Politica per la gestione dei rapporti con i soggetti che svolgono trattamenti di dati personali in relazione con la Struttura Sanitaria

Autore/i:	Alessandra Vitagliozzi	Cybermind S.r.l.
Rivisto Da	Fabrizio Matta	Cybermind S.r.l.
Approvato Da:	Carmine Maraio, Helga Fineo	Sistemi Informativi S.p.A., IBM S.p.A.
Accettato Da:	Alberto Genovese	So.Re.Sa. S.p.A.

Storia del documento

Data	Versione	Descrizione modifiche	Autore

Sommari

1 Generalità

Il principio di responsabilizzazione, sancito dal Regolamento UE 2016/679, di seguito GDPR o Regolamento, attribuisce al Titolare la piena responsabilità nel porre in atto tutte le misure necessarie a garantire il rispetto dei diritti dell'Interessato e un'adeguata sicurezza dei dati personali, durante tutto il ciclo di vita dei trattamenti. In accordo a questo principio, il Titolare del trattamento risponde anche dell'operato di soggetti esterni che svolgono trattamenti di dati personali per conto della Struttura Sanitaria.

1.1 Finalità del documento

Questo documento espone le politiche di base che regolamentano i rapporti tra la Struttura Sanitaria ed i soggetti, siano essi persone fisiche o giuridiche, che erogano servizi di qualsiasi natura, che richiedono il trattamento di dati personali riconducibili, in tutto o in parte, all'ambito delle responsabilità del Titolare.

Il rispetto degli indirizzamenti contenuti nel presente documento è affidato al DPO ed alle Unità Organizzative della Struttura Sanitaria che intrattengono rapporti con detti soggetti, in virtù di specifici riferimenti contrattuali che ne definiscono la natura, le modalità ed i vincoli applicabili ai servizi e/o alle prestazioni fornite.

1.2 Indirizzamenti normativi

Con la presente politica il Titolare del trattamento dispone l'attuazione delle misure organizzative e procedurali che assicurino una corretta applicazione degli articoli 24, 26, 28 e 79 del Regolamento, tenuto conto anche di quanto esposto dal Garante per la protezione dei dati personali in materia di trattamenti di dati sanitari, nel provvedimento n.55 del 7 Marzo 2019.

1.3 Documenti di riferimento

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e s.m.i.

[2] D.lgs 10 agosto 2018, n. 101. “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” e s.m.i.

[3] D.Lgs. 30 Giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e s.m.i.

[4] Provvedimento Garante n.55 del 7 Marzo 2019, “Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario”

[5] ISO/IEC 27001:2013 “Information Security Management Systems”, 01/10/2013

[6] ISO/IEC 27002:2013 “Code of practice for information security controls", 01/10/2013

[7] ISO/IEC 27001:2017 “Information technology — Security techniques — Information security management systems - Requirements”, 2017-03

[8] Politica per la Cancellazione Sicura e lo Smaltimento dei Supporti Elettronici della Struttura Sanitaria

[9] Politica per il corretto utilizzo delle risorse informative aziendali della Struttura Sanitaria

[10] Politica per la gestione delle utenze abilitate al trattamento dei dati e delle informazioni personali

[11] Politica per la gestione dei diritti dell’Interessato

[12] Politica per gli amministratori di sistema

[13] Linee Guida per la gestione delle violazioni della sicurezza dei dati personali

[14] Linee Guida per la Classificazione delle Informazioni e dei Trattamenti

[15] Linee Guida per la gestione del registro delle attività di trattamento

[16] Linee Guida per la conduzione delle attività di Data Protection Impact Assessment

[17] Linee Guida per la conduzione delle verifiche di conformità e adeguatezza delle misure preposte alla tutela dei dati personali

[18] Procedura per la gestione delle utenze del personale interno ed esterno

[19] Procedura per la gestione delle utenze amministrative

[20] Procedura per la gestione dei diritti dell’Interessato

[21] Procedura per la gestione del data breach

1.4 Acronimi e definizioni

Termine	Definizione
Classificazione	L'attribuzione all'informazione di un livello di classificazione ovvero il suo inserimento all'interno di una classe di sicurezza.
Categorie particolari di dati personali	Ai sensi dell'art. 9 del regolamento (UE) 2016/679 - GDPR [1]: Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Dato	L'informazione puntuale contenuta in un archivio cartaceo o informatico.

Termine	Definizione
Dato personale	Ai sensi dell'art. 4 del regolamento (UE) 2016/679 - GDPR [1]: 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.
DPIA	Data Protection Impact Assessment (art. 35 del GDPR).
DPO	Data Protection Officer.
GDPR	Regolamento UE n. 679/2016 – General Data Protection Regulation (Regolamento Generale per la Protezione dei Dati) [1]
Informazione	La rappresentazione di dati, atti o fatti rilevanti per la Struttura Sanitaria.
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.
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.
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

Termine	Definizione
	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	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.

Tabella 1 – Acronimi e definizioni

2 Soggetti interni alla Struttura Sanitaria

Per favorire una corretta applicazione del Regolamento, il Titolare si avvale della collaborazione del personale interno, i cui compiti ed ambiti di responsabilità sono stabiliti dal Regolamento e/o da specifici incarichi e/o deleghe. Nei paragrafi successivi sono descritti, oltre alla figura stessa del Titolare, i ruoli di supporto alla gestione della privacy, designati dal Titolare della Struttura Sanitaria.

2.1 Titolare del trattamento

In base all'art. 4, par. 1 n. 7 del Regolamento**,** è "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".

2.2 Responsabile per la Protezione dei Dati

Il Responsabile della Protezione dei Dati o Data Protection Officer, nel seguito DPO, è una figura definita negli artt. 37, 38 e 39 del Regolamento, designata dal Titolare e selezionata tra il personale interno o tra soggetti esterni, siano essi persone fisiche o giuridiche, avendo cura che la nomina riguardi figure professionalmente idonee e svincolate da ogni forma di conflitto di interessi.

