

CONVENZIONE PER LA GESTIONE DEI DATI PERSONALI DEI SOGGETTI RESIDENTI NEL TERRITORIO DELL'UNIONE TERRE D'ARGINE CHE VERSINO IN CONDIZIONI DI FRAGILITÀ E/O DI NON AUTOSUFFICIENZA

L'anno 2019 addì 22 del mese di maggio 2019 in Carpi, presso la sede dell'Unione delle Terre d'Argine in C.so A. Pio n. 91,

TRA

l'Azienda Unità Sanitaria Locale (AUSL) di Modena (di seguito "l'AUSL" o "Soggetto Erogatore" o, congiuntamente all'Unione Terre D'Argine, "le Parti") con sede legale in Modena, cod. fiscale/PI: 02241850367, rappresentata dalla dr.ssa Stefania Ascari, domiciliata per la carica in Carpi, via G. Molinari, 2, la quale dichiara di agire in nome, per conto e nell'esclusivo interesse dell'Ente

E

l'Unione Terre d'Argine (di seguito "l'Unione" o "Soggetto Fruitore", o congiuntamente all'AUSL, "le Parti") con sede legale in Carpi, Corso A. Pio n. 91 rappresentata dal Presidente pro-tempore Paola Guerzoni, nata a Modena il 31/05/1965, C.F.GRZPLA65E71F257M;

RICHIAMATI

- il D. Lgs. 117/2017 "Codice del Terzo settore";
- gli articoli 1, comma 1-bis, 11 e 15 della L. 241/1990 e s.m.i. "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- il D. Lgs. 267/2000 e s.m.i. "TUEL";
- la L. 328/2000 "Legge quadro per la realizzazione del sistema integrato di interventi e servizi sociali", che sancisce il diritto delle persone e delle famiglie ad usufruire di un sistema integrato di interventi e servizi sociali, promuovendo interventi per garantire la qualità della vita, pari opportunità, non discriminazione e diritti di cittadinanza, prevenendo, eliminando o riducendo le condizioni di disabilità, di bisogno e di disagio individuale e familiare, derivanti da inadeguatezza di reddito, difficoltà sociali e condizioni di non autonomia, in coerenza con gli articoli 2, 3 e 38 della Costituzione;
- la L. R. 2/2003 "Norme per la promozione della cittadinanza sociale e per la realizzazione del sistema integrato di interventi e servizi" che all'art. 20, comma 2, sottolinea il ruolo del Volontariato nella programmazione, progettazione, realizzazione ed erogazione degli interventi del sistema locale dei servizi sociali a rete;

- la L. R. 12/2005 e s.m.i. “Norme per la valorizzazione delle organizzazioni di volontariato” che, sottolineando l’apporto del volontariato nel quadro sociale e sanitario, promuove un atteggiamento di disponibilità e flessibilità tra il volontariato, sempre più volto a cogliere la complessa e ricca trama della solidarietà contemporanea e le istituzioni per un rapporto che, accanto alla collaborazione operativa su ragioni di “servizio”, crea spazi di stimolo reciproco, al fine di incentivare uno sforzo di adeguamento dell’azione pubblica e di quella volontaria ai bisogni e all’attesa della gente;
- l'articolo 9 del Regolamento (UE) 2016/679 in materia di protezione dei dati personali, che in tema di trattamento di categorie particolari di dati personali sancisce:
 - al paragrafo 1. il divieto di “trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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”;
 - al paragrafo 2., lett. g) che il suddetto divieto non opera se “il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
- l'articolo 2-*sexies*, comma 2, lett. s) del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018 che tra i trattamenti necessari per motivi di interesse pubblico rilevanza annovera le “attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci”;
- l'art. 6 del Regolamento UE 2016/679 in materia di protezione dei dati personali:
 - lettera E - Liceità del trattamento - “il trattamento è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento”;
 - lettera D - il trattamento è necessario per la salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica;
- la Scheda n. 6 dell'Allegato B del Regolamento N. 1/2014 “per il trattamento dei dati sensibili e giudiziari di competenza della giunta della Regione Emilia Romagna, delle aziende sanitarie, degli enti e delle agenzie regionali e degli enti vigilati dalla Regione”, (dichiarato tuttora applicabile dall'Autorità Garante per la protezione dei dati personali con comunicazione alla Conferenza delle regioni e delle province autonome del 27.11.2018, nonostante l'intervenuto mutamento normativo e “*nelle more dei pur opportuni aggiornamenti*”), la quale Scheda consente la trasmissione di “dati sanitari delle persone interessate dagli interventi di protezione civile, per poter predisporre tali interventi nell’ambito dei Piani di emergenza”;
- il D. Lgs. 1/2018 “Codice della protezione Civile”, il cui articolo 18, comma 1 recita “La pianificazione di protezione civile ai diversi livelli territoriali è l’attività di prevenzione non strutturale, basata sulle attività di previsione e, in particolare, di identificazione degli scenari di cui all’articolo 2, comma 2, finalizzata:
 - a) alla definizione delle strategie operative e del modello di intervento contenente l’organizzazione delle strutture per lo svolgimento, in forma coordinata, delle attività di protezione civile e della risposta operativa per la gestione degli eventi calamitosi previsti o in atto, garantendo l’effettività delle funzioni da svolgere con particolare riguardo alle persone in condizioni di fragilità sociale e con disabilità, in relazione agli ambiti ottimali di cui all’articolo 11, comma 3, definiti su base provinciale e comunale, quest’ultimo anche in forma aggregata;

