
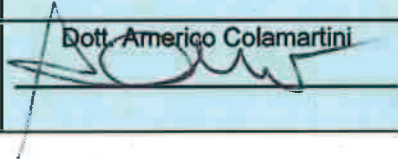





# Regolamento Videosorveglianza

| Redatto da   | Verificato da:   | Approvato da:  |
|--|--|--|
| Ing. Roberto Vespignani<br> | Dott. Americo Colamartini<br> | Dott. Giorgio Martelli<br> |

| N° Rev. | Data       | Paragrafi Modificati | Tipo – Natura Modifica  |
|---------|------------|----------------------|---|
| 1       | 23/12/2013 | Intero documento     | Revisione generale a seguito della modifica del piano di disposizione delle telecamere                                    |
| 2       | 04/07/2014 | Articolo 15          | Aggiunta planimetria della radioterapia di Ravenna  |
| 3       | 30/09/2019 | Intero documento     | Revisione generale a seguito della modifica del piano di disposizione delle telecamere e dell'introduzione del GDPR       |
| 4       | 01/02/2021 | Intero documento     | Revisione generale a seguito della modifica del piano di disposizione delle telecamere e aggiunta nuove telecamere triage |

## *Sommario*

|  |           |
|--|-----------|
| <b>Articolo 1: Finalità</b>  | <b>3</b>  |
| <b>Articolo 2: Definizioni</b>   | <b>3</b>  |
| <b>Articolo 3: Principi</b>  | <b>6</b>  |
| <b>Articolo 4: Ambito di applicazione</b>                                | <b>7</b>  |
| <b>Articolo 5: Soggetti</b>  | <b>7</b>  |
| <b>Articolo 6: Sistema di videosorveglianza</b>                          | <b>9</b>  |
| <b>Articolo 7: Accesso alle zone controllo e sicurezza dei dati</b>      | <b>11</b> |
| <b>Articolo 8: Conservazione delle registrazioni</b>                     | <b>13</b> |
| <b>Articolo 9: Modalità di raccolta e trattamento dei dati personali</b> | <b>13</b> |
| <b>Articolo 10: Personale autorizzato e segreto professionale</b>        | <b>14</b> |
| <b>Articolo 11: Informativa agli utenti</b>                              | <b>15</b> |
| <b>Articolo 12: Diritti dell'interessato</b>                             | <b>15</b> |
| <b>Articolo 13: Tutela</b>   | <b>16</b> |
| <b>Articolo 14: Entrata in vigore</b>                                    | <b>16</b> |
| <b>Articolo 15: Allegati</b>   | <b>16</b> |

## Articolo 1: Finalità

Il presente regolamento garantisce che il trattamento dei dati personali, effettuato mediante l'utilizzo di un impianto di videosorveglianza si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, ai sensi del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati di seguito denominato GDPR), del Decreto Legislativo 30 giugno 2003, n. 196 (così come modificato dal dal Decreto Legislativo 10 agosto 2018, n. 10) e secondo quanto disposto dalle direttive impartite dal Garante per la protezione dei dati personali.

## Articolo 2: Definizioni

Ai fini del presente regolamento si intende per:

- a. **"dato personale"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- b. **"trattamento"**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- c. **"titolare del trattamento"**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del

trattamento di dati personali; 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;

- d. **"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;
- e. **"interessato"**: qualsiasi informazione riguardante una persona fisica identificata o identificabile;
- f. **"comunicazione" o "diffusione"**: il dare conoscenza dei dati personali a soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- g. **"dato anonimo"**: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato
- h. **"archivio" o "banca dati"**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- i. **"GDPR"**: 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);
- j. **"Garante"**: il Garante per la protezione dei dati personali;
- k. **"Provvedimento in materia di videosorveglianza"**: il Provvedimento in materia di videosorveglianza - 8 aprile 2010 (Gazzetta Ufficiale n. 99 del 29 aprile 2010);
- l. **"Informativa"**: è il documento con il quale il titolare del trattamento, in forma scritta o orale, informa il soggetto interessato circa le finalità e le modalità del trattamento medesimo;