Nell'ambito della presente Politica il DPO designato dalla Struttura Sanitaria assolve ai seguenti compiti:

- Informare e fornire supporto consulenziale al Titolare del trattamento, ai dipendenti autorizzati al trattamento, ai Delegati o Referenti privacy della Struttura Sanitaria in merito agli obblighi derivanti dall'applicazione del Regolamento nei rapporti con i Contitolari e con i Responsabili;
- Gestire le relazioni e favorire le comunicazioni tra la Struttura Sanitaria ed i soggetti esterni, Contitolari o Responsabili del trattamento, interloquendo anche con i corrispettivi DPO da questi designati;

- Gestire, i rapporti e le comunicazioni tra la Struttura Sanitaria e l'Autorità di Controllo nazionale (Garante per la protezione dei dati personali);
- Supervisionare, anche con poteri di indirizzamento e controllo, le attività di aggiornamento del registro dei trattamenti, avendo cura di rilevare la correttezza delle informazioni relative agli eventuali contitolari, responsabili e sub-responsabili esterni;
- Supervisionare, anche con poteri di indirizzamento e controllo, le attività di valutazione degli impatti e dei rischi correlati ai trattamenti svolti in regime di contitolarità o affidati a Responsabili esterni;
- Coordinare le verifiche di adeguatezza e conformità delle attività svolte dai Responsabili esterni, che devono operare secondo le istruzioni impartite dal Titolare della Struttura Sanitaria;
- Supportare, anche con potere di indirizzamento e controllo, il Titolare della Struttura Sanitaria, i Delegati/Referenti privacy e i dipendenti autorizzati, nello svolgimento delle attività finalizzate ad agevolare l'esercizio dei diritti dell'Interessato;
- Supportare, anche con potere di indirizzamento e controllo, il Titolare della Struttura Sanitaria, i Delegati/Referenti privacy ed il personale interno, nella gestione delle violazioni alla sicurezza dei dati personali (data breach).

2.3 Delegato o Referente privacy

All'interno della Struttura Sanitaria, Il Titolare del trattamento ha la facoltà di nominare, mediante apposita delibera, uno o più Referenti privacy, individuati tra i Responsabili delle Unità Organizzative, ai quali sono attribuiti i compiti di promuovere, agevolare e verificare la corretta applicazione delle disposizioni in materia di trattamento dei dati personali. A tale scopo i Referenti privacy operano di concerto con il DPO, che svolge funzioni di supervisione con poteri di indirizzamento e controllo.
Nell'ambito della presente Politica, ai Referenti privacy della Struttura Sanitaria, spetta il compito di:

- Rilevare e comunicare al Titolare del trattamento ed al DPO le informazioni relative a soggetti esterni che svolgono, a qualsiasi titolo ed in qualsiasi modalità, trattamenti di dati personali in nome e per conto della Struttura Sanitaria e nello specifico dell'Unità Organizzativa di competenza;
- Collaborare con il Titolare del trattamento e/o con il DPO e/o con l'Unità Organizzativa Affari Legali:

  nella valutazione dei requisiti di idoneità dei Responsabili e dei sub-responsabili;
  nella stesura dei contratti di designazione dei Responsabili esterni;
- Segnalare, al Titolare del trattamento e al DPO, ogni variazione che necessiti di un aggiornamento del Registro dei trattamenti, derivanti da cambiamenti nella catena di fornitori designati come Responsabili o sub-responsabili;
- Collaborare con il DPO per agevolare il trasferimento delle istruzioni impartite dal Titolare del trattamento ai Responsabili esterni;
- Segnalare al Titolare del trattamento e al DPO, ogni variazione che necessiti di una revisione o di una nuova analisi degli impatti e dei rischi (DPIA), relativamente ai trattamenti svolti dai Responsabili e dai sub-responsabili designati;
- Gestire sotto il coordinamento del DPO, ricorrendo eventualmente anche a fornitori/consulenti esterni, il programma di verifiche sistematiche volto a rilevare il corretto svolgimento delle attività in carico ai Responsabili del trattamento, in termini di:

  conformità alle istruzioni impartite dal Titolare in forma di clausole contrattuali, politiche, linee guida, procedure ed istruzioni operative;
  adeguatezza delle misure di sicurezza logica, fisica ed organizzativa, finalizzate al contenimento dei rischi di violazione della sicurezza dei dati personali trattati;
  conformità e adeguatezza dei controlli esercitati da ciascun Responsabile sul/sui sub-responsabile/i da questo designati;
- Rilevare e segnalare prontamente al Titolare del trattamento e al DPO, eventuali scostamenti dei livelli di servizio prestabiliti con i Responsabili del trattamento relativi a:

tempi di notifica al Titolare del trattamento, all'Autorità di Controllo nazionale (Garante per la protezione dei dati personali) e, nei casi applicabili, agli Interessati, di eventuali violazioni della sicurezza riscontrati nel corso del trattamento di dati personali (data breach);
tempi di espletamento delle attività finalizzate a garantire l'esercizio dei diritti dell'Interessato.

2.4 Autorizzati al trattamento

Il personale dipendente della Struttura Sanitaria che, nell'espletamento delle proprie mansioni tratta dati personali posti sotto il dominio di responsabilità del Titolare del trattamento, si intende autorizzato a compiere tale trattamento, limitatamente al proprio ambito di competenza.
Il dominio di autorizzazione al trattamento s'intende esplicitato dal ruolo e dalle mansioni svolte da ciascun autorizzato all'interno della propria unità Organizzativa.
Ulteriori restrizioni al trattamento da parte del personale interno, sono esplicitate mediante specifiche procedure operative o misure di sicurezza, quali ad esempio controllo degli accessi ai locali e/o ai sistemi informativi e/o alle infrastrutture tecnologiche. A tale proposito, la Struttura Sanitaria pubblica le seguenti procedure operative:

- "Procedura per la gestione delle utenze del personale interno ed esterno" [18];
- "Procedura per la gestione delle utenze amministrative" [19].

In ottemperanza all'obbligo di informazione e formazione del personale interno autorizzato al trattamento, la Struttura Sanitaria fornisce inoltre un insieme di regole, documentate e strutturate in forma di Politiche e Linee guida, che indirizzano e regolamentano norme comportamentali di riservatezza, per una corretta gestione dei trattamenti in sicurezza, quali ad esempio:

- Linee guida per la classificazione delle informazioni e dei trattamenti [14];
- Politica per il corretto utilizzo delle risorse informative aziendali [9];
- Politica per gli amministratori di sistema [12];

- Politica per la gestione delle utenze abilitate al trattamento dei dati e delle informazioni personali [10].

