



ISPRO

Istituto per lo studio, la prevenzione
e la rete oncologica

DELIBERAZIONE DEL DIRETTORE GENERALE

(Nominato con D.P.G.R.T. n. 72 del 29/04/2022)

N° 148 del 21/07/2022

Oggetto: Recepimento Decreto Regione Toscana n. 14528 del 30.06.2022 recante "Approvazione schema di accordo tra la Regione Toscana e le Aziende sanitarie disciplinante i trattamenti derivanti dalla gestione del Fascicolo Sanitario Elettronico (FSE), che non sono esplicitamente regolamentati nella normativa e nei citati atti conseguenti, nazionali e regionali, già adottati."	
Struttura Proponente	Direzione Aziendale
	S.S. Programmazione e Gestione Risorse Economiche
Responsabile del procedimento	Dott.ssa <i>Caterina Ferrari</i>
Estensore	Dott.ssa <i>Caterina Ferrari</i>
Allegati n. 1	

IMMEDIATAMENTE ESEGUIBILE



Conti Economici			
Spesa	Descrizione Conto	Codice	Anno Bilancio

Eseguibile a norma di Legge il 21 LUG. 2022

Pubblicato a norma di Legge il 21 LUG. 2022

Inviato al Collegio Sindacale il 21 LUG. 2022

IL DIRETTORE GENERALE

di questo Istituto per lo studio, la prevenzione e la rete oncologica, con sede in Via Cosimo il Vecchio 2 - 50139 Firenze, in forza del Decreto del Presidente della Giunta Regionale Toscana n. 72 del 29.04.2022

Visti:

- il Decreto Legislativo 30 dicembre 1992, n. 502 e successive modifiche ed integrazioni;
- la Legge Regionale Toscana 24 febbraio 2005, n. 40 di disciplina del Servizio Sanitario Regionale e successive modifiche ed integrazioni;
- la Legge Regionale Toscana 14 dicembre 2017, n. 74 che stabilisce che, a seguito dell'assorbimento delle funzioni dell'Istituto toscano tumori (ITT), l'Istituto per lo studio e la prevenzione oncologica assume la denominazione di Istituto per lo studio, la prevenzione e la rete oncologica (ISPRO);
- la Delibera GRT n. 490 del 7 maggio 2018 di parere favorevole sullo statuto e regolamento dell'ISPRO;
- la Delibera DG ISPRO n. 150 del 31 maggio 2018 di presa d'atto della Delibera GRT n. 490 del 7 maggio 2018 sopra menzionata;
- la Delibera DG ISPRO n. 11 del 13 gennaio 2020 con la quale è stato modificato/integrato il Regolamento di organizzazione e l'organigramma adottato con Delibera DG ISPRO n. 150 del 31 maggio 2018;
- la Delibera DG ISPRO n. 277 del 11 ottobre 2021 con la quale è stato modificato lo Statuto Aziendale, il Regolamento di organizzazione e funzionamento e l'organigramma dell'Istituto adottati con delibera del Direttore Generale n. 150 del 31/05/2018 e già modificati con Delibera del Direttore Generale n. 11 del 13/01/2020.

Premesso che:

- la Regione Toscana ha istituito il Fascicolo Sanitario Elettronico (FSE), con L.R. n. 40/2005, art. 76 bis;
- l'art. 2 del D.L. n. 179/2012 dà mandato alle Regioni di istituire il Fascicolo Sanitario Elettronico (FSE), fornendo specifici obblighi volti anche ad allineare i FSE che le Regioni avessero già costituito;
- il DPCM n. 178/2015 disciplina nel dettaglio il funzionamento del FSE;
- la Regione Toscana ha modificato con la L.R. n. 84/2015 il richiamato articolo 76 bis della L.R. 40/2005, al fine di adeguare il proprio FSE alla normativa nazionale;
- la normativa nazionale che istituisce il FSE definisce i ruoli data protection, in particolare della Regione e delle strutture che erogano prestazioni sanitarie che alimentano il FSE.

Considerato che:

- è necessario procedere alla sottoscrizione di un Accordo (Data Protection Agreement) tra Regione Toscana e Aziende sanitarie, che si proponga di disciplinare quei trattamenti derivanti dalla gestione del FSE che non sono esplicitamente regolamentati nella normativa e nei citati atti conseguenti, nazionali e regionali, già adottati;
- tale Accordo si rende indispensabile in quanto nei trattamenti in oggetto i diversi soggetti coinvolti qualificati dalla legge come autonomi titolari del trattamento ex art. 4 par. 1 n. 7 GDPR perseguono finalità distinte;
- la Regione Toscana ha approvato con Decreto Dirigenziale n. 13245 del 5.7.2022 lo schema di Accordo tra la Regione Toscana stessa e le Aziende sanitarie toscane (allegato quale Allegato A alla presente Delibera) disciplinante i trattamenti derivanti dalla gestione del Fascicolo Sanitario Elettronico (FSE) che non sono esplicitamente regolamentati nella normativa e nei citati atti conseguenti, nazionali e regionali, già adottati.