PREMESSO CHE

- la sopra richiamata L. 241/1990 disciplina all'articolo 15 gli accordi tra pubbliche amministrazioni;
- l'articolo 50, comma 2, primo periodo del D. Lgs. 82/2005 "Codice dell'Amministrazione Digitale" prevede che "Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive";

PREMESSO ALTRESÌ CHE

- l'Unione ha avviato nell'anno 2015 un progetto per la gestione dei soggetti che versino in condizioni di fragilità e/o di non autosufficienza (in seguito anche indicati come pazienti "fragili") che prevede lo sviluppo di uno strumento informatico avente la finalità di individuare in tempo reale la residenza di tali soggetti al fine di consentirne il soccorso in tempo rapidi;
- lo strumento informatico succitato necessita di un insieme di dati e di informazioni che una volta elaborati possa rappresentare in maniera visuale ed efficace le informazioni;
- è necessario disporre di dati e di informazioni in possesso della AUSL in modo da ottenere un risultato dell'elaborazione di livello qualitativamente elevato;

LE PARTI CONCORDANO E STIPULANO QUANTO SEGUE:

Articolo 1

Oggetto e finalità della Convenzione

Al fine di realizzare una efficace gestione dei soggetti "fragili" per le attività di pianificazione e per la gestione delle emergenze di protezione civile, le Parti definiscono le modalità di accessibilità ai dati personali di tali soggetti, necessari per le finalità istituzionali dell'Unione compresi i Comuni ad essa aderenti (Campogalliano, Carpi, Novi di Modena, Soliera). La finalità della presente Convenzione è pertanto quella di normare le modalità relative alla corretta gestione dei dati in possesso della AUSL di Modena relativi alle persone fisiche che rientrino nella definizione di "soggetti fragili" verso il Soggetto Fruitore.

Articolo 2

Modalità di trasmissione dei dati

Le Parti concordano che i dati oggetto della presente Convenzione, indicati nell'*Allegato A* parte integrante della stessa, saranno trasmessi secondo le seguenti modalità condivise:

- accesso diretto con credenziali personali;
- trasmissione in formato nativamente digitale ed "aperto", ovvero sia i dati saranno contenuti in file in formato non proprietario, ad es. CSV;
- l'accesso ai dati avverrà tramite canale Secure File Transfer Protocol (SFTP) secondo le indicazioni e le configurazioni informatiche che le Parti divideranno.

Il tracciato dei dati e le eventuali successive modifiche verranno concordate dalle Parti.

Articolo 3

Proprietà dei dati - Responsabili della Convenzione

Il Soggetto Erogatore in quanto Titolare del trattamento provvede a consentire l'accesso ai dati secondo le modalità indicate al precedente Articolo 2.

Con la acquisizione dei dati secondo le modalità indicate al precedente Articolo 2 da parte del Soggetto Fruitore, la titolarità dei trattamenti effettuati su tali dati è individuata nella persona del Presidente dell'Unione (Soggetto Fruitore), con le conseguenti responsabilità derivanti dal trattamento di tali dati, ivi compreso il profilo della sicurezza.

Per il Soggetto Fruitore, il Responsabile della Convenzione è individuato nel Dirigente pro-tempore della Protezione Civile dell'Unione delle Terre d'Argine;

Per il Soggetto Erogatore, il Responsabile della Convenzione è individuato nel Dirigente pro-tempore dell'Area della Integrazione Socio Sanitaria del Distretto di Carpi.

Articolo 4

Figure di riferimento per l'attuazione della Convenzione

Ai fini della corretta applicazione di quanto previsto nella presente Convenzione, ciascuna delle Parti nomina un proprio Referente tecnico responsabile, in particolare, dell'attivazione, della gestione operativa, nonché della corretta applicazione delle regole di sicurezza tecnico-organizzative previste nella Convenzione.

I Responsabili della Convenzione per le Parti sono altresì individuati quali Supervisor preposti al monitoraggio e al controllo dell'utilizzo dei dati da parte degli utenti incaricati. Rientra nei compiti dei Supervisor comunicare eventuali abusi, anomalie e/o utilizzi non conformi alle finalità della Convenzione.

I nominativi ed i recapiti delle figure dei Referenti tecnici per l'attuazione della Convenzione verranno successivamente e reciprocamente comunicati dalle Parti.

Articolo 5

Integrazioni e modifiche

Le Parti, al fine di garantire la continuità agli impegni reciprocamente assunti nell'ambito del presente atto convenzionale, concordano sulla possibilità di dover intervenire sulla struttura della Convenzione, ivi compresi gli allegati, a seguito di nuove disposizioni di legge ovvero di ulteriori necessità operative, purché supportate da adeguata base normativa, nonché per recepire indicazioni dell'Autorità Garante per la protezione dei dati personali e/o per evoluzioni tecnico/informatiche.

Le stesse Parti concordano che eventuali modifiche alla Convenzione che attengano alla struttura della stessa in esito a quanto indicato nel periodo precedente ed all'introduzione di ulteriori impegni nelle modalità di erogazione e fruizione dei dati, saranno concordate tra le Parti per il tramite dei Responsabili della Convenzione.

Articolo 6

Misure di sicurezza e responsabilità

Le Parti si impegnano a rispettare i limiti e le condizioni di trasmissione/accesso ai dati al fine di assicurare la protezione dei dati personali e/o di natura particolare, ai sensi della normativa vigente.

Le Parti, laddove si renda necessario interrompere il flusso dei dati per esigenze organizzative e di sicurezza e/o per adeguamento a modifiche legislative, concorderanno tempestivamente, per il tramite dei Responsabili della Convenzione, modalità alternative di trasmissione dei dati stessi.

Il Soggetto Erogatore rende disponibili i dati, anche personali e/o di natura particolare, come risultano al momento della trasmissione/accesso e non assume responsabilità per la mancanza di

aggiornamenti che non dipenda dallo stesso, per variazioni che possano successivamente intervenire e per danni diretti e/o indiretti, nonché per eventuali interruzioni della trasmissione dei dati non preventivamente pianificabili.

Le Parti annualmente verificano il mantenimento dei presupposti e dei requisiti per la trasmissione/accesso ai dati oggetto della presente Convenzione.

Articolo 7

Trattamento dei dati

Le Parti si vincolano, per quanto di rispettiva competenza, alla scrupolosa osservanza delle disposizioni contenute nel Regolamento Europeo (UE) 679/2016 sulla protezione dei dati personali, nonché nel D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018, in particolare per quanto concerne la sicurezza dei dati, gli adempimenti e la responsabilità nei confronti degli interessati, dei terzi e dell'Autorità Garante per la protezione dei dati personali.

Le parti assicurano che i dati personali oggetto della presente Convenzione, compresi quelli di natura particolare, saranno trattati per le sole finalità previste dalle leggi citate nelle premesse e limitatamente ai trattamenti connessi agli scopi di cui alla presente Convenzione per le attività di protezione civile e di pianificazione finalizzate alla tutela e alla salvaguardia dell'incolumità pubblica.

Ciascuna Parte assicura che i dati oggetto della presente Convenzione non saranno divulgati, comunicati, ceduti a terzi, né in alcun modo riprodotti al di fuori dei casi previsti dalla legge, scongiurando, altresì, il rischio di duplicazione della base dati.

Le Parti garantiscono, inoltre, che l'accesso ai dati sarà consentito esclusivamente ai soggetti che verranno appositamente autorizzati al trattamento e abilitati ad accedere ai dati mediante apposite credenziali, impartendo loro per iscritto precise e dettagliate istruzioni, richiamando la loro attenzione sulle responsabilità connesse all'uso illegittimo dei dati. Ogni accesso è registrato.

Il soggetto Fruitore si obbliga inoltre a fornire ogni necessaria collaborazione nei casi di verifiche da parte del Soggetto Erogatore, previo preavviso tra le rispettive funzioni organizzative preposte alla sicurezza.