Per quanto concerne le prestazioni professionali e/o i servizi erogati da fornitori esterni, il Titolare della Struttura Sanitaria, supportato dal DPO, vigila sull'operato dei Responsabili del trattamento designati, verificando periodicamente le misure di sicurezza volte a garantire che i trattamenti vengano svolti esclusivamente dal personale autorizzato, verificando che tale garanzia sia fornita anche dagli eventuali sub-responsabili.

3 Soggetti esterni identificati dalla normativa

Il Regolamento distingue tre tipologie di rapporti possibili tra il Titolare del trattamento e gli altri soggetti esterni, che ricoprono altrettanti ruoli nell'ambito dei trattamenti di dati personali. Nei paragrafi successivi sono esplicitati i suddetti ruoli, contestualizzati agli scopi perseguiti dalla Struttura Sanitaria.

3.1 Contitolare

In base all'art. 26, par. 1 del Regolamento, si indicano con questo termine due o più Titolari che determinano in modo congiunto le finalità e i mezzi del trattamento in maniera trasparente e mediante un accordo interno scritto. Questo accordo, sottoscritto dalle Parti, deve individuare i rispettivi ambiti di responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo alla tutela dell'Interessato nell'esercizio dei propri diritti, alle rispettive funzioni di comunicazione delle informazioni agli Interessati (artt. 13 e 14 del Regolamento), nonché agli obblighi di comunicazione di violazioni della sicurezza dei dati personali (data breach) in adempimento agli artt. 33 e 34 del Regolamento.

Nell'ambito della presente Politica, l'instaurazione dei rapporti di contitolarità deve essere valutata caso per caso, dal Titolare del trattamento, che in tale compito può avvalersi del supporto del DPO e dei Referenti/Delegati privacy (vedi par. 2.3) nonché di consulenti esterni.

3.2 Responsabile

Secondo quanto stabilito all'art. 4, par. 1 n. 8 del Regolamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Nell'ambito della presente Politica, in adempimento alle disposizioni di cui all'art. 28 par. 1 del Regolamento, la designazione del Responsabile è obbligatoria per tutte le persone giuridiche esterne (genericamente detti fornitori), che erogano, a qualsiasi titolo ed in qualsiasi modalità,

prestazioni professionali e/o servizi di trattamento di dati personali riconducibili al dominio di responsabilità del Titolare del trattamento della Struttura Sanitaria.

3.3 Sub-responsabile

Questo ruolo indica un possibile secondo livello di responsabilità gerarchica, nei casi in cui un Responsabile decida di ricorrere alla collaborazione di uno o più soggetti giuridici per il conseguimento delle finalità di trattamento a lui affidate dal Titolare. A tale scopo, il Responsabile deve preventivamente comunicare la propria intenzione di integrare o sostituire uno o più sub-responsabili, lasciando al Titolare del trattamento la facoltà di opporsi, negandone l'autorizzazione (art. 28, par. 2 del Regolamento).

I rapporti tra il Responsabile ed il sub-responsabile sono vincolati alle medesime regole impartite dal Titolare del trattamento all'atto della designazione del Responsabile. È compito del Responsabile trasferire l'insieme delle regole applicabili ai trattamenti svolti dal sub-responsabile.

Successivamente all'autorizzazione scritta da parte del Titolare, la designazione di un sub-responsabile da parte del Responsabile deve essere formalizzata mediante uno specifico contratto scritto.

4 Gestione dei rapporti di contitolarità

I Contitolari sono soggetti giuridici, previsti dal Regolamento, che in virtù di un accordo scritto tra le parti, "determinano congiuntamente le finalità e i mezzi del trattamento" (art. 26 paragrafo 1 del regolamento).

Pertanto, il Titolare della Struttura Sanitaria condivide, con i Contitolari, con pari grado di responsabilità e discrezionalità decisionale nei confronti dell'Interessato, i trattamenti sottoposti a regime di contitolarità determinati dal verificarsi delle condizioni descritte al paragrafo 4.1.

Nei paragrafi successivi sono dettagliati i principi e gli indirizzamenti che regolamentano i rapporti tra il Titolare della Struttura Sanitaria ed altri Titolari del trattamento afferenti a soggetti giuridici esterni, che svolgono trattamenti in regime di contitolarità.

4.1 Regole per la definizione degli accordi di contitolarità

Ferma restando la discrezionalità decisionale di ciascun Titolare nell'intraprendere rapporti di contitolarità, le condizioni per la stipula di un tale accordo sussistono qualora si verifichino almeno una delle seguenti condizioni:

- Il Titolare del trattamento della Struttura Sanitaria, non disponendo della piena titolarità sui dati e/o sui trattamenti svolti da altri soggetti esterni, sia impossibilitato ad esercitare l'obbligo di indirizzamento e controllo sull'operato degli altri soggetti;
- Due o più titolari che perseguono le medesime finalità di trattamento decidano di condividere strumenti e risorse di supporto al trattamento.

Il rapporto di contitolarità deve essere formalizzato tramite un accordo scritto tra le parti, che espliciti in maniera chiara ed evidente:

- Tipologia dei dati personali e finalità dei trattamenti sottoposti a contitolarità;
- Impegno, da parte di ciascun contitolare, a comunicare il nominativo di tutti gli altri contitolari nelle informative agli interessati;

- Impegno da parte di ciascun contitolare ad acquisire il consenso al trattamento da parte degli interessati, nei casi, nei termini e nei modi derivanti dagli adempimenti normativi;
- Impegno da parte di ciascun contitolare ad annotare e manutenere nel proprio registro dei trattamenti, tutte le informazioni riconducibili ai trattamenti sottoposti a contitolarità;
- Impegno da parte di ciascun contitolare nell'esecuzione e nella documentazione delle analisi degli impatti (DPIA), nei casi previsti dalla legge, ovvero in presenza di rilevanti rischi per la sicurezza dei dati personali trattati in regime di contitolarità;
- Impegno da parte di ciascun contitolare nell'adozione di adeguate misure di sicurezza per minimizzare i rischi di violazioni della riservatezza, integrità e disponibilità dei dati trattati in regime di contitolarità;
- Impegno da parte di ciascun contitolare nell'adottare politiche e risorse adeguate a garantire un corretto esercizio dei diritti degli Interessati;
- Impegno da parte di ciascun contitolare ad informare tempestivamente tutti gli altri contitolari circa ogni evento che possa sottintendere modifiche o estensioni delle finalità di trattamento riconducibili ai termini dell'accordo di contitolarità;
- Impegno da parte di ciascun contitolare nel comunicare tempestivamente agli altri contitolari ogni presunta o accertata violazione della sicurezza dei dati personali sottoposti a regime di contitolarità (data breach);
- Impegno da parte di ciascun contitolare nel comunicare qualsiasi contenzioso intrapreso dagli interessati avente come oggetto il trattamento dei dati personali sottoposti a regime di contitolarità;
- Impegno da parte di ciascun contitolare nel comunicare qualsiasi osservazione o rilievo da parte dell'Autorità di Controllo nazionale (Garante per la protezione dei dati personali), avente come oggetto il trattamento e/o i dati personali sottoposti a regime di contitolarità;
- Clausole sul diritto di rivalsa in caso di applicazione dell'art. 26 par. 3 del Regolamento, che stabilisce la facoltà da parte dell'Interessato, indipendentemente dalle disposizioni