- m. **"videosorveglianza"**, il sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche di dati, di immagini di aree o zone delimitate;
- n. **"zone controllo"**, locali in cui si sono ubicati i monitor in grado di visualizzare in tempo reale le immagini riprese dalle telecamere (ad esclusione delle immagini per il controllo paziente).
- o. **"zone controllo paziente"**, locali in cui si sono ubicati i monitor in grado di visualizzare in tempo reale le immagini riprese dalle telecamere per il controllo dei pazienti.
- p. **"sala server"** il locale in cui si trovano i server e gli apparati predisposti a registrare tutte le riprese effettuate dai dispositivi periferici;
- q. **"Autorizzati al trattamento" o "Incaricati al trattamento"** ; persone fisiche che il titolare o il responsabile del trattamento possono prevedere ed espressamente designare, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, per svolgere specifici compiti e funzioni connessi al trattamento di dati personali;
- r. **"DPO"**: responsabile della protezione dei dati, figura deputata ad osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali;
- s. **"IRST"**: Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" S.r.l.;
- t. **"Data breach" o "Violazione di dati"**: 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.
- u. **"Referente della protezione dei dati"**: referenza aziendale istituita con l'ingresso della DIRETTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 (GDPR) che viene conferita ad ogni Responsabile/Direttore di UO/Servizio/Struttura, così come definite nel "Manuale Assetto Organizzativo". Questo soggetto ha un livello di conoscenze, abilità e competenze nel proprio contesto organizzativo tali da garantire il supporto al Titolare nell'adozione di idonee misure organizzative nel trattamento dei dati personali. La nomina di *Referente della protezione dei*

*dati* sostituisce la precedente nomina a responsabile "interno" del trattamento dei dati personali rimanendo inalterati i principi generali da osservare, i compiti particolari ai quali il *Referente della protezione dei dati* deve attenersi nonché la finalità della designazione. In particolare il *Referente della protezione dei dati* deve cooperare con il titolare nell'identificazione e nella gestione degli eventi di *data breach* e collaborare attivamente con il titolare e il DPO nell'applicazione del principio di *privacy by design* durante la progettazione di nuovi processi e/o servizi che prevedano il trattamento di dati personali;

Per tutto quanto non definito esplicitamente nel presente paragrafo si rimanda integralmente a quanto stabilito dall'art. 4 del GDPR.

### **Articolo 3: Principi**

1. I dati personali devono essere:
  - a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");
  - b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del GDPR, considerato incompatibile con le finalità iniziali ("limitazione della finalità");
  - c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");
  - d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");
  - e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca

scientifico o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

- f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

#### **Articolo 4: Ambito di applicazione**

1. Il presente regolamento disciplina il trattamento di dati personali, realizzato mediante l'impianto di videosorveglianza attivato nelle aree di pertinenza dell'IRST e mediante altri impianti eventualmente attivati in diversi locali di cui questo Istituto abbia il possesso o il diritto di uso a vario titolo, in conformità a quanto previsto Provvedimento del Garante in materia di videosorveglianza.
2. Le immagini ed i dati raccolti non possono essere utilizzati per finalità diverse rispetto a quelle stabilite nel presente regolamento, e non possono essere diffusi o comunicati a terzi, salvo quanto appresso disposto.

#### **Articolo 5: Soggetti**

1. **Titolare del trattamento.** Il titolare del trattamento dei dati è l'IRST nella persona del Direttore Generale pro-tempore: impartisce le istruzioni circa il trattamento dei dati ed esercita funzioni di vigilanza sull'osservanza delle regole che lo disciplinano.
2. **Referenti per il trattamento dei dati personali.** In relazione al trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza, il titolare ha individuato i seguenti Referenti per il trattamento dati:

- a. Il Responsabile del Servizio Informatico, con riferimento all'impianto di videosorveglianza avente aventi finalità di tutela del patrimonio e degli utenti;
- b. Il Direttore Sanitario, con riferimento all'impianto di videosorveglianza avente finalità di tutela dei pazienti.