Rilevata la legittimità e la congruenza dell'atto con le finalità istituzionali di questo Ente, stante l'istruttoria effettuata;

Ritenuto opportuno dichiarare il presente atto immediatamente eseguibile, ai sensi dell'art. 42, comma 4, L.R. n. 40 del 24/02/2005 e s.m.i.;

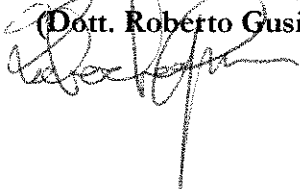
Con la sottoscrizione del Direttore Amministrativo e del Direttore Sanitario, ciascuno per quanto di competenza, ai sensi dell'art. 3 del Decreto Legislativo n. 502/1992 e ss.mm.ii.;

DELIBERA

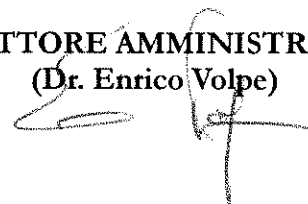
Per quanto esposto in narrativa che espressamente si richiama:

1. di recepire il Decreto Dirigenziale della Regione Toscana n. 13245 del 5.7.2022 , con cui è stato approvato lo schema di accordo tra la Regione Toscana e le Aziende sanitarie toscane - allegato quale Allegato A alla presente Delibera - disciplinante i trattamenti derivanti dalla gestione del Fascicolo Sanitario Elettronico (FSE) che non sono esplicitamente regolamentati nella normativa e nei citati atti conseguenti, nazionali e regionali, già adottati;
2. di disporre la relativa sottoscrizione dell'Accordo, di cui al punto precedente;
3. di dichiarare il presente atto immediatamente eseguibile, ai sensi dell'art. 42, comma 4, L.R. n. 40 del 24/02/2005 e s.m.i.;
4. di trasmettere il presente atto al Collegio Sindacale ai sensi dell'art. 42, comma 2, della L.R. n. 40/2005 e s.m.i. contemporaneamente all'inoltro all'albo di pubblicità degli atti di questo Istituto.

IL DIRETTORE SANITARIO
(Dott. Roberto Gusinu)



IL DIRETTORE AMMINISTRATIVO
(Dr. Enrico Volpe)



IL DIRETTORE GENERALE
(Avv. Katia Belvedere)



Elenco degli Allegati:

Allegato A: Schema di accordo tra la Regione Toscana e le Aziende Sanitarie Toscane

STRUTTURE AZIENDALI DA PARTECIPARE:

Tutte le strutture ISPRO

Data Protection Agreement (tra Titolari Autonomi)

Clausole Contrattuali Titolare – Titolare
(Titolari Autonomi)

Scopo del documento

Il presente documento ha per obiettivo la regolamentazione della governance sul Fascicolo Sanitario Elettronico, istituito in Regione Toscana con legge regionale n. 40/2005, art. 76 bis, tramite un accordo (Data Protection Agreement), che si propone di disciplinare quei trattamenti derivanti dalla gestione del FSE che non sono esplicitamente regolamentati nella normativa e negli atti conseguenti, nazionali e regionali, già adottati. Tale accordo si rende necessario in quanto nei trattamenti in oggetto i diversi soggetti che vi intervengono, qualificati dalla legge come titolari del trattamento ex art. 4 par. n. 7 GDPR, perseguono distinte finalità.

Si tratta di due tipologie di soggetti giuridicamente diversi (Regione Toscana e Aziende Sanitarie) che hanno la piena titolarità dei trattamenti secondo quanto stabilito sulla base di specifiche norme e finalità che ne determinano sia la titolarità che la liceità. Questi soggetti Titolari ognuno per le proprie finalità trattano, per le parti di competenza, dati personali e pertanto concordano di sottoscrivere un accordo, nel quale si dia atto, in particolare, del riconoscimento reciproco della titolarità nell'eseguire quei trattamenti, dei dati condivisi, delle misure adottate a garantire un livello di sicurezza adeguato al rischio, fra cui un canale di comunicazione sicuro e la corretta gestione e manutenzione dei repository, delle procedure di presa in carico delle richieste degli interessati, nonché della procedura da seguire in caso di data breach.