dell'accordo, di esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento.

Fermo restando l'obbligo di comunicazione dei nominativi dei contitolari tramite informativa agli interessati, dovrà essere messa a disposizione degli Interessati anche una sintesi dei punti principali dell'accordo di contitolarità. Questo documento potrà essere rilasciato su richiesta dell'Interessato o notificato anche in forma di allegato all'informativa fornita da ciascun contitolare, avendo cura di evidenziare la possibilità da parte dell'interessato a far valere i propri diritti nei confronti di ciascun contitolare.

4.2 Individuazione dei canali di comunicazione tra soggetti Contitolari

Salvo diversa disposizione, derivante dal contesto specifico entro il quale si svolgono trattamenti in regime di contitolarità, il referente per le relazioni esterne con i Contitolari è il Titolare della Struttura Sanitaria, che si avvale della collaborazione e della consulenza del DPO ed eventualmente di altre figure interne alle quali è attribuito il ruolo di Delegato/Referente privacy.

Per quanto riguarda i canali di informazione, devono essere inviate tramite PEC le comunicazioni tra i Contitolari relative a:

- Richieste da parte degli Interessati effettuate nell'esercizio dei propri diritti di cui al capo III del Regolamento;
- Constatazione di violazioni di sicurezza riconducibili al proprio dominio di contitolarità (data breach);
- Pronunciamenti, rilievi e sanzioni stabiliti dall'Autorità di Controllo (Garante della protezione dei dati personali), riguardanti i trattamenti e/o i dati personali in regime di contitolarità;
- Modifiche rilevanti sulle sui trattamenti e i dati personali sottoposti a regime di contitolarità;
- Risultati e successive modifiche rilevanti sulle valutazioni di impatto e di rischio per i trattamenti e i dati personali sottoposti a regime di contitolarità, qualora concordato tra i Contitolari;

- Variazioni relative ai Titolari ed ai Responsabili nell'ambito dei trattamenti sottoposti a regime di contitolarità;
- Richieste di variazione sulle informative e sulle eventuali modalità di acquisizione dei consensi da parte degli Interessati del trattamento di dati personali in regime di contitolarità;
- Ogni altra tipologia di richieste che si ritengono rilevanti ai fini di una corretta gestione dei trattamenti e dei dati sottoposti a regime di contitolarità.

Tutte le comunicazioni relative al trasferimento di informazioni personali devono essere effettuate adottando le misure di protezione previste nelle "Linee Guida per la Classificazione delle Informazioni e dei Trattamenti" [14].

Per quanto riguarda le comunicazioni relative all'operatività, quali ad esempio la gestione dei sistemi informativi, la gestione delle credenziali di accesso e la cessazione di trattamenti, i referenti preposti dalla Struttura Sanitaria dovranno essere individuati tra i Delegati/Referenti privacy nominati presso ciascuna Unità Operativa. I Delegati/Referenti privacy hanno la facoltà di inserire ulteriori riferimenti, in funzione delle specifiche esigenze operative. A tale proposito, ciascun Delegato/Referente privacy, dovrà redigere una lista contenente le informazioni di contatto (es. incarico, nominativo, recapito telefonico e indirizzo di posta elettronica aziendale di ciascun referente). La lista con i riferimenti di contatto dovrà essere inoltrata al DPO della Struttura Sanitaria, che a sua volta provvederà ad inoltrarla ai referenti indicati dagli altri Contitolari.

4.3 Individuazione dei trattamenti e dei dati personali

A differenza della Titolarità sul trattamento dei dati personali, che si concretizza nell'applicazione obbligata e non delegabile del principio di responsabilizzazione attribuito ad ogni soggetto giuridico che tratta dati personali, il rapporto di Contitolarità scaturisce da un accordo tra le parti, rappresentate da due o più Titolari che decidono deliberatamente di condividere le responsabilità derivanti dall'applicazione del Regolamento a specifici trattamenti condivisi.

Poiché la contitolarità implica la responsabilità in solido di tutti i contitolari, ad esempio nei confronti di eventuali contenziosi intrapresi dagli Interessati, appare di fondamentale importanza la definizione circostanziata del dominio sul quale si esercitano queste responsabilità condivise.

A tale scopo è opportuno definire l'insieme delle tipologie di trattamenti svolti in regime di contitolarità, tenendo presente che, in base all'art.4 del Regolamento, per trattamento si intende "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".

Poiché la corresponsabilità derivante dalla contitolarità implica anche l'assunzione condivisa dei rischi, si raccomanda di definire congiuntamente con gli altri titolari un livello di granularità (dettaglio) che definisca in maniera chiara ed univoca i trattamenti, le finalità di trattamento e le tipologie di dati personali sottoposti a regime di contitolarità, riportandoli con il medesimo criterio di aggregazione sui rispettivi registri dei trattamenti in carico a ciascun Contitolare.

4.4 Valutazioni degli impatti sulla protezione dei dati

Sebbene le analisi degli impatti sui diritti e sulle libertà individuali dell'interessato siano attività che ciascun Contitolare svolge in autonomia, è auspicabile una condivisione perlomeno dei risultati di tali analisi, al fine di evitare discrepanze rilevanti nelle valutazioni effettuate da ciascuna parte.

