cui al successivo comma 4, nel rispetto delle disposizioni di cui all'articolo 28 del RGPD, designa responsabili del trattamento, con apposita clausola inserita nel contratto principale o con atto separato che dovrà essere allegato al contratto stesso, le persone fisiche e giuridiche delle quali si avvale per il trattamento dei dati, ivi compresi i soggetti che procedono al trattamento nel contesto di un servizio concesso in appalto, contratto e/o convenzione, solo se presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD e garantisca la tutela dei diritti dell'interessato.

4. Il potere di designazione del responsabile del trattamento compete, in ogni caso, anche al dirigente dotato del potere di sottoscrizione del contratto di appalto, o dell'atto con il quale viene conferito il servizio, il quale, ai fini della designazione, dovrà attenersi alle istruzioni preventivamente fornite dal DPO.

Art. 4. Referenti Interni del trattamento.

1. I Direttori dei **Dipartimenti**, delle **Strutture Complesse**, **Strutture Semplici**, **Programmi**, aggregate nei **Dipartimenti ad Attività Integrata** e nei **Dipartimenti dei Servizi Trasversali e di Supporto**, e nei **Coordinamenti** sono individuati quali **Referenti Interni** del trattamento dei dati, ai quali è altresì conferito il compito di gestire i trattamenti dei dati svolti nell'ambito delle strutture di riferimento.

2. È comunque facoltà del titolare, anche con atto generale applicabile a casi omogenei, nominare ulteriori Referenti rispetto a quelli indicati nel comma precedente, qualora lo richiedessero particolari esigenze organizzative aziendali, o particolari caratteristiche di specifici trattamenti di dati.

3. Il Referente Interno, per quanto di propria competenza, e comunque attenendosi alle istruzioni del Titolare e/o del DPO, nonché alle indicazioni del Referente Interno della Struttura superiore, deve osservare e fare osservare:

- a) le direttive aziendali, comunque denominate (Disciplinare, Linee Guida, Istruzioni, Istruzioni operative, note, circolari, ecc.) in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, dal DPO, dal Referente dell'UOC Affari Istituzionali, legali e assicurativo e, per quanto di loro competenza, dal Referente UOC ICT e dal Referente UOC Ingegneria Clinica;
- b) le istruzioni di carattere generale impartite dal Titolare a tutti i soggetti autorizzati al trattamento dei dati personali; (c) eventuali ulteriori specifiche istruzioni, predisposte dal Titolare o dai Referenti Interni, in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- c) garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure aziendali da parte dei soggetti autorizzati al trattamento;
- d) fornire indicazioni e sorvegliare affinché nella struttura di sua competenza non vengano svolti trattamenti autonomi di dati e affinché non vengano trattati dati personali per finalità diverse da quelle per le quali sono stati raccolti e successivamente trattati.
- e) verificare la liceità e la correttezza dei trattamenti effettuati, anche attraverso controlli periodici, e verificare la qualità e la quantità dei dati oggetto dei trattamenti di competenza con specifico riferimento ai requisiti di esattezza, aggiornamento, pertinenza, non eccedenza rispetto alle finalità del trattamento;
- f) designare i responsabili del trattamento di cui all'art. 28 del RGPD, stipulando il contratto o l'atto giuridico di cui al medesimo art. 28, par. 3 e 4, eventualmente anche previa acquisizione del parere del DPO;
- g) fornire indicazioni e dare disposizioni, anche in accordo o su richiesta o previo parere del DPO, per l'adeguamento alle misure di sicurezza organizzative di cui all'art. 32 del RGPD, anche chiedendo o provvedendo all'acquisto delle strumentazioni ritenute necessarie dal medesimo DPO;
- h) porre in atto, all'interno della propria struttura organizzativa, le procedure e le linee guida aziendali per la corretta gestione dei dati assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori, ...) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt. 13 e 14 del RGPD;
- i) provvedere alla designazione dei soggetti autorizzati al trattamento dei dati personali per i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro, incarico e/o collaborazione, come previsto dal successivo art. 7, commi 3, 4 e 5 (a titolo non esaustivo: laureati frequentatori, tirocinanti, frequentatori volontari, ecc.);
- j) vigilare sulla conformità dell'operato dei soggetti autorizzati alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto e segnalando all'Ufficio Procedimenti Disciplinari i soggetti autorizzati che, nel trattamento dei dati, violano la normativa eurounitaria, italiana e aziendale;
- k) avvisare il Titolare, ai fini dell'adozione dei provvedimenti e/o della comunicazione al Garante previste dagli articoli di cui all'art. 2-ter, e 2-sexies, laddove ritenga di dover procedere a trattamenti di dati, ivi compresa la comunicazione o la diffusione degli stessi, che non siano previste dal diritto dell'Unione Europea, dalla legge o da regolamenti.
- l) procedere, laddove ritenuto necessario e/o opportuno, da lui medesimo o dal DPO, e salvo che la stessa non sia di competenza del Referente dell'UO ICT e/o dell'U.O.C. Ingegneria Clinica, alla valutazione di impatto di cui all'articolo 35 del RGPD, sottoponendola poi alla consulenza del medesimo DPO, e avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del RGPD;
- m) informare il titolare, secondo le modalità previste dalla Linee Guida aziendali in materia, dell'avvenuta violazione dei dati personali di cui all'articolo 33 del RGPD, e collaborare alla predisposizione della notifica al Garante, alla comunicazione agli interessati, e alla corretta compilazione del Registro delle Violazioni;