Premessa

Il trattamento in considerazione è il Fascicolo Sanitario Elettronico (FSE), istituito e disciplinato dalla seguente normativa:

Normativa nazionale

- Fascicolo sanitario elettronico: articolo 12 del D.L. 18/10/2012, n. 179, convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 221, e successive modificazioni
- Decreto-legge n. 69 del 21 giugno 2013 “Disposizioni urgenti per il rilancio dell’economia”
- Regolamento in materia di fascicolo sanitario elettronico: Decreto del presidente del Consiglio dei ministri 29 settembre 2015, n. 178
- Decreto 4 agosto 2017 “Modalità tecniche e servizi telematici resi disponibili dall’infrastruttura nazionale per l’interoperabilità del Fascicolo sanitario elettronico (FSE) di cui all’art.12, comma 15-ter del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n.221”
- Informativa semplificata per gli assistiti art. 1, comma 382 della Legge di Bilancio 2017 e artt. 14-17 DM 4/8/2017 “Disponibilità dei dati del Sistema Tessera Sanitaria nel FSE”
- Decreto del 25 ottobre 2018 “Modifica del decreto ministeriale 4 agosto 2017, concernente le modalità tecniche e i servizi telematici resi disponibili dall’infrastruttura nazionale per l’interoperabilità del Fascicolo sanitario elettronico (FSE)”
- Decreto-Legge n. 34/2020 "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19" convertito con modificazioni dalla L. 17 luglio 2020, n. 77
- Decreto-Legge n. 137 del 28 ottobre 2020 "Ulteriori misure urgenti in materia di tutela della salute, sostegno ai lavoratori e alle imprese, giustizia e sicurezza, connesse all'emergenza epidemiologica da Covid-19."
- Decreto del Ministero delle Finanze attuativo del 3 novembre 2020, “Modalità attuative delle disposizioni di cui all'articolo 19, comma 1, del decreto-legge n. 137 del 28 ottobre 2020 (c.d. "Decreto Ristori”).”

Normativa regionale

- Art. 76 bis L.R. 40/2005 «Fascicolo sanitario Elettronico»
- DGR n.125 del 23 febbraio 2009 “PSR 2008/2010 – punto 4.1.2 – approvazione progetto Carta Sanitaria Elettronica”
- Decreto Dirigenziale n. 1501 del 1° aprile 2010 “Definizione dell’Architettura del Fascicolo Sanitario Elettronico”

Sintesi del disposto normativo

Nello specifico, la normativa prevede che il FSE, istituito dalla Regione Toscana, nel rispetto della normativa vigente in materia di protezione dei dati personali, persegua le seguenti finalità:

- a) diagnosi, cura e riabilitazione;
- a-bis) prevenzione;
- a-ter) profilassi internazionale;
- b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
- c) programmazione sanitaria cosiddetta di seguito attività di governo, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

Nello specifico:

- le finalità di cui alla lettera a) sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali e da tutti gli esercenti le professioni Sanitarie.
- le finalità di cui alla lettera a-bis) sono perseguite dai soggetti del Servizio sanitario nazionale e dei servizi socio-sanitari regionali, dagli esercenti le professioni sanitarie nonché dagli Uffici della Regione Toscana competenti in materia di prevenzione sanitaria e dal Ministero della salute.
- le finalità di cui alla lettera a-ter) sono perseguite dal Ministero della Salute.
- le finalità di cui alle lettere b) e c) è perseguita da Regione Toscana, nonché dal Ministero del lavoro e delle politiche sociali e dal Ministero della salute nei limiti delle rispettive competenze attribuite dalla legge, senza l'utilizzo dei dati identificativi degli assistiti presenti nel FSE.

Responsabilità connesse al trattamento

Titolari del trattamento

In sintesi, nell'ambito del FSE, istituito da Regione Toscana, risultano le seguenti titolarità:

- Finalità di cura: Titolari del trattamento dei dati, sono le aziende sanitarie tramite, ciascuno per le attività e nei limiti delle rispettive competenze, gli operatori del Servizio sanitario nazionale e dei servizi socio-sanitari regionali che operano all'interno delle Aziende stesse e che prendono in cura gli assistiti.
- Finalità di ricerca: Giunta Regionale.
- Finalità di governo: Giunta Regionale.

Responsabili del trattamento ex articolo 28

I responsabili del trattamento ex art. 28 GDPR sono:

- Il soggetto gestore dell'infrastruttura hardware e software, collocata presso il centro servizi TIX di Regione Toscana
- DXC, il soggetto incaricato dello sviluppo del sistema di cui al seguente contratto: “Servizi inerenti il Sistema Informativo Sanitario, Socio-sanitario e Sociale di Regione Toscana”, CIG derivato 8014359A42, sottoscritto in data 30 settembre 2019 fra Regione Toscana ed Enterprise Services Italia S.r.l. quale mandataria del Raggruppamento Temporaneo di Imprese sottoscrittore il Contratto Quadro CONSIP – Sistemi Gestionali Integrati per le Pubbliche Amministrazioni. Lotto 5. ID SIGEF 1607
- Covisian SPA e Engineering Ingegneria informatica SPA che svolge le attività di help desk di primo livello per il FSE: “Adesione alla convenzione stipulata da Consip S.p.A. relativa a Servizi di Contact Center in Outsourcing 2 lotto 2 per le Amministrazioni delle regioni Emilia Romagna, Toscana, Marche, Umbria - CIG 68205564DD con il R.T.I. costituito da Covisian S.p.A. e Engineering Ingegneria Informatica S.p.A. per “Servizi di contact center per il supporto ai cittadini per l’accesso ai servizi on-line di Regione Toscana” CIG derivato 9158333F76 - CUP D19B22000070002”
- L'Ente di supporto tecnico e amministrativo regionale (ESTAR),. Estar gestisce l’infrastruttura di comunicazione degli eventi sanitari prodotti dalle Aziende e inviate al FSE
- ESTAR assicura il collegamento e la gestione delle componenti infrastrutturali e dei servizi seguiti per conto delle Aziende Sanitarie, e per i quali è stato individuato quale Responsabile del trattamento, nella interazione con i servizi contrattualizzati da Regione Toscana per la realizzazione del FSE
- Come meglio esplicitato all’art. 9, i singoli Titolari provvederanno a nominare i fornitori contrattualizzati da Regione Toscana quali Responsabili per i trattamenti di rispettiva competenza. Nell’ambito della loro titolarità, per conto delle Aziende Sanitarie la nomina degli ulteriori responsabili sarà effettuata da ESTAR; i fornitori contrattualizzati da Regione Toscana saranno nominati quali Sub-Responsabili del trattamento.