Per quanto riguarda la condivisione dei risultati delle valutazioni DPIA, occorre considerare che queste potrebbero assumere effettivamente valori diversi, in funzione delle modalità di trattamento applicate in autonomia da ciascun Contitolare, come ad esempio il ricorso a differenti tecnologie informatiche e mezzi di comunicazione. Pertanto, le ipotesi di condivisione dei risultati delle DPIA dovranno essere valutate caso per caso, tenendo conto degli effettivi benefici apportati da tale opzione.

Nel caso in cui i Contitolari condividano mezzi attraverso i quali vengono effettuati i trattamenti, è auspicabile che per tale ambito le analisi degli impatti sui diritti e sulle libertà individuali dell'interessato vengano svolte congiuntamente, al fine di individuare le opportune misure per la riduzione dei rischi.

4.5 Gestione delle informative agli Interessati e raccolta del consenso

Nelle informative agli Interessati è obbligatorio inserire le informazioni di tutti i contitolari del trattamento, per consentire, tra l'altro, a ciascun Interessato l'esercizio dei propri diritti di cui al capo III del Regolamento. Ferma restando l'obbligatorietà di questo adempimento, a ciascuno dei Contitolari è data la discrezionalità di decidere la forma e le modalità di comunicazione dell'informativa.

Sulla base delle precedenti considerazioni, le ipotesi di condivisione, anche solo per reciproca conoscenza, delle informative emanate da ciascun Contitolare, dovranno essere valutate caso per caso, tenendo conto degli effettivi benefici apportati da tale opzione.

Le medesime considerazioni valgono per la raccolta dei consensi al trattamento, nei casi in cui le finalità del trattamento non rientrino in almeno una delle basi giuridiche enunciate all'art. 6, lettera b-c-d-e, del Regolamento. Per quanto concerne i trattamenti di dati personali sanitari, il Titolare della Struttura Sanitaria adotta i criteri valutativi per la raccolta del consenso, definiti nel provvedimento del Garante per la protezione dei dati personali n.55 del 7 Marzo 2019, "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario" [4].

4.6 Gestione degli adempimenti per l'esercizio dei diritti dell'Interessato

L'esercizio dei diritti dell'interessato è garantito dal capo III del Regolamento e rappresenta uno dei principi cardinali su cui si fonda la tutela dei diritti e delle libertà individuali, durante il trattamento di dati personali. Oltre a ciò, i processi di espletamento delle richieste avanzate dagli Interessati nell'esercizio dei propri diritti, che possono essere inoltrate indifferentemente ad uno o più Contitolari, rendono assolutamente auspicabile la definizione di procedure operative congiunte, che

consentano una gestione trasversale di tali richieste, nel rispetto dei modi e dei termini temporali stabiliti dal Regolamento.

A tale scopo il Titolare della Struttura Sanitaria renderà disponibile agli altri Contitolari la "Politica per la gestione dei diritti dell'Interessato" [11], che documenta le modalità con cui il Titolare del trattamento affronta questa problematica all'interno della Struttura Sanitaria.

4.7 Gestione delle violazioni della sicurezza dei dati personali

L'obbligo di comunicazione di violazione della sicurezza dei dati personali è stabilito dagli artt. 33 e 34 del regolamento, che ne fissa anche i limiti massimi temporali (entro 72 ore per la comunicazione all'Autorità di Controllo) e le circostanze che ne determinano anche la comunicazione agli Interessati.

Fermo restando che l'impegno di ciascun Contitolare a comunicare agli altri Contitolari la constatazione di tali violazioni dovrebbe essere esplicitato negli accordi di contitolarità, come suggerito al paragrafo 4.1 del presente documento, è auspicabile che siano stabilite le modalità di cooperazione perlomeno nelle seguenti attività:

- Comunicazione di constatazione di violazione della sicurezza a tutti i contitolari;
- Cooperazione nel rilevamento delle circostanze, delle cause e nell'analisi delle possibili conseguenze derivanti dalla violazione constatata;
- Analisi degli impatti e condivisione delle decisioni in merito all'obbligo di comunicare la violazione al Garante per la protezione dei dati personali;
- Condivisione delle decisioni in merito alla necessità di comunicare la violazione al/agli Interessato/i.

La procedura dovrà inoltre definire ruoli e responsabilità organizzative del personale, preposto da ciascun Contitolare, allo svolgimento delle attività operative, in adempimento alle disposizioni di cui agli artt. 33 e 34 del Regolamento.

A tale scopo il Titolare della Struttura Sanitaria renderà disponibili agli altri contitolari la “Linee guida per la gestione delle violazioni della sicurezza dei dati personali” [13], che documenta le modalità con cui il Titolare del trattamento affronta questa problematica all’interno della Struttura Sanitaria.

5 Gestione dei rapporti tra il Titolare ed i Responsabili del trattamento

Il Responsabile del trattamento è un soggetto esterno alla Struttura Sanitaria, identificato in virtù di un contratto o altra forma giuridica, mediante il quale il Titolare gli affida lo svolgimento di trattamenti per conto della Struttura Sanitaria. Tale contratto stabilisce un rapporto che vincola il Responsabile al pieno rispetto delle istruzioni impartite dal Titolare, al quale spetta inoltre l'obbligo di vigilanza e verifica.

Al fine di consentire una corretta gestione delle relazioni tra Il Titolare della Struttura Sanitaria ed i Responsabili da lui designati, sono di seguito esposte le principali iniziative che agevolano il Titolare nell'esercizio delle proprie funzioni di indirizzamento e controllo, durante l'intero ciclo di vita del trattamento.

5.1 Regole per la designazione dei Responsabili del trattamento

Qualora un trattamento o parte di esso venga affidato a persona fisica o giuridica esterna alla Struttura Sanitaria, che opera o presta un servizio in nome e per conto di essa, questa deve essere designata Responsabile del trattamento. Qualora il Titolare non ritenga necessario ricorrere a tale designazione, egli rimane unico responsabile in solido nei confronti dell'Autorità di Controllo e nei confronti degli Interessati.

Nel caso di Raggruppamenti Temporanei di Impresa, costituiti per erogare servizi alla Struttura Sanitaria, il ruolo di Responsabile può essere attribuito:

- All'impresa mandataria nel caso di RTI di tipo orizzontale;
- A ciascuna delle imprese costituenti il RTI, relativamente al proprio specifico ambito di fornitura, nel caso di RTI di tipo verticale.

Nel caso di raggruppamenti permanenti, quali ad esempio consorzi stabili e società consortili, cooperative ed altre tipologie di associazioni che si configurano come soggetto giuridico, è preferibile la designazione di un unico Responsabile del trattamento.