- n) comunicare al Referente ICT e al DPO le attività di trattamento in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti e, comunque, collabora con gli stessi ai fini dell'aggiornamento del Registro delle attività di trattamento aziendale;
- o) dare previo avviso al Direttore dell' UOC Ricerca e Sviluppo Organizzativo, laddove debba procedere al trattamento dei dati particolari per finalità di ricerca scientifica, al fine di verificare il rispetto delle disposizioni in materia di trattamento dei dati per tali finalità, rispettando le indicazioni del medesimo e/o di eventuali Linee Guida, Disciplinari e/o istruzioni operative in materia.
- p) provvedere ad ogni altro atto o adempimento necessario per l'applicazione, ai trattamenti di dati dell'Azienda e/o delle Aziende, del RGPD, del Codice, e/o di ogni altra norma in materia, eurounitaria e nazionale, anche in relazione alle indicazioni del Titolare o del DPO, collaborando a tal fine con quest'ultimo e con il Garante per la protezione dei dati o con la diversa autorità di controllo competente e/o coinvolta;
- q) provvedere ad ogni adempimento gli sia indicato dal DPO, fermo restando la possibilità di rivolgersi al Titolare laddove non condivida o non ritenga di adempiere alle indicazioni del DPO medesimo;
- r) segnalare con tempestività al Titolare e/o al DPO eventuali problemi relativi all'applicazione della disciplina di cui al RGPD e al Codice riscontrati nell'esercizio delle attività di competenza.

Art. 5. Referente dell'UOC ICT.

1. Il **Direttore dell'UOC ICT**, oltre ai compiti di cui al precedente articolo 4:
 - a) sovrintende le risorse del sistema informatico centralizzato (software dipartimentali e trasversali) e ne consente l'utilizzo a tutti i responsabili e i soggetti autorizzati che ne abbiano titolo, mediante l'adozione delle misure di sicurezza tecniche di cui all'art. 32 del RGPD;
 - b) garantisce la gestione e manutenzione degli strumenti elettronici aziendali;
 - c) garantisce la protezione dei dispositivi e dei programmi contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare secondo la cadenza ritenuta necessaria in conformità all'art. 32 del RGPD;
 - d) garantisce gli aggiornamenti periodici, almeno con cadenza semestrale, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti;
 - e) garantisce il salvataggio dei dati con frequenza almeno quotidiana e, comunque, in modo tale da garantire tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - f) adotta idonee misure che assicurino l'integrità e la disponibilità dei dati;
 - g) adotta idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;

- h) in caso di trattamento di dati particolari, predispone misure di pseudonimizzazione e cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
 - i) predispone misure di sicurezza finalizzate a garantire che la dismissione e la distruzione dei supporti che contengono dati personali avvenga nel rispetto del provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, pubblicato in G.U. n. 287 del 9 dicembre 2008 e successive eventuali modifiche e/o integrazioni e/o nuove versioni;
 - j) redige, conserva e aggiorna il Registro delle attività del trattamento, eventualmente previa consultazione con il DPO, anche dando o chiedendo indicazioni ai Referenti per la trasmissione delle informazioni necessarie per l'aggiornamento del Registro stesso;
 - k) procede, relativamente alle attività di trattamento automatizzate, laddove ritenuto necessario e/o opportuno, da lui medesimo o dal DPO, e salvo che la stessa non sia di competenza del Referente dell'U.O.C. Ingegneria Clinica, alla valutazione di impatto di cui all'articolo 35 del RGPD, sottoponendola poi alla consulenza del medesimo DPO, ed avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del RGPD;
 - l) procede alla individuazione degli amministratori di sistema e agli altri adempimenti previsto nel provvedimento del Garante recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"* (G.U. n. 300 del 24 dicembre 2008) e successive modifiche ed integrazioni;
 - m) implementa ogni misura finalizzata al rispetto del Disciplinare sull'uso dei Servizi Informatici e informativi Aziendali.
2. Tenuto conto che l'accesso ai dati e alle procedure aziendali è consentito, per necessità di operatività e sicurezza dei sistemi, ai soli soggetti autorizzati dell'UOC ICT, il Referente dell'UOC ICT procede all'individuazione del preposto all'intervento sui sistemi e procedure aziendali in assenza dei soggetti autorizzati al trattamento, nel rispetto del Disciplinare sull'uso dei Servizi Informatici Aziendali.

Art. 6. Referente dell'U.O.C. Ingegneria Clinica.