**Accordo Data Protection fra Titolari Autonomi
(Data Protection Agreement)**

TRA

Regione Toscana P.I. 01386030488, con sede legale in Piazza Duomo, 10 Firenze, in persona Dirigente Responsabile del settore Sanità digitale e innovazione Ing. Andrea Belardinelli, in qualità di delegato del titolare ex DGR 585/2018

E

L'Azienda USL Toscana Nord Ovest, con sede legale in via A. Cocchi, 7/9 - 56124 Pisa - P.I. e C.F. 02198590503, rappresentata dal Direttore generale Maria Letizia Casani

E

L'Azienda USL Toscana Centro, con sede legale in Piazza Santa Maria Nuova, 1 - 50121 Firenze – P.I. e C.F. 06593810481, rappresentata dal Direttore generale Paolo Morello Marchese

E

L'Azienda USL Toscana Sud Est, con sede legale in via Curtatone, 54 - 52100 Arezzo - P.I. e C.F. 02236310518, rappresentata dal Direttore generale Antonio D'Urso

E

L'Azienda Ospedaliero-Universitaria Careggi, con sede legale in Largo Brambilla, 3 - 50134 FIRENZE – P.I. e C.F. 04612750481, rappresentata dal Direttore generale Rocco Donato Damone

E

L'Azienda Ospedaliero-Universitaria Pisana, con sede legale in Via Roma n. 67 56126 Pisa – P.I. e C.F. 01310860505, rappresentata dal Direttore generale Silvia Briani

E

L'Azienda Ospedaliero-Universitaria Senese, con sede legale in Strade delle Scotte,14 - 53100 Siena – P.I. e C.F. 00388300527, rappresentata dal Direttore generale Antonio Davide Barretta

E

L'Azienda Ospedaliero-Universitaria Meyer, con sede legale in Viale Pieraccini 24 - 50139 Firenze – P.I. e C.F. 02175680483, rappresentata dal Direttore generale Alberto Zanobini

E

L'Istituto per lo studio, la prevenzione e la rete oncologica (ISPRO), con sede legale in Via Cosimo Il Vecchio 2 - 50139 Firenze – P.I. 05872050488 e C.F. 94158910482, rappresentata dal Direttore generale Katia Belvedere

E

La Fondazione Toscana Gabriele Monasterio (FTGM), con sede legale in Via Trieste, 41 - 56126 Pisa – P.I. 01851550507 e C.F. 93062260505, rappresentata dal Direttore generale Marco Torre

(di seguito, congiuntamente, le Parti)

Art. 1

Oggetto e premesse

Le premesse costituiscono parte integrante e sostanziale del presente Accordo.

Oggetto del presente accordo è la regolamentazione, per le parti di rispettiva competenza di Regione e delle Aziende sanitarie, del FSE ex d.l. 179/2012 s.m.i., in particolare:

- il riconoscimento reciproco della titolarità autonoma nell'eseguire i trattamenti di seguito specificati,
- quali sono i dati condivisi,
- le misure adottate a garantire un livello di sicurezza adeguato al rischio, fra cui un canale di comunicazione sicuro,
- la corretta gestione e manutenzione dei repository,
- le procedure di presa in carico delle richieste degli interessati,
- la procedura da seguire in caso di data breach.

Le Parti si danno reciprocamente atto di conoscere ed applicare, nell'ambito delle proprie organizzazioni, tutte le norme vigenti ed in fase di emanazione in materia di trattamento dei dati personali, sia primarie che secondarie, rilevanti per la corretta gestione del Trattamento, ivi compreso il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito "GDPR") e il Decreto Legislativo n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali.

Le parti si danno reciprocamente atto che il trattamento dei dati oggetto del presente DPA risponde ai principi di liceità determinati dalle specifiche norme richiamate in premessa.