I trattamenti affidati a ciascun Responsabile devono essere disciplinati da un contratto o altro atto giuridico scritto, da cui si evinca in maniera chiara il rapporto di subordinazione del Responsabile al potere di indirizzamento e controllo esercitato dal Titolare della Struttura Sanitaria, relativamente ad ogni circostanza riconducibile al/i trattamento/i affidato/i.

Il contratto/atto giuridico tra le parti deve descrivere puntualmente le prestazioni del Responsabile (natura delle operazioni, finalità del trattamento, dati personali trattati, etc.) e la durata del contratto, esplicitando i seguenti impegni da parte del Responsabile nei confronti del Titolare:

- Osservare le istruzioni impartite dal Titolare relativamente alle finalità ed alle modalità di trattamento;
- Garantire che le persone autorizzate al trattamento dei dati personali siano tenute al rispetto della riservatezza ed opportunamente formate;
- Tenere conto, utilizzando i materiali, i prodotti, le applicazioni od i servizi, dei principi di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di default;
- Adottare, durante l'intero ciclo di vita del trattamento, le misure di sicurezza suggerite dal Titolare ovvero proposte dal Responsabile ed approvate dal Titolare (art. 32 del Regolamento);
- Notificare al Titolare ogni violazione dei dati a carattere personale inerenti all'ambito contrattuale, secondo le modalità ed i tempi definiti tra le parti (artt. 33-34 del Regolamento);
- Assistere il Titolare nella realizzazione di analisi d'impatto relative alla protezione dei dati e nella consultazione preventiva dell'autorità di controllo (artt. 35-36 del Regolamento);
- Informare il Titolare, prima del trattamento, di eventuali obblighi giuridici a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto;

- Consentire l'esercizio dell'obbligo di controllo da parte del Titolare, del DPO o di terza parte da questi incaricata, garantendo la disponibilità a:

  fornire le evidenze di idoneità in termini di requisiti e competenze che assicurino il corretto svolgimento del trattamento, in adempimento al Regolamento ed alle normative di legge nazionali in materia di privacy;
  fornire tempestivamente tutte le informazioni e la documentazione comprovante il rispetto degli obblighi di legge e l'osservanza delle disposizioni impartite per iscritto dal Titolare della Struttura Sanitaria;
  consentire al Titolare o ad altri soggetti da lui delegati, di effettuare verifiche di controllo sui locali, sui sistemi e sulle infrastrutture informatiche impiegate per lo svolgimento dei trattamenti affidati;
  garantire gli interventi di adeguamento correttivo/migliorativo a seguito di eventuali rilievi o raccomandazioni conseguenti alle verifiche.
- Rispettare le condizioni descritte al paragrafo 5.3 per ricorrere ad altro responsabile del trattamento (sub-responsabile);
- Assistere attivamente il Titolare del trattamento mettendo a disposizione misure tecniche e organizzative che agevolino l'esercizio dei diritti dell'interessato di cui al capo III, artt. da 12 a 23 del Regolamento;
- Tenere per iscritto un registro di tutte le categorie di attività di trattamento effettuate per conto del Titolare nel rispetto di quanto previsto dal Regolamento (art. 30);
- Garantire, su richiesta del Titolare, la tempestiva restituzione o cancellazione di tutti i dati personali oggetto di trattamento, eliminando in maniera definitiva ed irreversibile anche tutte le copie esistenti, fatto salvo quanto eventualmente previsto dal diritto dell'Unione o degli Stati membri in materia di conservazione dei dati.

Contestualmente all'atto della designazione, la Struttura Sanitaria fornisce una copia, anche in formato elettronico, delle politiche, delle linee guida, delle procedure ed istruzioni operative emanate dal Titolare del trattamento, ritenute pertinenti con le finalità e l'operato del Responsabile.

Qualora la suddetta documentazione non sia sufficiente a regolamentare i trattamenti svolti dal Responsabile, la Struttura Sanitaria, con il supporto del DPO, provvederà ad impartire, in maniera chiara e documentata, ulteriori istruzioni di dettaglio.

5.2 Individuazione dei canali di comunicazione

Il referente per le relazioni con i Responsabili è il Titolare della Struttura Sanitaria, che si avvale della collaborazione e della consulenza del DPO.

Per quanto riguarda i canali di informazione, devono essere inviate tramite PEC le comunicazioni relative a:

- Richieste da parte degli Interessati effettuate nell'esercizio dei propri diritti di cui al capo III del Regolamento;
- Constatazione di violazioni di sicurezza riconducibili all'operato del Responsabile (data breach);
- Pronunciamenti, rilievi e sanzioni stabiliti dall'Autorità di Controllo (Garante della protezione dei dati personali), riguardanti i trattamenti e/o i dati personali riconducibili al Responsabile;
- Copia del Registro dei trattamenti redatto e aggiornato dal Responsabile, relativamente alle sole parti riconducibili all'oggetto contrattualizzato all'atto della designazione;
- Copia della documentazione e successivi aggiornamenti relativi alla/e valutazione/i di impatto e di rischio svolte dal Titolare della Struttura Sanitaria, riconducibili all'oggetto contrattualizzato all'atto della designazione;
- Proposte, di designazione di sub-responsabili, formulate dal Responsabile e sottoposte ad approvazione del Titolare della Struttura Sanitaria;
- Richieste di variazione sulle informative e sulle eventuali modalità di acquisizione dei consensi da parte degli Interessati del trattamento di dati personali riconducibili all'oggetto contrattualizzato all'atto della designazione.

- Ogni altra tipologia di comunicazione che si ritenga rilevante, ai fini di una corretta gestione dei trattamenti e dei dati personali riconducibili all'oggetto contrattualizzato all'atto della designazione.

Tutte le comunicazioni relative al trasferimento di informazioni personali devono essere effettuate adottando le misure di protezione previste nelle "Linee Guida per la Classificazione delle Informazioni e dei Trattamenti" [14].