Articolo 8

Durata della Convenzione

La presente Convenzione ha durata dalla data di sottoscrizione e fino al 31 dicembre 2020 compreso.

Le Parti potranno in ogni momento modificare e/o riformulare o anche recedere dalla presente Convenzione qualora dovessero intervenire mutamenti delle esigenze di trasmissione/accesso ai dati e/o in caso di modifiche di disciplina (giuridica e/o amministrativa) di uno o più trattamenti oggetto della stessa.

Il recesso deve essere comunicato con documento firmato digitalmente e inviato per mezzo di Posta Elettronica Certificata (PEC) all'altra Parte.

Articolo 9

Oneri economici

Per l'esecuzione della presente Convenzione non sono previsti oneri economici a carico delle Parti.

Articolo 10

Allegati alla Convenzione

Forma parte integrante della presente Convenzione:

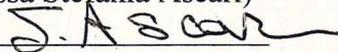
- Allegato A) Dati sottoposti a trattamento.
- Allegato B) DPIA (Data Protection Impact Assessment) progetto Fragili.

Articolo 11

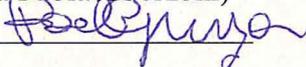
Rinvio

Per tutto quanto ivi non riportato si rinvia alla normativa vigente in materia.

La Direttrice del Distretto
(D.ssa Stefania Ascari)



Il Presidente prot-tempore dell'UTD
(D.ssa Paola Guerzoni)



Allegato A

Progetto *Fragili*

Dati sottoposti a trattamento

Nome documento	<i>Dati sottoposti a trattamento.pdf (Allegato A alla Convenzione)</i>
Versione documento	<i>1.0</i>
Data rilascio documento	<i>26/4/2019</i>
Autore del documento	<i>Sistema Informativo Associato S.I.A. – Unione delle Terre d'Argine</i>

Sommario

1. Introduzione	3
2. Dati oggetto del trattamento.....	3
3. Trasmissione dei dati	4

1. Introduzione

Il presente documento definisce i dati che saranno sottoposti al trattamento nel contesto della Convenzione tra l'AUSL di Modena e l'Unione delle Terre d'Argine per la gestione dei dati personali dei soggetti residenti nel territorio dell'Unione delle Terre d'Argine che versino in condizioni di fragilità e/o di non autosufficienza.

2. Dati oggetto del trattamento

Con la sottoscrizione della Convenzione, l'AUSL di Modena si impegna a trasmettere all'Unione delle Terre d'Argine i seguenti dati, che saranno sottoposti al trattamento da parte dell'Unione delle Terre d'Argine per le finalità connesse al Progetto Fragili di cui alla Convenzione, di seguito riportati:

Nome campo	Descrizione
CodFisc	Codice Fiscale assistito
Nome	Nome assistito
Cognome	Cognome assistito
Sesso	M/F
Data_nascita	gg/mm/aaaa
Comune_nascita	
Indirizzo	
Piano	Indicazione del piano
Ascensore	si/no
Condizionatore	si/no
MMG	Cognome e nome del Medico di Medicina Generale
Rete	
Telefono	Numero di rete fissa
Cellulare	Numero di rete mobile
Riferimento1	
Riferimento2	
Convivente	Eventuale convivente (es. coniuge, figlio, cognata, badante, etc)
Disturbo_cognitivo	[assente/lieve/moderato/grave]
Mobilità	[nessuna/parziale/con assistenza]
Dispositivi	Eventuale presenza di dispositivi di supporto all'assistito

3. Trasmissione dei dati

La trasmissione dei dati di cui al precedente paragrafo avverrà a cura dell'AUSL secondo le specifiche di seguito indicate:

- Cadenza di trasmissione dati: almeno mensile;
- Numero file trasmessi mensilmente: unico per tutto il territorio dell'Unione delle Terre d'Argine;
- Formato dati trasmessi: digitale, estensione file CSV;
- Modalità di trasmissione dati: mediante SFTP oppure Accesso diretto HTTPS.

--- FINE DOCUMENTO ---

UNIONE DELLE TERRE D'ARGINE

Corso Alberto Pio, 91
41012 Carpi (MO)
Tel: +39 059 649 111 - Fax: +39 059 649 774
P.IVA 03069890360



DATA PRIVACY IMPACT ASSESSMENT

Scopo di questo documento di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato da UNIONE DELLE TERRE D'ARGINE per una valutazione dell'impatto sui trattamenti.

Elenco per trattamento

I rischi associati ai trattamenti sono la somma pesate dei rischi logici ed organizzativi sui dati e dei rischi presenti sugli archivi utilizzati per il trattamento.

● FRAGILI - PROGETTO GESTIONE SOGGETTI IN CONDIZIONE DI FRAGILITA' E/O DI NON AUTOSUFFICIENZA

FRAGILI - PROGETTO GESTIONE SOGGETTI IN CONDIZIONE **Fattore di rischio residuo dopo valutazione di impatto** **2/10** (Basso)
DI FRAGILITA' E/O DI NON AUTOSUFFICIENZA

Livello di copertura:	<ul style="list-style-type: none">• Fattore di rischio iniziale: 10/10• Fattore di rischio residuo: 2/10• Copertura misure attuate: 78%• Copertura misure dopo valutazione di impatto: 80%
Dati Comuni trattati :	<ul style="list-style-type: none">• codice fiscale ed altri numeri di identificazione personale;• nominativo, indirizzo o altri elementi di identificazione personale;• dati relativi alla famiglia e a situazioni personali;• lavoro;• abitudini di vita o di consumo;• Dati relativi al medico di medicina generale.
Dati Particolari trattati:	<ul style="list-style-type: none">• stato di salute.
Unità di archiviazione utilizzate per il trattamento	<ul style="list-style-type: none">• ARCHIVIO CARTACEO SERVIZI SOCIALI SOLIERA (sede: Comune di Soliera - sede servizi sociali).• fragili (sede: Sede distaccata di Via III Febbraio, 2).• POLIZIA MUNICIPALE - DIREZIONE (sede: Sede distaccata di Via III Febbraio, 2).• POLIZIA MUNICIPALE - PROTEZIONE CIVILE (sede: Sede distaccata di Via III Febbraio, 2).

Interessati al trattamento, finalità e base giuridica

- ▶ **interessati al progetto fragili**
 - attuazione degli strumenti e delle strategie di rete per l'individuazione e l'attivazione dei interventi di sostegno ai soggetti "Fragili" e della crescita del Welfare di comunità [interesse pubblico].
 - gestione del monitoraggio delle persone fragili necessario per gli interventi di welfare comunitario - "Protezione Fragili" [interesse pubblico].
 - individuazione dei soggetti "Fragili" sconosciuti ai servizi con intercettazione dei bisogni al fine di agire in modo proattivo e preventivo [interesse pubblico].
 - monitoraggio dei bisogni e rafforzamento delle capacità di supportare i "fragili nelle emergenze" [interesse pubblico].

Rischio di Integrità dei dati

▶ Trattamento dei dati secondo modalità differenti da quelle dichiarate	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
▶ Eliminazione o perdita dei dati al di fuori dell'ambito definito	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
▶ Mancata disponibilità dei dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
▶ Modifica errata o mancato aggiornamento dei dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Rischio di Riservatezza dei dati

▶ Comunicazione dei dati al di fuori dell'ambito definito	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
▶ Diffusione dei dati al di fuori dell'ambito definito	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
▶ Trattamento dei dati al di fuori dell'ambito degli addetti autorizzati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Accadimenti possibili sugli archivi

Allagamento	Rischio Residuo Livello di Copertura	BASSO NESSUNO
Crollo Struttura	Rischio Residuo Livello di Copertura	BASSO NESSUNO
Fenomeni climatici (Uragani, Nevicate, Fulmini)	Rischio Residuo Livello di Copertura	MOLTO BASSO NESSUNO

Incendio	Rischio Residuo Livello di Copertura	MOLTO BASSO MEDIO
Accesso non autorizzato ai dati cartacei	Rischio Residuo Livello di Copertura	MOLTO BASSO MEDIO
Rottura aria condizionata o distribuzione acqua	Rischio Residuo Livello di Copertura	MOLTO BASSO ALTO
Introduzione di persone non autorizzate al di fuori dell'orario di lavoro	Rischio Residuo Livello di Copertura	MOLTO BASSO MEDIO
Eccesso di traffico sulle linee di TLC	Rischio Residuo Livello di Copertura	MOLTO BASSO ALTO
Divulgazione Intenzionale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO ALTO
Errori di trasmissione (incluso il misrouting)	Rischio Residuo Livello di Copertura	MOLTO BASSO MEDIO
Furto di Identità degli Addetti	Rischio Residuo Livello di Copertura	MOLTO BASSO ALTO
Danni alle linee di TLC	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Presenza di Virus	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Perdita di energia, sbalzi di tensione.	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Saturazione dei sistemi IT	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errori di manutenzione hardware e software	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Divulgazione accidentale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Indisponibilità erogazione energia elettrica	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Furti di Dati perpetrati da personale Interno	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Accesso a Sistemi contenenti informazione da parte di addetti non autorizzati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Mancato recupero di informazioni da media (principalmente memorie di massa) di backup up.	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Furto di apparati o sistemi	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errore di salvataggio sui supporti di Back-up	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Scrittura Dati errati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione o Modifica volontaria dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione di strumentazione da parte di persone malevole	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Errori non volontari durante modifica o cancellazione di Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Furti di Dati perpetrati dall'esterno	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Distruzione o Modifica accidentale dei Dati	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Accesso non autorizzato o Furto di dati personali	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Fault o malfunzionamento della strumentazione IT	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Malfunzionamenti software	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO
Importazione o esportazione illegale di Dati e Informazioni	Rischio Residuo Livello di Copertura	MOLTO BASSO MOLTO ALTO

Misure Adottate

Misure Fisiche

- ▶ Chiusura a chiave
- ▶ Installazione Allarme
- ▶ Dotazione serrature ufficio.
- ▶ Estintori
- ▶ Sistemi di Accesso Controllato
- ▶ Gruppo Elettrogeno
- ▶ Linea Dati Ridondante
- ▶ Installazione di un Firewall.
 - Firewall software.
 - Firewall hardware.
- ▶ Contratto di Manutenzione Hardware.
- ▶ Analisi Impegno Linea.
- ▶ Sistema di condizionamento
- ▶ Installazione Impianto Antiincendio

- ▶ Accesso Controllato al locale.
- ▶ Gruppo di continuità
- ▶ Monitoraggio Accessi.
- ▶ Copie di Back-up.
 - Back-Up eseguito in Automatico.
 - Back-Up Incrementale.
 - Back-Up giornaliero.
 - Utilizzo 4 Supporti Differenti.
 - Back-Up su Sistemi SAN
- ▶ Credenziali di autenticazione, assegnate individualmente ad ogni addetto.
 - Autenticazione mediante user-id e password.
 - Parola chiave di almeno 8 caratteri.
 - Disattivazione delle vecchie credenziali.
 - Disposizioni scritte per la disponibilità dei dati.
- ▶ Sistema Operativo.
 - Linux Server
- ▶ Aggiornamento Software.
- ▶ Cifratura dei dati trasmessi.
 - Cifratura con protocollo SSL.
- ▶ Installazione Software testato e certificato.
- ▶ Sospensione manuale delle sessioni di Lavoro.
- ▶ FIREWALL PERIMETRALE
- ▶ BACKUP COMPLESSO
- ▶ sistema RAID.
- ▶ Sistema di Mirroring.
- ▶ Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
- ▶ Verifica ed eventuale nomina degli amministratori di sistema se presenti
- ▶ Profili di autorizzazione di ambito diverso per diversi incaricati.
 - E' utilizzato un sistema di autorizzazione.
 - I profili di autorizzazione vengono specificati prima di ogni trattamento.
 - Verifica periodica del profilo di autorizzazione.

Misure Logiche e Organizzative

- ▶ Individuazione estremi identificativi delle persone fisiche preposte quali amministratori di sistema dell'azienda di outsourcing esterna.
- ▶ Verifica annuale operato Amministratori di Sistema
- ▶ Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile
- ▶ Redazione documento Privacy by Design e By Default
- ▶ Nomina del DPO
- ▶ Procedure Gestione Data Breach
- ▶ Implementazione Procedura di Nomina a Responsabile del trattamento
- ▶ Implementazione procedura di verifica per i Responsabile del trattamento
- ▶ Distruzione dei supporti removibili.
- ▶ Descrizione scritta degli interventi effettuati da terzi.
- ▶ Redazione di un piano di formazione per gli addetti
- ▶ Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.
- ▶ Consegna istruzioni dettagliate agli addetti.
 - Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali.
 - Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento.
 - Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari.
 - Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei.
- ▶ Procedure per ripristino dei dati.

Ultima modifica 10/04/2019

DPIA

Cod.Doc. 10799.56.0.1441033

Misure Previste per il Piano di Compliance

Misure Fisiche

- ▶ Spostamento del sistema in server farm ubicata a Ravenna e disaster Recovery a Parma entro fine 2019