Le parti si danno reciprocamente atto che lo scambio di dati oggetto del presente DPA è conforme alle disposizioni, alle linee guida e alle regole tecniche previste per l'accesso, la gestione e la sicurezza dei dati dalla normativa in materia di amministrazione digitale (in specifico, d.lgs. 82/2005, lr 1/2004 e relative linee guida e regole tecniche) e dalle altre norme di riferimento.

Le componenti infrastrutturali, gestionali e di supporto che compongono l'intera architettura del FSE, al fine di garantire la fruibilità, la tempestività delle risposte e l'efficienza/efficacia dei processi collegati, necessitano l'implementazione di una opportuna gestione unitaria delle attività di manutenzione e assistenza delle componenti tecniche e dei processi di assistenza ed help desk alla utenza, rappresentata dai cittadini e dal personale sanitario autorizzato ad accedere ai dati.

Regione Toscana, ove non diversamente concordato, in relazione al ruolo istituzionale e ai compiti assegnati dalla normativa, contrattualizza tutti i servizi necessari ad una corretta gestione del servizio.

ESTAR assicura il collegamento e la gestione delle componenti infrastrutturali e dei servizi seguiti per conto delle Aziende Sanitarie, e per i quali è stato individuato quale Responsabile del

trattamento, nella interazione con i servizi contrattualizzati da Regione Toscana per la realizzazione del FSE.

Come meglio esplicitato all'art. 9, i singoli Titolari con specifici atti, provvederanno a nominare i fornitori contrattualizzati da Regione Toscana quali Responsabili per i trattamenti di rispettiva competenza. La nomina sarà essere effettuata da ESTAR, per conto delle Aziende Sanitarie nell'ambito della loro titolarità, i fornitori contrattualizzati da Regione Toscana saranno nominati quali Sub-Responsabili del trattamento.

I dati sanitari e i documenti che li contengono trattati per finalità di prevenzione, diagnosi, cura, vengono gestiti dai soggetti che li producono come ad esempio le Aziende Sanitarie, tramite trasferimento in repository prestazionali all'interno del TIX (Tuscany Internet Exchange) che rientrano nel dominio delle aziende (Titolari del dato). Tali dati sono importati nei relativi repository in modo pseudonimizzato. Al momento in cui i MMG/PLS provvederanno all'alimentazione del FSE con il patient summery, tale dato andrà a popolare i repository delle Aziende territoriali di riferimento.

Il FSE è costituito da un indice che lega ogni cittadino a tutte le prestazioni che lo riguardano e garantisce la visibilità delle stesse. Questo sottosistema rientra tra le attività tecniche infrastrutturali contrattualizzate da Regione Toscana.

I dati personali identificativi sono fisicamente divisi dai dati prestazionali; la loro ricomposizione avviene, all'accesso del cittadino (o degli operatori abilitati) alle informazioni, mediante l'indice che lega l'identificativo univoco dell'assistito agli identificativi delle prestazioni a lui erogate.

Per le finalità di ricerca e governo, i dati personali identificativi relativi all'assistito non vengono correlati con i dati sanitari.

I dati sono gestiti su una infrastruttura tecnologica composta da sistemi in disaster recovery, sistemi operativi linux cento os per le componenti application server e Linux Oracle per la gestione della base di dati, Oracle 11.2.0.4 o successive per la base di dati, apache, tomcat e jboss per il front end nelle ultime versioni alla data.

Art. 2

Rapporti fra autonomi Titolari di trattamento dati

Le Parti tratteranno in via autonoma i dati personali oggetto della condivisione, per le finalità connesse alla gestione del FSE.

Le parti, in relazione agli impieghi dei predetti dati nell'ambito della propria organizzazione, assumeranno, pertanto, la qualifica di Titolare autonomo del trattamento ai sensi dell'articolo 4, nr. 7) del GDPR, sia fra di loro che nei confronti dei soggetti cui i dati personali trattati sono riferiti.

Art. 3

Tipologia di dati oggetto del trattamento

I tipi di dati personali trattati in ragione delle attività in oggetto sono:

- per finalità di titolarità delle AA.SS: in riferimento al DPCM 29 settembre 2015, n. 178 sono così suddivisi:
 - o dati personali:
 - dati identificativi e amministrativi (Nome, Cognome, data di nascita, CF, sesso, residenza, domicilio, cittadinanza, ASL di residenza, ASL di domicilio, medico curante MMG o pediatra, azienda di assistenza)
 - o categorie particolari di dati personali che concorrono all'alimentazione del FSE sulla base della normativa vigente.

- per finalità di titolarità di Regione Toscana: i dati trattati sono esclusivamente dati pseudonimizzati.

Tali dati sono privati dei dati identificativi quali:

- o nome e cognome;
- o codice fiscale;
- o giorno e mese di nascita per gli assistiti con età superiore all'anno compiuto;
- o giorno di nascita per gli assistiti con età inferiore all'anno compiuto;
- o estremi di documenti di identità;
- o via e numero civico di residenza o di domicilio;
- o recapiti, telefonici o digitali, personali;
- o copie per immagine su supporto informatico di documenti analogici;
- o informazioni non strutturate di tipo testuale;
- o informazioni non strutturate di tipo grafico, sia statiche (immagini) che dinamiche (video).