Per quanto riguarda le comunicazioni relative all'operatività, quali ad esempio i processi di trattamento, la gestione dei sistemi informativi, la gestione delle credenziali di accesso e la cessazione di trattamenti, queste sono affidate ai referenti preposti dalla Struttura Sanitaria, individuati tra i Delegati/Referenti privacy nominati presso ciascuna Unità Operativa. I Delegati/Referenti privacy hanno la facoltà di inserire ulteriori riferimenti, in funzione delle specifiche esigenze operative. Ciascun Delegato/Referente privacy, dovrà redigere una lista contenente le informazioni di contatto (es. contesto del riferimento, nominativo, recapito telefonico e indirizzo di posta elettronica aziendale di ciascun referente). La lista con i riferimenti di contatto dovrà essere inoltrata al DPO della Struttura Sanitaria, che a sua volta provvederà ad inoltrarla a ciascun Responsabile designato.

5.3 Designazione dei sub-responsabili

Il Sub-responsabile, è una figura introdotta dal Regolamento che individua un ruolo stabilito in virtù di un contratto stipulato tra il Responsabile del trattamento ed uno o più soggetti esterni, sulla base di un rapporto che vincola il sub-responsabile al pieno rispetto delle istruzioni impartite dal Responsabile.

Un Responsabile designato dal Titolare non può designare altri Responsabili (sub-responsabili) che lo supportino nel trattamento dei dati personali a lui affidato, senza un'autorizzazione scritta da parte del Titolare. Il Responsabile ha dunque l'obbligo di comunicare preventivamente questa intenzione al Titolare, che ha la facoltà di opporsi (art.28 par. 2 del Regolamento). In particolare, nei casi in cui l'impresa che tratta dati personali per conto della Struttura Sanitaria, sia intenzionata a

subappaltare parte di tali attività, questa ha l'obbligo di comunicare al Titolare del trattamento la propria intenzione di designare uno o più sub-responsabili, individuati tra le imprese subappaltatrici. Nei casi in cui il Titolare ricorra a procedure di gara per l'acquisizione di servizi/prestazioni professionali, è opportuno esplicitare nel capitolato di gara:

- L'impegno da parte della società appaltatrice ad accettare il ruolo di Responsabile mediante contratto/atto giuridico di cui al paragrafo 5.1, seguito dalle istruzioni impartite dal Titolare, compreso l'impegno ad impartire istruzioni e vigilare sull'operato degli eventuali sub-responsabili;
- L'autorizzazione preliminare in via generale, concessa dalla stazione appaltante (Committente e Titolare del trattamento) alla società appaltatrice (futura Responsabile del trattamento), a designare sub-responsabili del trattamento, fermo l'obbligo di comunicare preventivamente il nome del sub-responsabile. Nel caso in cui il Responsabile faccia effettivo ricorso a sub-responsabili, egli si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti in merito a trattamenti effettuati in applicazione della normativa pro tempore vigente e che garantiscano la tutela dei diritti degli interessati. Il Responsabile si impegna altresì a stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili a mezzo dei quali il Responsabile descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con particolare riferimento alla disciplina sulla protezione dei dati personali.

L'autorizzazione o il diniego, da parte del Titolare della Struttura Sanitaria, alla designazione di sub-responsabili è indipendente da ogni altra autorizzazione al subappalto afferente alla commessa ovvero, l'autorizzazione al subappalto non costituisce implicita autorizzazione a designare sub-responsabili del trattamento.

Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti. Il Responsabile informa il Titolare di eventuali modifiche

previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Le clausole contrattuali che regolamentano la designazione del sub-responsabile da parte del Responsabile seguono, applicando le dovute contestualizzazioni, le medesime indicazioni valide per la designazione del Responsabile.

5.4 Individuazione dei trattamenti e dei dati personali affidati ai Responsabili

L'art. 30 del Regolamento stabilisce l'obbligo di redigere ed aggiornare nel tempo un "Registro delle attività di trattamento", estendendo tale obbligo anche al Responsabile, relativamente ai trattamenti svolti per conto del Titolare del trattamento (art.30 par.2).

Il Titolare ha l'obbligo di indicare i riferimenti del Responsabile nel proprio registro dei trattamenti, e a sua volta il Responsabile ha l'obbligo di indicare i riferimenti del Titolare del trattamento nel proprio "Registro di tutte le categorie di attività relative ai trattamenti". Il Titolare del trattamento può altresì fornire indicazioni vincolanti, circa le modalità di compilazione e manutenzione delle registrazioni dei trattamenti svolti dal Responsabile che opera per conto della Struttura Sanitaria.

A tale proposito il Titolare della Struttura Sanitaria ha la facoltà di indirizzare il Responsabile designato, fornendogli la documentazione relativa alle "Linee guida per la classificazione delle informazioni e dei trattamenti" [14] ed alle "Linee Guida per la gestione del Registro delle Attività di Trattamento" [15], in vigore presso la Struttura Sanitaria, richiedendo al Responsabile, se opportuno, la stesura di una specifica procedura operativa che recepisca tali indicazioni.

5.5 Valutazioni di impatto sulla protezione dei dati

L'art. 35 del regolamento introduce l'obbligo, per alcune tipologie di trattamenti e di dati, sottoposti a rischi rilevanti di violazioni della sicurezza, di svolgere le valutazioni di impatto sulla protezione dei dati (DPIA). Nel caso di trattamenti svolti da un Responsabile, l'art.35 par. 2 stabilisce che il Titolare si consulta con il Responsabile per effettuare le analisi di impatto. Pertanto, nei casi in cui il Titolare non disponga di tutte le informazioni necessarie a svolgere la DPIA, il Responsabile è tenuto, anche

per obbligo contrattuale (vedi par. 5.1 del presente documento), a fornire supporto e informazioni utili per la redazione della DPIA da parte del Titolare, secondo quanto definito nelle "Linee guida per la conduzione delle attività di Data Protection Impact Assessment" [16], emesse e pubblicate dalla Struttura Sanitaria.

Per agevolare l'espletamento di tali attività, il Responsabile deve fornire, su richiesta del personale incaricato delle valutazioni, tutta la documentazione utile, rendendosi disponibile anche ad accettare sessioni di intervista verbale e/o compilazione di questionari.

5.6 Comunicazione dei requisiti di sicurezza dei dati personali trattati

Al termine della attività di valutazione degli impatti sulla protezione dei dati (DPIA) il Titolare comunica al Responsabile:

- Gli esiti delle valutazioni in termini di rischio valutato allo stato dell'arte;
- L'eventuale lista dei requisiti necessari per il conseguimento di livelli accettabili di rischio.

A fronte di tali indicazioni, nel caso in cui siano stati formulati requisiti necessari al contenimento dei rischi entro i livelli di accettabilità stabiliti dal Titolare, il Responsabile deve fornire un Piano di Sicurezza, contenente le misure di sicurezza correttive ed i relativi tempi di attuazione necessari a soddisfare i suddetti requisiti. Qualora il Titolare, sentito anche il parere del DPO, non ritenga soddisfacente il Piano di Sicurezza proposto dal Responsabile e non raggiuga un accordo con quest'ultimo, egli ha la facoltà di sospendere l'erogazione del servizio di trattamento e, nei casi più gravi, di risolvere il contratto di affidamento, per motivi di non idoneità al trattamento dei dati personali.

Nel caso in cui, per scadenza dei termini contrattuali delle prestazioni/servizi erogati, un Responsabile del trattamento debba essere sostituito con altro Responsabile, quest'ultimo dovrà essere preventivamente informato sui requisiti di sicurezza necessari a garantire un'adeguata protezione dei dati, durante l'intero corso del trattamento. Nel caso in cui la Struttura Sanitaria indica una gara di appalto relativa al servizio di trattamento già erogato in precedenza da altri

fornitori, i requisiti di sicurezza dovranno essere dettagliati in un'apposita sezione del capitolato di gara dedicata ai "Requisiti di sicurezza per la protezione dei dati personali".

Il Titolare ha la facoltà di procedere ad un riesame della DPIA, nei casi in cui avvengano variazioni significative del rischio precedentemente valutato. In questo caso le relative variazioni, così come i nuovi eventuali requisiti di sicurezza, verranno comunicati al Responsabile, per l'adeguamento delle contromisure, attenendosi alle indicazioni già formulate nel presente paragrafo.

5.7 Gestione delle informative agli Interessati e raccolta dei consensi al trattamento

Qualora il Responsabile, nello svolgimento dei trattamenti a lui affidati, abbia la necessità di raccogliere dati personali direttamente presso gli Interessati, è obbligato ad informare gli interessati al momento della raccolta dei dati, secondo quanto disposto nell'art. 13 del Regolamento.

Per adempiere a tale obbligo, il Responsabile sottopone all'approvazione del Titolare della Struttura Sanitaria una bozza del documento di "Informativa all'Interessato", con l'obbligo di recepire tutte le eventuali modifiche richieste dal Titolare.

Qualora il Responsabile non sia nelle condizioni di redigere l'informativa, il Titolare del trattamento provvederà a redigerla per proprio conto ed a consegnarla al Responsabile, che assume l'impegno a comunicarla agli Interessati al momento della raccolta dei dati personali.

In ogni caso, spetta al Titolare della Struttura Sanitaria il compito di vigilare che le informative siano correttamente presentate nei modi e nei termini previsti dal Regolamento.

Le medesime considerazioni valgono per la raccolta dei consensi al trattamento, nei casi in cui le finalità del trattamento non rientrino in almeno una delle basi giuridiche enunciate all'art. 6, lettera b-c-d-e, del Regolamento. Per quanto concerne i trattamenti di dati personali sanitari, il Titolare della Struttura Sanitaria adotta i criteri valutativi per la raccolta del consenso, definiti nel provvedimento del Garante per la protezione dei dati personali n.55 del 7 Marzo 2019, "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario" [4].

Spetta in ogni caso al Titolare della Struttura Sanitaria, coadiuvato dal DPO, l'obbligo di verificare la corretta applicazione da parte del Responsabile, delle disposizioni di legge in materia di acquisizione del consenso dell'Interessato.

5.8 Gestione degli adempimenti per l'esercizio dei diritti dell'Interessato

L'esercizio dei diritti dell'interessato di cui agli artt. da 15 a 22 del Regolamento, qualora riguardi in tutto o in parte i trattamenti affidati al Responsabile, richiede la collaborazione attiva del Responsabile il quale dovrà estendere tale obbligo di collaborazione anche agli eventuali sub-responsabili designati.

Nell'ambito delle istruzioni che il Titolare della Struttura Sanitaria fornisce ai Responsabili, sono da ritenersi come adempimento contrattuale obbligatorio, l'osservanza scrupolosa delle disposizioni impartite mediante i seguenti documenti, aventi carattere di indirizzamento e regolamentazione:

- "Politica per la gestione dei diritti dell'interessato" [11], che stabilisce i criteri generali per l'applicazione degli articoli definiti al capo III del Regolamento;
- "Procedura per la gestione dei diritti dell'Interessato" [20], che stabilisce ruoli, responsabilità e modalità operative per la gestione dei diritti dell'Interessato presso la Struttura Sanitaria, in tutti i casi previsti dal Regolamento.

L'aderenza alle suddette linee guida e procedure si intende obbligatoriamente applicabile anche nei casi in cui le richieste dell'Interessato siano indirizzate solo al Responsabile e/o riguardino esclusivamente trattamenti a lui affidati.

5.9 Gestione delle violazioni della sicurezza dei dati personali

Qualora il Responsabile rilevi violazioni o sospette violazioni della sicurezza dei dati personali trattati per conto del Titolare della Struttura Sanitaria, egli è tenuto, anche per obbligo contrattuale sottoscritto in sede di designazione, a seguire scrupolosamente le disposizioni impartite dal Titolare, ed in particolare quelle documentate nella "Procedura per la gestione del data breach" [21] .

5.10 Gestione delle verifiche svolte dal Titolare

Al momento della designazione, il Responsabile assume l'impegno contrattuale ad acconsentire ed agevolare le verifiche effettuate dal Titolare del trattamento, dal DPO e/o da terze parti incaricate. Questo impegno è inoltre stabilito dall'art. 28, lettera h del Regolamento, che obbliga il Responsabile a "mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato".

A tale scopo il Titolare della Struttura Sanitaria fornisce, all'atto della designazione del Responsabile, le "Linee guida per la conduzione delle verifiche di conformità e adeguatezza delle misure preposte alla tutela dei dati personali" [17], nelle quali sono dettagliate le istruzioni per la conduzione delle verifiche, estendibili anche al contesto dei trattamenti svolti dal Responsabile.

Eventuali variazioni alle modalità operative definite nella suddetta linea guida, possono essere stabilite attraverso una procedura operativa specifica, che risponda in maniera più contestualizzata al modello organizzativo ed ai processi di trattamento svolti dal Responsabile.