Entrambi i Referenti della protezione dei dati personali devono concorrere a perseguire il rispetto della normativa rilevante in materia di protezione dei dati, nonché del presente regolamento, collaborando con il titolare e il DPO nell'attuare tutte le precauzioni di natura tecnica, procedurale ed organizzativa per garantire che il trattamento avvenga secondo la legge e le misure di sicurezza, al fine di impedire un uso improprio dei dati.

I Referenti per il trattamento dei dati personali collaborano inoltre con il titolare ed il DPO nel formulare le indicazioni idonee a prevenire assunzioni o rilevamento di dati da parte delle persone autorizzate all'accesso per le operazioni di manutenzione degli impianti. Provvedono inoltre a proporre e supportare le iniziative di formazione ed aggiornamento degli autorizzati o incaricati al trattamento, con particolare riferimento alle eventuali modifiche delle modalità di utilizzo dei sistemi.

## **2.1 Responsabile del trattamento**

Nei contratti di affidamento a soggetti esterni all'Istituto (outsourcing) relativi, a vario titolo, all'attività di videosorveglianza, il Titolare predisponde, ove pertinente, specifico addendum contrattuale con la quale il soggetto affidatario si impegna, per i trattamenti di dati effettuati in forza del rapporto contrattuale, all'osservanza delle norme di legge sulla protezione dei dati personali e delle disposizioni dell'IRST. In tali ipotesi il Titolare può provvedere alla individuazione di un responsabile esterno ai sensi dell'art. 28 e 29 del GDPR.

## **3. Autorizzati (o incaricati) al trattamento**

Persone fisiche autorizzate sia ad accedere ai luoghi ove sono situate le postazioni di controllo, preposte all'utilizzo degli impianti e laddove sia indispensabile per gli scopi perseguiti a visionare le immagini. Il titolare individua i diversi livelli di accesso in corrispondenza delle



specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono esclusivamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (quali ad esempio copiare, cancellare, spostare l'angolo di visuale, modificare lo zoom ecc).

Gli autorizzati devono effettuare l'attività di trattamento dei dati personali (visione in tempo reale delle immagini e visione delle registrazioni) ai quali hanno accesso per mezzo del sistema di videosorveglianza attenendosi scrupolosamente alle indicazioni dei rispettivi Referenti per la protezione dei dati personali. Agli autorizzati è comunque vietata la visione delle registrazioni, se non su esplicita indicazione del Referente della protezione dei dati per esigenze di difesa di un diritto, di riscontro di un'istanza ad un accesso, oppure di collaborazione con la competente autorità o polizia giudiziaria. Le immagini non saranno in alcun modo comunicate o diffuse a terzi, salvo esigenze di polizia e giustizia.

## **Articolo 6: Sistema di videosorveglianza**

Le telecamere sono installate in luoghi che non si prestano ad alcun uso, neanche preterintenzionale o indiretto a controlli a distanza delle prestazioni lavorative dei dipendenti. Come previsto all'art. 4 della L. 300/1970 (Statuto dei lavoratori) l'installazione di impianti audiovisivi e di altre apparecchiature di controllo avviene previo accordo con le rappresentanze sindacali.

Le aree dell'Istituto sottoposte a controllo video sono:

- Aree e punti strategici per l'Istituto (es. accesso a laboratori ed archivi, strumentazioni, punti accesso alla struttura ecc.).
- Aree di degenza o cura critiche ove è necessario che il personale sanitario tenga sotto controllo video i pazienti per la loro tutela in quanto non direttamente visibili dalle postazioni di lavoro quali ad es. guardiole. In tale contesto il sistema di videosorveglianza risulta indispensabile per la tutela della salute dei pazienti che persino in particolari situazioni di criticità, non altrimenti tutelabili.