1. Il Direttore dell'UOC Ingegneria Clinica, oltre ai compiti di cui al precedente articolo 3:
 - a) sovrintende le risorse dei programmi per elaboratore qualificati e/o certificati Dispositivi Medici (in breve DM) e ne consente l'utilizzo a tutti i responsabili e i soggetti autorizzati che ne abbiano titolo, mediante l'adozione delle misure di sicurezza tecniche di cui all'art. 32 del RGPD;
 - b) garantisce la gestione e manutenzione dei programmi DM, siano essi integrati nelle tecnologie biomediche, accessori di tecnologie biomediche oppure autonomi e indipendenti da qualsivoglia tecnologia (cosiddetti stand alone);
 - c) garantisce la protezione dei programmi DM contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare secondo la cadenza ritenuta necessaria in conformità all'art. 32 del RGPD;

- d) garantisce gli aggiornamenti periodici dei programmi DM al fine di prevenirne la vulnerabilità secondo la periodicità ritenuta necessaria in conformità all'art. 32 del RGPD;
 - e) impartisce istruzioni organizzative e tecniche che prevedano il salvataggio dei dati con la periodicità ritenuta necessaria in conformità all'art. 32 del RGPD, al fine di garantire tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - f) promuove l'adozione di idonee misure che assicurino l'integrità e la disponibilità dei dati;
 - g) promuove l'adozione di idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e comunque non superiori a tre giorni;
 - h) predispone misure di sicurezza finalizzate a garantire che la dismissione e la distruzione dei supporti che contengono dati personali avvenga nel rispetto del provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, pubblicato in G.U. n. 287 del 9 dicembre 2008;
 - i) in caso di trattamento di dati particolari predispone misure di pseudonimizzazione e cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
 - j) procede, laddove ritenuto necessario e/o opportuno da lui medesimo, o dal DPO, relativamente ai trattamenti di dati svolti nell'ambito dei programmi DM, alla valutazione di impatto di cui all'articolo 35 del RGPD, avvalendosi della consulenza del medesimo DPO, avvisando il Titolare laddove derivi la necessità di procedere alla consultazione preventiva di cui all'articolo 36 del RGPD;
 - k) procede alla individuazione degli amministratori di sistema e agli altri adempimenti previsto nel provvedimento del Garante recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 24 dicembre 2008) e successive modifiche ed integrazioni;
 - l) collabora con il Referente ICT alla redazione e all'aggiornamento del Registro delle attività del trattamento per le attività di trattamento di propria competenza;
2. L'individuazione delle misure di sicurezza è svolta, unitamente al Referente ICT, in relazione ai criteri individuati dall'Agenzia per l'Italia Digitale e, comunque, in conformità a quanto disposto dall'art. 32 del RGPD.
3. La tipologia di dati trattati e le modalità del trattamento sono identificati mediante la compilazione di specifica modulistica all'atto dell'ingresso di una tecnologia biomedica o programma DM.

Art. 7. Autorizzazione al trattamento.

1. I dipendenti, i collaboratori e i consulenti, a qualsiasi titolo, delle Aziende, sono autorizzati al trattamento dei dati personali svolti nelle strutture alle quali sono preposti e, comunque, relativamente al personale sanitario, al trattamento dei dati particolari relativi agli interessati che hanno in cura oppure relativi agli interessati per i quali, o a favore dei quali, viene richiesta una specifica prestazione.
2. La preposizione dei soggetti di cui al comma 1 alle singole strutture aziendali è effettuata dall'UOC Gestione Giuridica ed economica delle Risorse Umane all'atto dell'assunzione o del trasferimento e/o mutamento di mansioni, e tale preposizione costituisce

atto autorizzativo al relativo trattamento ai sensi degli articoli 29 del RGPD e 2-*quaterdecies* del Codice.

3. I medici in formazione specialistica, gli studenti dei corsi di studi di livello superiore e/o universitario, i tirocinanti, i frequentatori, i titolari di borsa di studio, di assegno di ricerca e i dottorandi di ricerca ammessi a svolgere attività nelle strutture ospedaliere ai sensi dei regolamenti aziendali in materia, sono autorizzati al trattamento dei dati personali svolti nell'ambito della struttura alla quale sono preposti.

4. La preposizione dei soggetti di cui al comma 3 alle singole strutture aziendali è effettuata dal Referente Interno della struttura di afferenza all'atto del primo ingresso nella struttura stessa, e tale preposizione costituisce atto autorizzativo al relativo trattamento ai sensi degli articoli 29 del RGPD e 2-*quaterdecies* del Codice.

5. La preposizione dei singoli soggetti autorizzati avviene mediante atto scritto, anche contenuto nel contratto, convenzione, atto unilaterale, o altro atto giuridico che regola il rapporto tra le Aziende e il soggetto autorizzato, o anche in forma automatizzata, contenente l'autorizzazione al trattamento e l'informativa sull'obbligo, per il singolo soggetto autorizzato, di

- a. garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza;
- b. attenersi alle istruzioni impartite dal Titolare, dal DPO e dal Referente Interno;
- c. effettuare il trattamento in ottemperanza ai principi di liceità, correttezza, pertinenza e non eccedenza dei trattamenti effettuati
- d. trattare i dati per le sole finalità strettamente inerenti all'oggetto dell'incarico;
- e. non comunicare i dati trattati a soggetti ai quali la comunicazione non è consentita;
- f. prendere visione e rispettare le istruzioni, i Regolamenti aziendali, i Disciplinari, le Linee Guida e, in genere, le istruzioni operative in materia di trattamento dei dati personali resigli noti e/o pubblicati nella Sezione Privacy del sito istituzionale delle Azienda;
- g. partecipare agli incontri e alle iniziative di formazione organizzati periodicamente e/o indicati dai Referenti Interni e/o dall'UOC Formazione.

6. La normativa aziendale in materia di protezione dei dati è pubblicata nella Sezione Privacy del sito internet istituzionale delle Aziende che, relativamente alle disposizioni in materia di protezione dei dati, assume il valore di affissione di cui all'art. 7, comma 1, della legge 20 maggio 1970 n. 300.

Art. 8. Modalità di raccolta e requisiti dei dati.

1. I Referenti Interni e i soggetti autorizzati al trattamento sono tenuti a trattare i dati nel rispetto delle disposizioni di cui all'articolo 5 del RGPD (*"Principi applicabili al trattamento di dati personali"*).

2. I Referenti Interni e i soggetti autorizzati sono tenuti a raccogliere e registrare i dati da trattare in forma automatizzata attraverso gli strumenti elettronici messi a disposizione dall'azienda, invitando il paziente e/o l'utente ad esibire la tessera sanitaria europea, anche nel caso in cui l'erogazione della prestazione sanitaria sia preceduta dalla prenotazione.

3. Ciascun soggetto autorizzato è tenuto a identificare i pazienti e/o gli utenti al momento dell'erogazione di ciascuna prestazione senza trattenere copia del documento esibito per tale identificazione, salvo che sia previsto da norme di legge o di regolamento.

Art. 9. I diritti dell'interessato.

1. L'adempimento delle richieste formulate dall'interessato ai sensi degli articoli 12 e seguenti del RGPD, e il riscontro agli interessati stessi, avviene nei termini e secondo le modalità determinate dalle Linee Guida adottate dal Direttore dell'UOC Comunicazione, Accoglienza, Partecipazione
2. In ogni caso è istituito, presso l'UOC Comunicazione, Accoglienza, Partecipazione, il Registro dei Diritti dell'Interessato, nel quale verranno annotate la data di ricezione dell'istanza, il numero di protocollo assegnato, il nominativo dell'interessato e dell'istanza (se diverso dal primo), la descrizione dell'istanza, la struttura organizzativa e le eventuali banche dati coinvolte, l'azione intrapresa, la data e il numero di protocollo del riscontro all'interessato, nonché eventuali note o commenti, nelle quali verrà indicato l'eventuale parere del DPO.
3. L'UOC Comunicazione, Accoglienza, Partecipazione che abbia dubbi sulle modalità per provvedere al riscontro all'interessato potrà avvalersi della consulenza del DPO contattandolo mediante il canale di contatto **dpo@ausl.fe.it**.
4. L'interessato che eserciti i diritti previsti dagli articoli 12 e seguenti del RGPD dovrà essere identificato ai sensi dell'art. 65 del d.lgs. 7 marzo 2005 n. 82. La persona che agisce per conto dell'interessato esibisce o allega copia della procura o di delega sottoscritta dall'interessato nelle stesse forme di cui al periodo precedente o, comunque, nelle forme di cui all'articolo 38 del DPR 28 dicembre 2000, n. 445.
5. L'eventuale richiesta verbale da parte dell'interessato dovrà essere annotata a cura del Referente e/o del personale autorizzato.
6. Il personale autorizzato che riceva una richiesta di cui al presente articolo è tenuto a trasmetterla con immediatezza al Direttore dell'UOC Comunicazione, Accoglienza, Partecipazione.

Art. 10. Informazioni agli interessati.

1. I Referenti Interni sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del RGPD nel rispetto delle indicazioni fornite dal Titolare e/o dal DPO.
2. Fermo restando quanto previsto al comma precedente, le predette informazioni sono fornite attraverso il modello predisposto dall'Azienda, eventualmente anche diversificandole in relazione alle particolarità di taluni trattamenti:
 - a. mediante affissione nei punti della struttura ben visibili dall'utenza (c.d. informativa di primo livello), nel rispetto di quanto previsto al comma 3;
 - b. mediante pubblicazione nella Sezione Privacy del sito Internet delle aziende
 - c. mediante indicazione, nei fogli di prenotazione, dell'indirizzo del sito dove è reperibile l'informativa completa;
 - d. mediante rinvio, inserito nella modulistica che viene sottoposta all'interessato al momento del ricovero, alla Sezione Privacy dei siti internet aziendali.
3. Le informazioni da rendere ai pazienti ai sensi del precedente comma 2, lett. a) devono essere riportate in una cartellonistica predisposta dall'Area Comunicazione con la consulenza del DPO che riporti le informazioni essenziali dei trattamenti svolti (quantomeno comprensive dell'elenco delle categorie di dati trattati, dell'elenco delle finalità del trattamento perseguite, e

dei dati di contatto dei titolari e del DPO) e il codice QR della pagina internet nella quale è possibile leggere e/o scaricare l'informativa completa (c.d. informativa di secondo livello).

4. Le informazioni da rendere per i fini di cui all'articolo 6, par. 2, lett. b) del RGDP (trattamento necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso) e all'art. 6, par. 2, lett. b) del medesimo RGPD (trattamento 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) devono essere inserite nei relativi atti contrattuali e, laddove il rapporto sia soggetto a procedure concorsuali, devono essere indicate nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.

5. Inoltre, le predette informazioni dovranno essere rese:

- a) in materia di attività dell'URP, consegnando o inviando la specifica modulistica messa a disposizione dall'Azienda oppure inserendo le informazioni nella modulistica, cartacea o elettronica, messa a disposizione degli interessati;
- b) in materia di recupero crediti del dipendente a seguito di infortuni in itinere o infermità causata da terzi, consegnando o inviando la specifica modulistica messa a disposizione dall'Azienda oppure inserendo le informazioni nella modulistica, cartacea o elettronica, messa a disposizione degli interessati;
- c) in materia di responsabilità civile di terzi, inviando la specifica modulistica messa a disposizione dall'Azienda unitamente alla comunicazione dell'apertura del sinistro;
- d) in materia di valutazione delle necessità assistenziali nell'ambito delle attività socio-sanitarie integrate, consegnando la specifica modulistica messa a disposizione dall'Azienda unitamente alla consegna dei moduli messi a disposizione per la segnalazione oppure inserendo le informazioni nella modulistica, cartacea o elettronica, messa a disposizione degli interessati.

6. Il Referente Interno che procede ad attività di trattamento per le quali ritiene necessario prevedere specifiche modalità per fornire le informazioni di cui agli articoli 13 e 14 del RGPD, ai fini delle informazioni da rendere e per determinare le modalità per fornirle è tenuto ad avvalersi della consulenza del DPO.

Art. 11. Ricerca medica, biomedica, epidemiologia e sperimentazioni cliniche.

1. Le attività di trattamento connesse alle ricerche mediche, biomediche, epidemiologiche e alle sperimentazioni cliniche avvengono nel rispetto dei provvedimenti del Garante n. 515 del 19 dicembre 2019 recante *"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"* e n. 146 del 5 giugno 2019, recante *"Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"* e di ogni eventuale provvedimento successivo.

2. In particolare, dette attività vengono svolte sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, allegando e documentando che il trattamento stesso e l'eventuale utilizzo dei campioni biologici vengano effettuati per idonei ed effettivi scopi scientifici.

3. Il progetto di cui al comma precedente deve contenere:

- a) le specifiche misure da adottare nel trattamento di dati personali, al fine di garantire il rispetto delle regole deontologiche e della normativa in materia di protezione dei dati personali; nel caso in cui lo studio concerna i dati genetici, le predette misure devono estendersi a quelle necessarie riguardanti la custodia e la sicurezza dei dati e dei campioni biologici;
 - b) l'individuazione degli eventuali responsabili del trattamento designati o designandi, nominativamente indicati, con indicazione dei loro dati di contatto;
 - c) nel caso in cui la base giuridica del trattamento non sia il consenso dell'interessato, l'indicazione delle particolari ed eccezionali ragioni per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o pregiudicare gravemente il conseguimento delle finalità della ricerca;
 - d) le dichiarazioni di impegno a conformarsi alle regole deontologiche con evidenza che analoga dichiarazione dovrà poi essere sottoscritta anche dai soggetti –ricercatori, responsabili e soggetti autorizzati al trattamento– che fossero coinvolti nel prosieguo della ricerca, conservata nelle stesse forme e nei medesimi termini del progetto;
 - e) relativamente agli studi che abbiano ad oggetto dati genetici e campioni biologici, l'indicazione dell'origine, della natura, delle modalità di prelievo e/o di conservazione dei campioni biologici nonché l'indicazione delle misure adottate per garantire la volontarietà del conferimento del materiale biologico da parte dell'interessato.
4. Fermo restando l'applicazione degli articoli 104 e seguenti del Codice e dei provvedimenti del Garante in materia, le informazioni di cui agli articoli 13 e 14 del RGPD devono essere fornite secondo le modalità indicate dal DPO, in modo tale da mettere in grado gli interessati di distinguere le attività di ricerca da quelle di tutela della salute. A tal fine, in particolare, il modulo contenente le predette informazioni, così come il modulo da sottoporre al paziente per la prestazione del consenso al trattamento dei suoi dati per finalità di ricerca e sperimentazione, laddove necessario, deve essere predisposto separatamente da quello relativo alla partecipazione alla ricerca.
5. I dati che devono essere comunicati ai promotori della ricerca e/o alle aziende farmaceutiche devono essere resi anonimi o, comunque, pseudoanonimizzati. In ogni caso, l'accesso delle aziende farmaceutiche alla documentazione medica è subordinato al rispetto delle disposizioni concernenti la responsabilità e la titolarità del trattamento dei dati personali, nonché delle disposizioni previste dalle norme regolanti il trattamento dei dati sanitari, dal D.M. 18.3.1998 e nella Carta Europea dei Diritti dell'Uomo, nei codici della deontologia medica nazionale e internazionale e in particolare nella Dichiarazioni di Helsinki e nella Convenzione di Oviedo.
6. Ai fini di cui ai precedenti commi il Referente Interno dell'UOC Ricerca e sviluppo organizzativo cura che, all'esito del parere favorevole del Comitato Etico, vengano autorizzati i soli studi che rispettino i predetti commi da 1 a 5 e che lo studio sia soggetto alla valutazione di impatto e, nei casi previsti dalla normativa vigente, alla consultazione preventiva.

Art. 12. Cartelle cliniche.

1. Le finalità perseguite dall'art. 92 del Codice sono garantite, in ciascuna struttura, dal singolo Referente Interno.

2. In considerazione di quanto previsto dall'art. 92, comma 2, del Codice, in caso di richiesta di cartella clinica e/o di altri documenti sanitari ai fini della difesa nel processo civile, o ai sensi dell'art. 391-bis del codice di procedura penale, ai fini della valutazione dell'ammissibilità e fondatezza della richiesta, il richiedente è tenuto specificare le ragioni per le quali ritiene che le informazioni contenute nei documenti richiesti siano rilevanti per la finalità difensiva, anche mediante la produzione di documenti che ritenga all'uopo giustificativi. Laddove la richiesta sia presentata dal difensore, quest'ultimo è tenuto a produrre copia della procura speciale, autenticata nelle forme di cui all'art. 65 del d.lgs. 82/2005 o nelle forme di cui all'art. 38, comma 3, del DPR 445/2000, oppure a documentare la sua qualità, anche mediante dichiarazione sostitutiva di certificazione che individui gli estremi del procedimento nel quale svolge tale funzione.

Art. 13. Dati genetici.

1. Il trattamento dei dati genetici e dei campioni biologici da chiunque effettuato è consentito nei soli casi previsti dall'articolo 9, paragrafo 2 del RGPD e dalle misure di garanzia approvate dal Garante per la protezione dei dati personali in attuazione dell'art. 2-septies del Codice e, comunque, è consentito esclusivamente all'interno di locali protetti e accessibili ai soli soggetti autorizzati al trattamento.
2. Il trasporto dei dati e dei campioni biologici all'esterno dei locali riservati al loro trattamento deve avvenire, esclusivamente applicando tecniche di pseudoanonimizzazione, e comunque in contenitori muniti di serratura o dispositivi equipollenti.
3. Il trasferimento e la comunicazione dei dati in formato elettronico deve essere cifrato o, comunque, può essere effettuato nel rispetto delle disposizioni date dal Referente ICT, previo parere del DPO.

Art. 14. Telemedicina.

4. L'Azienda promuove e attua la Telemedicina quale modalità attraverso la quale erogare a distanza prestazioni sanitarie come la visita, il consulto, il monitoraggio di parametri e l'assistenza.
5. In particolare, 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 modalità telematica, anche per la presa in carico domiciliare secondo i PDTA delle patologie croniche.
6. 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 e accelerare l'assistenza sanitaria, anche nel rispetto del principio di economicità e funzionalità dell'azione amministrativa, e aiutare i cittadini ad accedere ed ottenere le migliori cure possibili.
7. Tale modalità può interessare tanto la pratica clinica diagnostica, assistenziale e riabilitativa quanto l'ambito dell'innovazione, ricerca scientifica e sviluppo.
8. L'Azienda esegue il trattamento dei dati personali effettuato tramite gli strumenti acquisiti nella piena osservanza delle normative europee e nazionali e, comunque, mettendo in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del RGPD e tutelare i diritti degli interessati.

9. L'Azienda mette inoltre in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento e, comunque, procede alla valutazione di impatto nei termini e secondo le modalità previste dal RGPD.

10. In ogni caso l'Azienda procede ai trattamenti previsti dai precedenti commi nel rispetto delle eventuali indicazioni del DPO.

Art. 15. Misure di sicurezza.

1. I Referenti Interni e i soggetti autorizzati al trattamento sono tenuti:
 - a. a trattare i soli dati essenziali per svolgere l'attività istituzionale riducendo al minimo l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi, dati di natura meno invasiva od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
 - b. introdurre e controllare i dati in modo da ridurre al minimo i rischi di distruzione e perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla qualità della raccolta, tramite l'applicazione di misure di sicurezza adottate dall'UOC ICT, anche su parere del DPO, in conformità all'articolo 32 del RGPD ed anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, secondo le indicazioni impartite dall'UOC ICT.
2. I dati su supporto cartaceo dovranno essere conservati in luoghi e contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento, nel rispetto peraltro del principio della tutela della riservatezza di terzi.
3. Il personale autorizzato può accedere ai soli dati la cui conoscenza sia direttamente necessaria per adempiere ai compiti assegnati.
4. Gli atti e i documenti devono essere conservati in archivi ad accesso selezionato e gli incaricati debbono conservarli e restituirli al termine delle operazioni effettuate.
5. Nel caso di trattamenti di dati particolari di cui agli articoli 9 e 10 del RGPD, oltre a quanto sopra previsto, devono essere osservate le seguenti modalità:
 - a. gli atti e documenti devono essere conservati in locali o contenitori muniti di serratura, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti dalle norme in materia di scarto degli atti d'archivio;
 - b. l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l'orario di chiusura degli archivi stessi.
6. Ciascun Referente Interno è tenuto a individuare e rappresentare all'UOC Economato e Gestione Contratti, l'insieme dei beni materiali necessari per garantire la sicurezza dei dati trattati su supporto cartaceo nelle proprie articolazioni di competenza.
7. Per ogni singolo trattamento di dati deve essere individuata la finalità e la compatibilità con i fini istituzionali. I trattamenti di dati raccolti e conservati per espressa disposizione normativa deve essere specificata la relativa fonte normativa
8. I Referenti Interni, anche mediante controlli periodici, sono tenuti a verificare costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al