Art. 4

Rispetto della normativa

In quanto Titolari autonomi del trattamento, le parti sono tenute a rispettare tutte le normative rilevanti sulla protezione ed il trattamento dei dati personali che risultino applicabili ai rapporti reciproci sulla base del presente DPA. Le Parti sono, altresì, tenute al rispetto della normativa in materia di amministrazione digitale e in materia di accesso, gestione e sicurezza dei dati.

Art. 5

Misure di sicurezza

Le parti concordano sull'adeguatezza delle misure di sicurezza messe in atto al fine di garantire lo scambio sicuro dei dati.

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, le Parti si impegnano ad adottare misure di sicurezza tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono:

- Controllo degli accessi logici

Relativamente all'accesso degli utenti: amministratori di sistema Utente password protocollo SSH all'interno di una rete privata di management e protetta da due livelli di firewall (isolata) - incaricati delle aziende sanitarie tramite CNS o SPID di livello 3 L'amministratore del sistema è autorizzato dal Responsabile dell'infrastruttura tecnologica con profili e persone distinte per dati anagrafici e dati non anagrafici in quanto l'archivio complessivo è soggetto a pseudonimizzazione.

- Archiviazione

I dati sono mantenuti in linea su archivio relazionale Oracle, vengono effettuate politiche di salvataggio attraverso transaction log e backup completo bisettimanale con retention 30 giorni. Le modifiche integrazioni e cancellazioni sono storicizzate. Alla morte dell'interessato il fascicolo viene chiuso all'accesso e i dati verranno rimossi dopo 30 anni.

- Crittografia

- Pseudonimizzazione

I dati sono archiviati in due separati motori Data base su hw diversi per la componente identificativa della persona e per i dati relativi al fascicolo, solo in fase di accesso alla lettura delle persone autorizzate il sistema provvede alla lettura dei due distinti data base e la ricomposizione del contenuto solo sotto il profilo logico e senza conservazione in alcun stato di persistenza (es. Cache).

- Tracciabilità

- Tutti gli eventi sia da parte di utenti del sistema sia degli amministratori sono tracciati e conservati per 24 mesi: in security logger archsight elasticsearch a livello applicativo.

- Vulnerabilità

Il software applicativo è inventariato in archivio dedicato e contenute sia la componente sorgente, sia l'eseguibile sia la documentazione. Associati la continuity integration per la verifica della qualità del codice sorgente. attivazione processi di vulnerability assessment sugli asset che ospitano il codice in esecuzione, (sistemi operativi, e componenti middleware) sia al vulnerability assessment dell'applicativo volto a verificare la presenza di componenti applicative a rischio di sicurezza.

- Lotta contro il malware

Presenza di componenti infrastrutturali e perimetrali di protezione quali firewall web application firewall, in corso di attivazione controlli su ip reputation, antivirus con funzionalità sandblast e zero Day protection.

- Sicurezza dei siti web

Utilizzo di protocolli TLS per le comunicazioni web application firewall, e vulnerability assessment applicativi.

- Manutenzione

Regolata sulla base di quanto contrattualizzato applicando le buone e migliori pratiche di cui alla certificazione iso 27001 presente sul TIX.

La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

A tal fine si impegnano a collaborare ad assistere ed assicurare la piena, fattiva e puntuale collaborazione.

Le Parti concordano sulla necessità di una specifica procedura per la gestione delle richieste di modifica/cancellazione, disciplinata dal successivo articolo 6.

Art. 6

Richieste degli interessati

Al fine di meglio supportare i cittadini in difficoltà nell'utilizzo/accesso del FSE, le parti concordano per l'istituzione di un help desk dedicato a ricevere e gestire le richieste e le segnalazioni dei cittadini, in stretto raccordo con le Aziende sanitarie.

Il primo livello di help desk è svolto attraverso il citato responsabile "Covisian" che ha il compito di raccogliere le segnalazioni dei cittadini.

Le segnalazioni sono classificate in base all'urgenza e all'argomento. In caso di problemi sui dati, il primo livello inoltra la segnalazione all'Azienda sanitaria che ha erogato la prestazione in quanto titolare del dato e, in caso di scambio dati, anche al DPO dell'azienda stessa in modo che possa vigilare sui tempi di risposta e intraprendere immediatamente le iniziative necessarie.

Se la risoluzione del ticket comporta un accesso ai repository prestazionali per effettuare una attività di cancellazione o modifica o riassegnazione, l'Azienda sanitaria deve rivolgersi all'help desk di secondo livello (denominato helpsis) gestito dal citato responsabile DXC che accede per suo conto ai dati ed effettua quanto richiesto.

Gli SLA degli help desk sono definiti nei rispettivi documenti contrattuali con i fornitori.