- Aree con finalità di tutela dell'utenza da possibili aggressioni, furti, rapine, danneggiamenti e atti vandalici.
  - Aree di elevata affluenza e transito degli utenti che consentano l'accesso a diverse aree di istituto per finalità di prevenzione e tutela dei pazienti e del patrimonio aziendale
  - Aree perimetrali degli immobili ai fini di tutela del patrimonio.
1. Il sistema attualmente installato presso l'IRST consta di una zona controllo presidiata dal Responsabile al trattamento dati e di più zone di controllo paziente presidiate esclusivamente da personale sanitario (autorizzati dal Titolare) preposto e non sono soggette a videoregistrazione. Il locale tecnico per la gestione del sistema e l'archiviazione delle registrazioni sono collocati presso la sala Server dell'IRST dotata di accesso mediante tessera personale di riconoscimento.
  2. Le telecamere consentono, tecnicamente, riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale. Il sistema di videoregistrazione si attiva ogni qualvolta la telecamera rileva un movimento e non a ciclo continuo. Le telecamere telecontrollabili e quindi dotate di brandeggio (in orizzontale e in verticale) sono in numero limitato e dislocate solo in zone dell'Istituto (es. aree esterne all'edificio molto estese) la cui sorveglianza richiede tale dotazione tecnologica. Le immagini video riprese dalle telecamere sono trasmesse alle zone controllo attraverso tecnologia IP. Nessuna telecamera è configurata per poter trasmettere segnali audio.
  3. I segnali video vengono raccolti dai sistemi installati presso la sala Server dove le immagini digitali vengono registrate su appositi server. Tali sistemi mettono inoltre a disposizione remotamente agli Amministratori di Sistema i software necessari all'eventuale esportazione su varie tipologie di media. Le immagini registrate sono conservate per un periodo non superiore ai 7 giorni naturali consecutivi.

4. Per una migliore rappresentazione dell'articolazione distributiva dei sistemi di ripresa e delle zone controllo al presente regolamento si allega planimetria del sistema installato.
5. Il Responsabile del Servizio Informatico mantiene aggiornata la suddetta documentazione.
6. Previa autorizzazione da parte del Titolare il sistema di videosorveglianza può essere ampliato alle diverse strutture ad uso istituzionale dell'Istituto.
7. Al fine di consentire il perseguimento dei fini istituzionali, sono presenti altri sistemi video, la cui finalità non è strettamente la sorveglianza con fini di sicurezza e tutela delle persone o cose, ma prevalentemente la finalità clinica o didattica in quanto la documentazione raccolta è di supporto alla attività di formazione o ha valenza clinica nella diagnosi e cura del paziente. Rientrano in queste attività di trattamento mediante sistemi video dei dati le telecamere connesse alle apparecchiature elettromedicali per la registrazione di immagini durante l'esecuzione di esami o trattamenti sanitari, installazione di sistemi video presso le sale riunioni per esecuzione di videoconferenza o registrazione per diffusione di eventi formativi.

## **Articolo 7: Accesso alle zone controllo e sicurezza dei dati**

1. La zona controllo è a presidio continuo. Le zone controllo paziente sono soggette a presidio continuo durante lo svolgimento dell'attività sanitaria di reparto. La sala Server è ubicata in un locale il cui accesso è limitato tramite sistema automatico di accesso mediante badge personale di riconoscimento.
2. L'accesso alla zona controllo e alle zone controllo paziente è riservato:
  - al titolare del trattamento;
  - al responsabile del trattamento;

- ai referenti del trattamento;
- agli autorizzati al trattamento, istruiti sull'utilizzo dell'impianto e sul trattamento dei dati;
- al personale di pubblica sicurezza o di polizia giudiziaria;
- al personale addetto alla manutenzione degli impianti ed alla pulizia dei locali. In riferimento agli accessi del personale addetto alla pulizia dei locali sono adottate apposite misure di sicurezza ed è assicurata la presenza di un incaricato con compiti di vigilanza circa la sicurezza e riservatezza delle immagini riportate sui monitor.

L'accesso alla Sala Server é riservato agli Amministratori di Sistema, al Titolare, ai Referenti del trattamento, al personale addetto alla manutenzione degli impianti e, sporadicamente, alla pulizia dei locali. In riferimento agli accessi del personale addetto alla pulizia dei locali sono adottate apposite misure di sicurezza ed è assicurata la presenza di un incaricato con compiti di vigilanza circa la sicurezza dei sistemi.