rapporto e alla prestazione in corso, da instaurare o cessati, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.

9. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

10. Il trattamento dei dati, anche particolari, effettuato con strumenti elettronici è consentito solo previa adozione, da parte dell'U.O. ICT, le seguenti misure minime:

- a. autenticazione informatica, con le specifiche procedure di gestione delle credenziali di autenticazione;
- b. utilizzazione di un sistema di autorizzazione;
- c. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato e agli addetti alla gestione o alla manutenzione degli strumenti elettronici;
- d. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- e. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- f. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale.

11. È fatto divieto di utilizzo degli apparecchi fax. Laddove l'uso dei singoli apparecchi sia strettamente necessario, il Referente Interno ne informa il DPO che fornirà indicazioni per la trasmissione e la ricezione delle comunicazioni e affinché la relativa apparecchiatura sia collocata in un'area protetta e presidiata.

12. La trasmissione interna ed esterna di corrispondenza e di documentazione contenente dati particolari dovrà essere effettuata attraverso il servizio "cloud" aziendale o attraverso altri accorgimenti tecnici individuati dal Referente ICT, previo parere del DPO; in caso di impossibilità, nel caso sia strettamente necessario procedere alla trasmissione di corrispondenza o documentazione cartacea o, comunque, non elettronica, detta trasmissione dovrà essere effettuata necessariamente in busta chiusa e sigillata che riporti il nominativo del destinatario senza che all'esterno della busta sia apposte diciture o segni dai quali possa individuarsi il Servizio mittente.

13. I documenti cartacei che contengano dati personali e dei quali non sia imposta la conservazione devono essere smaltiti attraverso appositi distruggidocumenti o, se non disponibili, distruggendo fisicamente il supporto cartaceo in modo che ne sia impedita la ricostruzione.

14. La distruzione di ingenti quantità di documenti cartacei deve essere effettuata, in accordo con il Referente Interno, attraverso l'incarico ad esperti del settore (es. società di smaltimento rifiuti) che dovranno essere designati alla responsabilità del trattamento ai sensi dell'art. 28 del RGPD.

15. I documenti e, in genere, i beni smarriti che contengono dati personali dovranno essere gestiti sulla base di apposite Linee Guida adottate dal Direttore dell'UOC Comunicazione, Accoglienza, Partecipazione.

16. È vietato l'utilizzo di strumenti di messaggistica di terze parti (es: whatsapp, Messenger, Signal, Telegram, ecc.) per il trattamento, in qualsiasi forma, di dati personali di titolarità dell'Azienda. In applicazione di tale comma è vietata la comunicazione istantanea e/o la

costituzione di gruppi di comunicazione istantanea (es. gruppi whatsapp, gruppi telegram, ecc.) con interessati terzi (es. pazienti, utenti).

17. Fermo restando quanto previsto dal comma precedente, eventuali comunicazioni tra dipendenti e/o collaboratori dell'Azienda, così come l'eventuale partecipazione a gruppi di comunicazione istantanea (es. gruppi whatsapp), essendo effettuati per fini personali, ex art. 2, paragrafo 2, lett. c) del RGD, rientra nella libera iniziativa individuale e, pertanto, non è soggetta all'applicazione delle disposizioni del presente Regolamento. Resta fermo che l'eventuale invito a gruppi, laddove abbia ad oggetto dati personali del quale il dipendente ha il possesso per ragioni professionali, deve avvenire previo consenso del dipendente e/o mediante invito dello stesso attraverso funzionalità che non comporti, senza il suo intervento, la messa a disposizione dei suoi dati personali.

Art. 16. Misure di sicurezza particolari.

1. Le Aziende adottano, nell'organizzazione delle prestazioni e dei servizi, misure volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati particolari e di misure di sicurezza.

2. Tali misure comprendono:

- a. soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati che prescindano dalla individuazione nominativa, salvo che si tratti di minori, per i quali dovranno essere utilizzati accorgimenti che tengano conto del principio educativo;
- b. l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere e della situazione logistica;
- c. soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- d. cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
- e. il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati. In particolare, la dignità deve essere rispettata anche in relazione alle modalità di visita e di intervento sanitario effettuati alla presenza di studenti autorizzati. Durante tali prestazioni devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.
- f. la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione in urgenza o emergenza;
- g. la formale previsione di adeguate modalità per informare i terzi, in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni di volontà;

- h. la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei, un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- i. la sottoposizione dei soggetti autorizzati che non sono tenuti, per legge, al segreto professionale a regole di condotta analoghe al segreto professionale.

Art. 17. Misure per la riconoscibilità del personale.

1. L'attività delle Aziende si ispira ad alcuni principi, ritenuti essenziali per la realizzazione di un ospedale ad alto contenuto tecnologico ed assistenziale, tra cui si annoverano, in particolare:
 - a. 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;
 - b. 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.
2. Da tali principi deriva un "modello etico" che richiama con forza gli aspetti della trasparenza, della veridicità delle informazioni, anche e soprattutto nei rapporti tra gli operatori dell'Azienda 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.
3. Nell'ambito di tali principi, le Aziende adottano, nel complesso dei mezzi per la tutela degli interessi degli utenti, strumenti che garantiscano la riconoscibilità del personale operante all'interno delle Aziende, dipendente e non. In particolare, il tesserino di identificazione personale, nella parte esposta al pubblico, può riportare, quali elementi essenziali, la fotografia, il primo nome e/o un codice identificativo, la qualifica e/o il Servizio di appartenenza.

Art. 18. Comunicazione dei dati sanitari.

1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato, solo per il tramite di un medico designato dall'interessato o dalle Aziende. Il presente comma non si applica ai dati personali forniti in precedenza dall'interessato stesso.
2. Il responsabile del trattamento può autorizzare esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti, a rendere noti all'interessato o agli altri soggetti di cui al comma 1, nei casi ivi previsti, i dati personali idonei a rivelare lo stato di salute.

Art. 19. Diffusione dei dati particolari o giudiziari.

1. Fermo restando il generale divieto di diffusione di dati particolari, o di dati soggetti a particolare tutela, gli atti delle Aziende soggetti a pubblicazione, che riportino tali dati, devono essere pubblicati in forma di estratto, omettendo qualsiasi indicazione dei dati di cui è vietata, a qualsiasi titolo, la diffusione, nel rispetto delle eventuali indicazioni generali fornite dal DPO.

Art. 20. Registro delle attività di trattamento.

1. Il Registro delle attività di trattamento previsto dall'art. 30 del RGPD è conservato e aggiornato dal Referente ICT il quale ne trasmette copia al Direttore Generale e al DPO entro il 15 dicembre ogni anno.
2. I Referenti Interni sono tenuti ad informare il Referente ICT della modifica delle attività di trattamento rilevanti ai fini della compilazione del Registro, ivi compresa l'eventuale nomina dei Responsabili del trattamento.

Art. 21. Violazione dei dati personali.

1. I casi di violazione dei dati personali devono essere notificati al Garante, comunicati agli interessati e annotati nel Registro di cui al comma 2 a cura del Direttore dell'UOC Affari Istituzionali, Legali e assicurativo
2. Il Registro delle Violazioni è conservato e aggiornato dal Direttore dell'UOC Affari Istituzionali, legali e assicurativo il quale ne trasmette copia al Direttore Generale e al DPO entro il 15 dicembre di ogni anno.
3. Le attività di cui ai commi precedenti e, comunque, le procedure inerenti le modalità e i tempi della notifica e delle comunicazioni di cui agli articoli 33 e 34 del RGPD sono individuati nelle Linee Guida adottate dal Referente Interno degli Affari Istituzionali. Le predette Linee Guida sono pubblicate nella Sezione Privacy del sito Internet di ciascuna Azienda e sono obbligatorie per tutti i Referenti Interni e i soggetti autorizzati al trattamento.

Art. 22. Attività di monitoraggio.

1. Il titolare, mediante propri collaboratori all'uopo individuati, o il DPO, svolgono costante attività di monitoraggio e sorveglianza in ordine all'applicazione del RGPD, del Codice e delle norme aziendali in materia, ivi comprese le relative istruzioni applicative, sia nei confronti dei Responsabili sia nei confronti dei Referenti Interni. Il monitoraggio può essere eseguito anche tramite la richiesta di compilazione di un questionario.
2. Di tali attività vengono redatti verbali riassuntivi che riportano, tra l'altro, le indicazioni relative alle procedure suggerite al Responsabile e/o al Referente Interno.
3. Tale documentazione viene trasmessa in copia alla Direzione Strategica, al Referente Interno, alle strutture aziendali di riferimento per gli adempimenti di competenza e, se designato, al Responsabile del trattamento.

Art. 23. Consulenza del Responsabile della Protezione di Dati.

1. Il Titolare, i Referenti Interni e i soggetti autorizzati al trattamento, in caso di dubbi in materia di trattamento dei dati personali, o comunque in genere per ogni questione inerente il trattamento dei dati di titolarità delle Aziende, sono tenuti a richiedere consulenza al DPO, scrivendo al suo dato di contatto: dpo@ausl.fe.it.
2. I Referenti Interni e i soggetti autorizzati, in ogni caso, sono tenuti a conformarsi alle informative e ai pareri espressi dal DPO, salvo specifica deroga o indicazione contraria del Titolare.