Art. 7

Procedura Operativa per la gestione dei dati errati/scambiati - Data Breach

La procedura corretta in caso di dati scambiati consiste nel re-inviare l'evento con la stessa chiave e con l'identificativo del soggetto corretto (ID), sistemando automaticamente tutta la situazione sia a livello locale, che su INI.

Tuttavia, considerato che Estar e le Aziende sanitarie, non sono al momento in grado di attivare la procedura automatica sopra indicata, attualmente il procedimento richiede un'attività di cancellazione logica manuale dei dati e la correzione, sempre manuale, sul livello nazionale.

Nelle more di un servizio che consenta alle aziende di essere completamente autonome nell'attività di modifica/correzione, le Aziende ed Estar possono inoltrare le loro richieste di correzione direttamente all'help-desk tecnico, via mail: helpsis@regione.toscana.it, indirizzo gestito dal sopra citato responsabile del trattamento DXC, con la stessa chiave: SPCOOPID e l'identificativo del soggetto corretto (ID).

Nel caso di errata attribuzione di dati, il messaggio di richiesta dovrà riportare, sia gli estremi del dato da cancellare, sia gli estremi del dato ritenuto corretto dall'azienda.

In considerazione della concreta probabilità che l'episodio di dati errati/scambiati sia configurabile quale data breach ex art. 4 par. n. 12 RGPD, il titolare del trattamento competente, al momento dell'attivazione dell'help desk di secondo livello (helpsis) con la procedura precedentemente descritta, indica nell'oggetto della email "DATI ERRATI FSE - URGENTE-DB" e il fornitore è chiamato a rispondere nei tempi previsti dall'articolo 33 del RGPD, a fornire tutte le informazioni necessarie, fra cui quelle indicate dall'art. 33 par. 3 RGPD e a collaborare nell'eventuale procedimento di notifica all'Autorità Garante per la protezione dei dati personali.

I contatti dell'help desk di primo livello sono i seguenti:

Numero verde: 800 004477

Numero nero: 06 77619420

mail: help.cse@regione.toscana.it (per problemi tecnici e di accesso)

mail: help.saluteonline@regione.toscana.it (per informazioni e problemi sui dati)

Lun-Ven: 09:00 – 19:00, Sab: 09:00 – 13:00

I contatti dell'help desk di secondo livello (helpsis) sono i seguenti:

mail: helpsis@regione.toscana.it

Numero verde: 800558080

Fax: 0691868952

Lun-Sab: 08:00 – 18:00

Art. 8

Nomina dei Responsabili ai sensi dell'articolo 28 del RGPD

Le Parti si impegnano a nominare i Responsabili richiamati in premessa secondo le modalità di cui all'articolo 28 del RGPD per le finalità di propria competenza.

I singoli Titolari provvederanno a nominare i fornitori contrattualizzati da Regione Toscana, quali Responsabili per i trattamenti di rispettiva competenza.

Art. 9

Istruzioni integrative da parte delle Aziende sanitarie ad Estar

La L.R.T. n. 26/2014 al capo 1 "Modifiche alla legge 24 febbraio 2005 n. 40 (Disciplina del Servizio Sanitario Regionale) istituisce l'ESTAR per l'esercizio delle funzioni tecniche, amministrative e di supporto delle aziende sanitarie, degli enti del servizio sanitario regionale e delle società della salute, attribuendo, tra le materie di competenza quelle relative alle "tecnologie dell'informazione e della comunicazione".

Con delibera della Giunta Regionale Toscana n. 785/2016 sono state individuate in via preliminare, fra le materie elencate nell'art. 101 della legge 40/2005 e ss.mm.ii., quelle in cui Estar tratta i dati personali in qualità di Titolare del trattamento e quelle nelle quali tratta i dati personali in qualità di Responsabile del trattamento dell'azienda sanitaria titolare del trattamento.

Con delibera della Giunta Regionale Toscana n. 742/2018 si stabilisce che le aziende sanitarie nominino Estar quale Responsabile del trattamento dei dati personali con proprio atto e sottoscrivano con lo stesso Estar una convenzione ove siano specificate finalità e durata del trattamento, tipi di dati personali e categorie di interessati, nonché obblighi del responsabile e del titolare.

Fra i trattamenti che Estar effettua per conto delle Titolari AASS rientra il "Supporto alla produzione di flussi informativi e RFC" all'interno del quale sono ricompresi anche i flussi e gli eventi destinati al popolamento del FSE, compreso il supporto per interventi di correzione e reinvio dei suddetti flussi ed eventi prodotti dagli applicativi sanitari.

In considerazione del suddetto quadro normativo, valutata la necessità di assicurare il corretto dialogo tecnico tra le professionalità presenti in Estar, con i fornitori dei servizi contrattualizzati da Regione Toscana, in modo da dare unitarietà alla complessa infrastruttura tecnologica di dispiegamento del FSE; e nell'ottica di assicurare efficienza nella verifica, correttezza e validazione del processo di disponibilità nel FSE degli eventi inviati; nella catena di supporto per la fruizione del servizio agli operatori sanitari e ai cittadini e che accedono al FSE; assicurare tempestività nella risoluzione di problematiche che dovessero verificarsi nella disponibilità e nella efficienza dei servizi tecnici, le Aziende sanitarie concordano di avvalersi di Estar, quale Responsabile del Trattamento, per le nomine di loro competenza degli ulteriori Responsabili.