3. All'atto dell'introduzione del sistema di videosorveglianza, il Responsabile informa le persone autorizzate al trattamento sulle rispettive responsabilità, relative al trattamento medesimo, nonché alla conservazione dei dati, alla loro protezione contro eventi dannosi e agli altri obblighi di legge. Gli incaricati del trattamento devono essere in possesso di credenziali di autenticazione che consentano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
4. I server del sistema di registrazione sono posizionati esclusivamente all'interno della sala Server.
5. Nelle ipotesi di accesso per manutenzione, devono essere adottate specifiche cautele e i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si

renda indispensabile al fine di effettuare verifiche tecniche e alla presenza di soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini.

## **Articolo 8: Conservazione delle registrazioni**

1. Al fine di garantire le funzioni di tutela del patrimonio e prevenzione degli atti vandalici, nonché la sicurezza dei pazienti ed utenti, anche con riferimento ad eventi avvenuti in occasione di chiusura dei servizi per festività consecutive o prolungate, la conservazione dei dati videoregistrati avrà luogo per la durata massima 7 giorni naturali e consecutivi, salvo speciali esigenze determinate dalle indagini necessarie per l'accertamento di eventuali reati da parte dell'Autorità giudiziaria. Il sistema è programmato in modo da prevedere la cancellazione automatica da ogni supporto, mediante sovraregistrazione, con modalità tali da escludere la riutilizzabilità dei dati cancellati, dopo il decorso massimo di 7 giorni.
2. Per le stesse esigenze, le immagini videoregistrate, nei limiti del tempo della loro conservazione, possono essere utilizzate anche con riferimento a fatti che si verificano oltre i confini dell'area di Istituto, ma comunque ad una distanza tale da ricadere nell'ambito del raggio coperto dal brandeggio delle telecamere.
3. In caso di cessazione di un trattamento per qualsiasi causa, i dati personali sono distrutti.

## **Articolo 9: Modalità di raccolta e trattamento dei dati personali**

1. I dati personali sono ripresi attraverso le telecamere dell'impianto di videosorveglianza dichiarato dall'installatore conforme alle misure minime ed alle norme previste dalla normativa vigenti e dal provvedimento in materia di videosorveglianza.

2. I soggetti autorizzati a compiere le operazioni del trattamento dal Titolare sono tenuti a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto. Le immagini riprese dalle telecamere sono visualizzate in tempo reale sui monitor presenti nella zona controllo e registrate nei sistemi informatici installati presso la sala Server (nel caso di telecamere non necessarie al controllo dei pazienti). La visione delle immagini registrate deve essere effettuata solo, ove strettamente indispensabile, dagli autorizzati interni all'Istituto specificatamente autorizzati dal Titolare o dai Referenti del trattamento dati o direttamente dai Referenti del trattamento. Le immagini vengono rese disponibili agli autorizzati dagli Amministratori di Sistema su richiesta degli incaricati preventivamente autorizzati.

Eventuale attività di duplicazione dei dati su supporto ottico deve essere eseguita solo dall'incaricato su indicazione del Titolare o del Referente ed a seguito di specifica richiesta dell'Autorità giudiziaria. Per tale attività inoltre deve essere redatto apposito verbale elettronico firmato digitalmente dal Responsabile.

3. Ogni specifica indicazione dal Titolare o del Referente rivolta agli autorizzati deve avvenire in forma scritta anche a mezzo mail istituzionale.

## **Articolo 10: Personale autorizzato e segreto professionale**

1. Tutti coloro che hanno accesso al sistema di videosorveglianza sono vincolati al rigoroso segreto professionale su tutte le informazioni, dati personali o immagini di terze persone cui possono accedere. Le informazioni o dati o immagini oggetto di trattamento durante la gestione ordinaria o straordinaria del sistema di videosorveglianza non potranno essere diffusi o divulgati o comunicati salva l'ipotesi di comunicazione all'Autorità Giudiziaria. Le immagini idonee a rilevare stato di salute non devono comunque essere diffuse.

## **Articolo 11: Informativa agli utenti**

1. In ottemperanza a quanto disposto GDPR e al Provvedimento in materia di videosorveglianza, prima del raggio di azione delle telecamere e non necessariamente a contatto con gli impianti è affissa adeguata segnaletica contenente l'informativa semplificata formulata secondo lo schema che costituisce allegato 1 del predetto provvedimento. E' presente inoltre una informativa estesa all'ingresso principale dell'Istituto (zona adiacente alla Portineria) riportata anche sul sito di Istituto nell'apposita sezione "INFORMAZIONI SULLA PROTEZIONE DEI DATI". La registrazione delle immagini è effettuata dall'Istituto per finalità di cura e tutela dei pazienti, tutela dei patrimonio, di prevenzione di atti vandalici e per indagini di polizia giudiziaria. L'interessato è titolare dei diritti previsti dalla Sezione 2 "Informazione e accesso ai dati personali" del GDPR.

## **Articolo 12: Diritti dell'interessato**

1. Ciascun interessato al trattamento ha facoltà di esercitare i diritti (art. 15 del GDPR) al fine di poter richiedere la cancellazione o il blocco dei dati se trattati in violazione di legge. Con riferimento alle immagini videoregistrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo. Le richieste di esercizio dei diritti previsti dall'art. 15 del Regolamento Generale sulla Protezione dei Dati a favore dell'interessato possono essere rivolte al Responsabile della Protezione dei Dati presso l'IRST contattabile al seguente indirizzo PEC: [privacy@irst.legalmail.it](mailto:privacy@irst.legalmail.it), al seguente indirizzo MAIL: [privacy@irst.emr.it](mailto:privacy@irst.emr.it) o al seguente numero di telefono: 0543.739415. Ai medesimi recapiti può essere richiesto l'elenco completo ed aggiornato dei Responsabili del trattamento nominati.

Il Titolare del trattamento è l'Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" (I.R.S.T.) S.r.l. 47014 Meldola (FC) - Via Piero Maroncelli, 40 - Tel. 0543.739100. e-mail: direzione.generale@irst.emr.it . L'interessato ha il diritto di presentare un reclamo all'autorità di controllo in tema di protezione dei dati, nello Stato membro in cui risiede abitualmente, qualora ritenga che siano stati violati i diritti di cui gode e sanciti dal GDPR.

### **Articolo 13: Tutela**

1. La materia dei danni cagionati dal trattamento dei dati personali è disciplinata dalla normativa vigente applicata alla fattispecie.
2. La tutela amministrativa e giurisdizionale è regolata dagli artt. 141 e seguenti del Codice, e successive modifiche ed integrazioni.
4. Le operazioni non conformi al presente regolamento ed il trattamento illecito o non corretto dei dati espongono alle sanzioni amministrative, disciplinari, civili e penali previste dalla normativa vigente applicata alla fattispecie.

### **Articolo 14: Entrata in vigore**

Il presente regolamento entra in vigore il giorno successivo a quello della sua approvazione, da parte del Direttore Generale, ed è pubblicato sul sito dell'IRST

### **Articolo 15: Allegati**

- "Allegato 1 piano seminterrato": planimetria e aree di sorveglianza piano seminterrato
- "Allegato 2 piano rialzato": planimetria e aree di sorveglianza piano rialzato
- "Allegato 3 piano primo": planimetria e aree di sorveglianza piano primo
- "Allegato 4 piano secondo": planimetria e aree di sorveglianza piano secondo
- "Allegato 5 piano terzo": planimetria e aree di sorveglianza piano terzo



- “Allegato 6 Radioterapia Ravenna”: planimetria e aree di sorveglianza radioterapia Ravenna
- “Allegato 7 San Giuseppe - piano seminterrato”: planimetria e aree di sorveglianza piano seminterrato
- “Allegato 8 San Giuseppe - esterno”: planimetria e aree di sorveglianza esterno
- “Allegato 9 San Giuseppe - piano terra”: planimetria e aree di sorveglianza piano terra
- “Allegato 10 San Giuseppe - piano primo”: planimetria e aree di sorveglianza piano primo
- “Allegato 11 San Giuseppe - piano secondo”: planimetria e aree di sorveglianza piano secondo
- “Allegato 12 esterno”: planimetria e aree di sorveglianza esterno