Estar provvederà nominando i fornitori elencati in premessa e già contrattualizzati da Regione Toscana ai sensi del paragrafo 4 articolo 28 del RGPD.

Il contenuto del presente atto, per quanto in correlazione, con particolare riferimento all'art. 5 (Misure di Sicurezza), nonché agli articoli 6 (Richieste degli interessati) e 7 (Gestione Data Breach), rappresenta integrazione delle istruzioni già ricevute da Estar da parte delle Aziende Sanitarie nei precedenti atti di nomina quale Responsabile del Trattamento.

Art. 10

Obblighi del personale autorizzato

Le parti si impegnano a far sì che l'accesso ai dati personali oggetto dello scambio sia consentito solo a coloro e nella misura in cui ciò sia necessario per l'esecuzione del contratto/Convenzione/protocollo di intesa, e che l'uso dei dati personali da parte del soggetto utilizzatore rispetti gli stessi impegni assunti dal produttore riguardo alla conformità legale del trattamento e la sicurezza dei dati trattati con misure adeguate alla tipologia dei dati degli interessati e dei rischi connessi.

Ognuna delle parti individua un proprio referente tecnico, responsabile dell'accesso, della gestione e della sicurezza dei dati e dell'applicazione delle relative norme, linee guida e regole tecniche, tenuto a comunicare tempestivamente all'altra parte modifiche, aggiornamenti, esigenze, problematiche, incidenti e quanto ritenuto necessario nella corretta gestione dei dati, al fine di assicurarne la conformità ai principi e alle disposizioni normative di riferimento.

Art. 11

Responsabilità

Fatto salvo quanto previsto come inderogabile dalla legge, nessuna responsabilità sarà imputabile a ciascun Titolare per i trattamenti operati da altro Titolare eccettuati i casi di cattiva gestione o maltrattamento nella fase di raccolta originaria dei dati personali. Ferma restando la responsabilità assunta dai singoli Titolari verso i terzi e verso gli altri Titolari firmatari, ciascun Titolare si obbliga a manlevare e tenere indenne gli altri – per qualsiasi danno, incluse spese legali – che possa derivare

da pretese avanzate da terzi - inclusi i soggetti cui i dati personali trattati sono riferiti - a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento.

Art. 12

Impostazione organizzativa

Le parti si garantiscono reciprocamente che i dati trattati da ciascuna di esse in esecuzione del presente DPA formano oggetto di puntuale verifica di conformità alla disciplina rilevante in materia di trattamento di dati personali - ivi compreso il GDPR - , alla normativa in materia di amministrazione digitale e in materia di accesso, gestione e sicurezza dei dati e si impegnano altresì alla ottimale cooperazione reciproca nel caso in cui una di esse risulti destinataria di istanze per l'esercizio dei diritti degli interessati previsti dall'articolo 12 e ss. del GDPR, applicabili al presente trattamento di seguito elencati:

- verificare se i dati presenti nel FSE sono esatti, completi e aggiornati;
- richiedere l'accesso ai Suoi dati personali, la loro rettifica e la loro integrazione;
- richiedere di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato dei Suoi dati;
- revocare il consenso al trattamento dei dati che La riguardano (in tal caso rimane salva la liceità dei trattamenti svolti prima della revoca del consenso).

Si impegnano alla medesima cooperazione in caso di richieste delle Autorità di controllo che riguardino ambiti di trattamento di competenza dell'altra parte.

Art. 13

Durata

Il presente Data Protection Agreement ha durata di tre anni dalla sua sottoscrizione rinnovabile tacitamente, salvo richiesta di una delle parti da inoltrare entro 60 giorni dalla data di scadenza.

Art. 14

Rescissione

La rescissione del presente DPA avviene per istanza di parte qualora, la stessa ritenga che lo scambio di informazioni leda per qualsivoglia motivo i legittimi diritti degli interessati

Art. 15

Notifica

Il presente accordo sarà notificato ai soggetti che a vario titoli sono chiamati in causa dal presente accordo per gli adempimenti di loro competenza.

Firma per la Regione Toscana:

Firma per l'Azienda USL Toscana Nord Ovest:

Firma per l'Azienda USL Toscana Centro:

Firma per l'Azienda USL Toscana Sud Est:

Firma per l'Azienda Ospedaliero-Universitaria Careggi:

Firma per l'Azienda Ospedaliero-Universitaria Pisana:

Firma per l'Azienda Ospedaliero-Universitaria Senese:

Firma per l'Azienda Ospedaliero-Universitaria Meyer:

Firma per l'Istituto per lo studio, la prevenzione e la rete oncologica:

Firma per la Fondazione Toscana Gabriele Monasterio: