

Procedura Operativa Standard

Data Privacy negli studi clinici

Procedura N.: GEN06

Versione N.: 1

| | Nome | Ruolo | Data | Firma |
|--------------|--------------|------------------------------------------------------|------|-------|
| Autore | R. Porcino | Referente Privacy | | |
| Rivisto da | M. Fumarola | Coordinatore Clinical Operations FROM – E.T.S. | | |
| Rivisto da | G. Latteri | Quality Assurance Manager FROM – E.T.S. | | |
| Approvato da | E. Sfreddo | Direttore Operativo FROM – E.T.S. | | |
| Approvato da | A. Gavazzi | Direttore Medico Unità Fase I FROM – E.T.S. | | |
| Approvato da | A. Bombassei | Presidente FROM | | |

INDICE

| | |
|---------------------------------------------------------------------------|----|
| 1. ABBREVIAZIONI | 3 |
| 2. SCOPO | 3 |
| 3. AMBITO DI APPLICAZIONE | 3 |
| 4. RESPONSABILITA' | 3 |
| 5. PROCEDURE | 5 |
| 5.1 Studio clinico con Promotore FROM – E.T.S. | 5 |
| 5.2 Studio clinico supportato da FROM – E.T.S. per conto di terzi | 6 |
| 5.3 Conservazione dei dati e sicurezza | 6 |
| 5.4 Diritti dei soggetti..... | 6 |
| 5.5 Informativa privacy e consenso al trattamento dei dati | 7 |
| 5.6 Visite on site | 7 |
| 5.7 Ricezione accidentale di dati personali..... | 8 |
| 5.8 Violazione dei dati personali (Data Breach)..... | 8 |
| 5.9 Gestione del Data Breach | 8 |
| 1.1.1. Studio clinico con Promotore FROM – E.T.S. | 8 |
| 1.1.2. Studio clinico supportato da FROM - E.T.S. per conto di terzi..... | 9 |
| 6. BIBLIOGRAFIA | 10 |
| 7. ALLEGATI | 10 |
| 8. CRONOLOGIA VERSIONI..... | 10 |

1. ABBREViaZIONI

| | |
|----------------|-----------------------------------------------------------------------------|
| CCO: | Coordinatore <i>Clinical Operations</i> |
| CRA: | <i>Clinical Research Associate</i> |
| DO: | <i>Direttore Operativo</i> |
| DM: | <i>Data Manager</i> |
| DPO: | <i>Data Protection Officer</i> |
| FROM – E.T.S.: | FROM-Fondazione per la Ricerca Ospedale di Bergamo – Ente del Terzo Settore |
| GCP: | <i>Good Clinical Practice</i> |
| GDPR: | <i>General Data Protection Regulation</i> |
| ICH: | <i>International Council of Harmonization</i> |
| ISF: | <i>Investigator's Site File</i> |
| PM: | <i>Project Manager</i> |
| POS: | <i>Procedura Operativa Standard</i> |
| TMF: | <i>Trial Master File</i> |
| UE: | Unione Europea |

2. SCOPO

Le *Good Clinical Practice* (ICH-GCP) stabiliscono che “la confidenzialità dei dati che potrebbero permettere l'identificazione dei soggetti deve essere protetta, rispettando la privacy e la confidenzialità in accordo alla normativa applicabile” (§ 2.11).

Il Regolamento Europeo 2016/679 (GDPR) regola il processamento dei dati personali in UE.

Il Decreto Legislativo n. 196/2003 è stato modificato dal Decreto Legislativo n. 101/2018 per allinearli con il GDPR.

Il Garante per la protezione dei dati personali è l'autorità responsabile della supervisione dell'applicazione del GDPR.

La presente procedura, descrive come FROM – E.T.S. raccoglie, utilizza e divulga le informazioni, quali sono i diritti dei soggetti e come questi possono accedere ai dati, in conformità ai requisiti della normativa applicabile.

Questa Procedura Operativa Standard (POS) è conforme all'articolo 29 del GDPR.

3. AMBITO DI APPLICAZIONE

Questa procedura si applica esclusivamente agli studi clinici di cui FROM – E.T.S. è Promotore e agli studi supportati da FROM – E.T.S. per conto di terzi, compresi gli studi di Fase I.

4. RESPONSABILITA'

Nell'ambito di applicazione definito al punto 3 si individuano le seguenti responsabilità.

Il *Data Protection Officer* (DPO) è responsabile di:

- Informare e fornire consulenza a FROM – E.T.S. circa la conformità dei presidi di *governance* e delle modalità di trattamento dei dati alla normativa applicabile in materia di *data protection*;
- Coordinare le comunicazioni tra il personale FROM - E.T.S. e il Garante della Privacy;
- Coordinare e revisionare il *Data Protection Impact Assessment (DPIA)* per gli studi promossi da FROM;
- Definire le linee guida di riferimento per la stesura e revisionare i *Data Processing Agreement (DPA)*;
- Prestare assistenza e consulenza in ordine alle attività relative alla notifica di violazione di dati personali (*Data Breach*);
- Agire da punto di contatto interno per la valutazione delle richieste di accesso ai dati da parte dei soggetti interessati.

Il *Direttore Operativo (DO)* è responsabile di:

- Nominare il DPO, esercitando l'apposita delega del Consiglio di Amministrazione;
- Assicurare che i contatti del DPO siano disponibili al Garante della Privacy, al personale FROM - E.T.S. e al pubblico;
- Assicurare che le prescrizioni del DPO siano attuate in FROM - E.T.S.;
- Presidiare l'aggiornamento del modello di *governance* della normativa *privacy* adottato da FROM – E.T.S. e il corretto funzionamento;
- Agire da punto di contatto tra DPO e Consiglio di Amministrazione.

Il *Referente Privacy (RP)* è responsabile di:

- Aggiornare il DO, il Coordinatore Clinical Operations (CCO) e il Direttore Medico FASE I (per studi FASE I) sulle prescrizioni del DPO e la loro attuazione.
- Inviare al DPO i protocolli degli studi per la definizione delle informative privacy (per studi promossi da FROM).
- Avviare la gestione del Data Breach
- Coadiuvare il DO, in caso di *Data Breach* ed in caso di esercizio dei diritti degli interessati, nella gestione della problematica e nelle comunicazioni al DPO e ai soggetti interessati.

Il *Project Manager (PM)/Data Manager (DM)* dello studio clinico è responsabile di:

- Seguire il processo di protezione dei dati e le procedure, collaborando con l'RP riguardo i potenziali *Data Breach*;
- Collaborare con l'RP nel caso in cui un soggetto eserciti i suoi diritti in accordo al Capitolo III del GDPR;

Il *System Administrator* è qualsiasi persona coinvolta nella gestione dei sistemi di informazione, che è rilevante in termini dei rischi relativi alla protezione dei dati, come gli amministratori di server, gli amministratori di database, gli amministratori di network e apparecchiature di sicurezza e gli amministratori di software complessi. I *System Administrator* che gestiscono l'architettura e l'infrastruttura informatica sono responsabili di assicurare la protezione di questi sistemi per prevenire accessi non autorizzati.

Il personale FROM - E.T.S. è responsabile di:

- Seguire la presente procedura;
- Notificare eventuali *Data Breach* di cui si viene a conoscenza.

Il *Clinical Monitor* è responsabile di:

- Accertare che le versioni aggiornate e approvate dal DPO delle Informative al trattamento dei dati personali e dei relativi moduli di rilascio del Consenso, siano disponibili presso i Centri sperimentali;
- Verificare, durante le visite di monitoraggio, che i soggetti partecipanti abbiano firmato i moduli di Consenso Informato al Trattamento Dati Personali e ricevuto/compreso la relativa Informativa e che i documenti siano disponibili presso gli *Investigator's Site File* (ISF).

Lo *Sperimentatore Principale* è responsabile di raccogliere i moduli Consenso Informato al Trattamento Dati Personali e il consenso alla partecipazione allo studio secondo le regole definite dalla normativa vigente.

5. PROCEDURE

5.1 Studio clinico con Promotore FROM – E.T.S.

Il Promotore, prima dell'avvio della sperimentazione, identifica i possibili Centri partecipanti verificandone l'idoneità e il relativo interesse; predispone il protocollo dello Studio e impartisce ai Centri le necessarie direttive sul trattamento dei dati. Condivide con il personale del Centro partecipante le istruzioni relative alle modalità di utilizzo dei sistemi informativi previsti per la raccolta, la custodia e la sicurezza dei dati raccolti.

FROM - E.T.S. e il Centro partecipante allo studio si qualificano come titolari autonomi al trattamento dei dati.

I titolari autonomi provvederanno, ciascuno nell'ambito del proprio assetto organizzativo, alle eventuali nomine di Responsabili del trattamento, ai sensi dell'art.28 del GDPR e attribuzione di funzioni e compiti a soggetti designati ai sensi del GDPR e della normativa vigente.

I rapporti tra FROM - E.T.S. e soggetti terzi coinvolti nella sperimentazione (a titolo esemplificativo *Clinical Research Organization, Monitor, Data Manager*, ecc.) relativi al trattamento dei dati personali sono disciplinati dalle clausole contrattuali che specificano i ruoli rivestiti da ciascuna delle parti coinvolte in una sperimentazione clinica.

Tutti i dati di persone fisiche (esclusi quelli dei pazienti sottoposti alla sperimentazione per i quali si applicano le prescrizioni sotto predisposte) afferenti a FROM - E.T.S. e/o ai Centri partecipanti allo studio verranno reciprocamente trattati dai due titolari del trattamento in conformità al Regolamento 679/2016/UE, al D.Lgs. 196/2003 come novellato dal D.Lgs. 101/2018 e s.m.i. ed ai provvedimenti dell'Autorità Garante.

In merito, specifica clausola contrattuale è prevista nei contratti tra FROM – E.T.S. e il Centro Partecipante.

Per i pazienti partecipanti allo studio FROM – E.T.S. predispone:

- Informativa e consenso al trattamento dei dati,
- Consenso Informato alla sperimentazione clinica.

Per la predisposizione dell'informativa e consenso al trattamento dei dati il Referente Privacy invia per mail al DPO la documentazione predisposta ad hoc per lo studio.

FROM - E.T.S. affida al Centro di sperimentazione il compito di informare in modo chiaro e completo, prima che abbia inizio lo studio, ogni paziente, o un suo rappresentante legalmente riconosciuto, circa natura, finalità, risultati, conseguenze, rischi e modalità del trattamento dei dati personali e di acquisire i necessari consensi dei pazienti partecipanti allo studio prima dell'arruolamento.

Il Promotore non effettua alcuna attività di raccolta diretta dei dati, né può interloquire con gli individui inclusi nella Sperimentazione, compiti questi, spettanti agli Sperimentatori. FROM - E.T.S. acquisisce i dati dei pazienti previamente pseudonimizzati da ciascun Centro partecipanti e sugli stessi effettua le operazioni autorizzate di trattamento previste dal Protocollo di studio tramite proprio personale incaricato.

In ogni caso, FROM – E.T.S., nella sua qualità di Promotore, mantiene le proprie prerogative di monitoraggio e auditing nei confronti della documentazione sanitaria e dei dati clinici afferenti allo studio, nonché rispetto ad ogni altra informazione che possa essere rilevante per lo studio, nel rispetto delle misure di sicurezza e della confidenzialità dei dati. Dette attività potranno altresì essere effettuate per mezzo di Monitor e Auditor a ciò espressamente incaricati dal Promotore.

Il Centro di sperimentazione è responsabile della corretta archiviazione dei moduli cartacei sottoscritti dai pazienti. I moduli dovranno essere custoditi in apposite armadiature dotate di serratura accessibile dal solo personale autorizzato.

5.2 Studio clinico supportato da FROM – E.T.S. per conto di terzi

FROM - E.T.S. riceve dal Titolare al trattamento dei dati dello studio specifica lettera di nomina che rappresenta l'atto giuridico di formalizzazione delle responsabilità come previsto dal paragrafo 3 dell'articolo 28 del Regolamento 679/2016/UE. FROM E.T.S. garantisce l'attuazione di misure tecniche organizzative tali da soddisfare i requisiti del Regolamento 679/2016/UE.

FROM E.T.S. provvederà a nominare in forma scritta i propri sub-responsabili.

Le lettere di nomina devono essere sottoscritte dal DO e archiviate dall'RP nella documentazione contrattuale dello studio oggetto della nomina.

5.3 Conservazione dei dati e sicurezza

Tutti i dati personali raccolti da FROM - E.T.S. sono conservati per il tempo strettamente necessario al raggiungimento delle finalità per cui i dati sono stati raccolti.

Quando lo scopo originario si è esaurito, il personale di FROM – E.T.S. dà indicazioni per rimuovere i dati personali dai sistemi elettronici a meno che non possa fornire un chiaro requisito legale per conservarli ancora. Questi requisiti non devono essere in conflitto con quanto indicato nella relativa informativa al trattamento dei dati personali e con il consenso espresso dal soggetto.

FROM - E.T.S. conserva i dati in un luogo controllato e sicuro e ad accesso controllato. Il tempo di conservazione dei dati è determinato per ciascun trattamento.

L'accesso ai dati personali su modulo cartaceo è protetto in apposite armadiature dotate di serrature e accessibili al solo personale autorizzato.

L'accesso ai dati personali è ristretto solo al personale dipendente o ai collaboratori, e i dati in formato digitale sono protetti da password. FROM - E.T.S. utilizza un software per la creazione delle eCRF elettroniche per l'acquisizione e gestione di dati clinici conforme al GDPR e alla normativa locale applicabile. FROM - E.T.S. effettua audit periodici sul fornitore del sistema.

Il DPO coordina la revisione periodica dei dati personali conservati da FROM - E.T.S. (almeno ogni 3 anni) per determinare se le informazioni sono ancora necessarie o se possono essere eliminate.

Nelle attività di *auditing* del DPO potranno essere sviluppate verifiche sulla sussistenza delle condizioni di conservazione dei dati acquisiti.

5.4 Diritti dei soggetti

Il GDPR prevede i seguenti diritti per i soggetti:

- Il diritto di essere informato riguardo i dati che FROM - E.T.S. raccoglie e come sono utilizzati ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679;
- Il diritto di revocare il consenso in qualsiasi momento, senza però pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- Il diritto di chiedere di poter accedere ai propri dati personali ed estrarne copia;

- Il diritto di chiedere di poter rettificare i propri dati personali, ove ciò non contrasti con la normativa vigente sulla conservazione dei dati stessi e con la necessità di tutelare in caso di contenzioso giudiziario i professionisti sanitari che li hanno trattati;
- Il diritto di chiedere la cancellazione dei propri dati personali nei limiti previsti dalla normativa, ove ciò non contrasti con la normativa vigente sulla conservazione dei dati stessi e con la necessità di tutelare in caso di contenzioso giudiziario i professionisti sanitari che li hanno trattati;
- Il diritto di chiedere la limitazione del trattamento dei propri dati personali;
- Il diritto di opporsi al trattamento;
- Il diritto di chiedere, solamente nei casi previsti all'art. 20 del Regolamento UE 2016/679, che venga compiuta la trasmissione dei propri dati personali ad altro operatore sanitario in formato leggibile.

Le richieste di accesso ai propri dati personali, di rettifica, aggiornamento, cancellazione, integrazione dei dati, nonché di opposizione al trattamento possono essere presentate a FROM - E.T.S. a mezzo mail all'indirizzo privacy@fondazionefrom.it¹. I dati di contatto sono disponibili nella sezione Privacy del sito fondazionefrom.it.

È importante che qualsiasi richiesta di esercitare i suddetti diritti sia prontamente comunicata internamente. Tutte le istanze provenienti dagli interessati devono essere inoltrate all'indirizzo privacy@fondazionefrom.it¹ di FROM – E.T.S., il cui team (DO, CCO, Direttore Medico Fase I, Referente Privacy) provvederà ad una valutazione preliminare ed alla trasmissione al DPO per le valutazioni di sua competenza.

5.5 Informativa privacy e consenso al trattamento dei dati

L'informativa al trattamento dei dati personali deve essere predisposta in accordo alle prescrizioni del DPO. Il Referente Privacy riceve dal Coordinatore delle Clinical Operations la documentazione predisposta ad hoc per lo studio necessaria all'invio della richiesta al DPO.

Il Referente Privacy invierà al DPO la documentazione predisposta per approvazione.

I monitor, durante le visite di monitoraggio, verificano che i partecipanti agli studi clinici abbiano espresso il consenso alla raccolta e processamento dei propri dati da parte di FROM - E.T.S utilizzando la modulistica dedicata e condivisa con il DPO.

5.6 Visite on site

In occasione di una visita di monitoraggio o di un audit per gli studi, al personale FROM - E.T.S. (rispettivamente *Clinical Monitor* e *Auditor*) appositamente incaricato è richiesto di monitorare l'attività dello studio.

FROM E.T.S., nel caso in cui sia necessario individuare personale esterno per lo svolgimento delle visite on site procederà con la nomina a Responsabile del trattamento se è il Titolare al trattamento ovvero con la nomina a Sub-responsabile se è Responsabile al trattamento (ai sensi dell'art.28 del GDPR).

FROM - E.T.S nell'individuare i *Clinical Monitor* e *Auditor* verifica che possiedano i requisiti di esperienza, capacità e affidabilità tali da fornire idonee garanzie del pieno rispetto delle istruzioni da impartire e delle regole di riservatezza e confidenzialità previste dalla disciplina in materia di protezione di dati personali e dalle disposizioni di settore.

Gli addetti al monitoraggio e all'audit devono essere sottoposti a regole di condotta analoghe al segreto professionale. Il loro processo di designazione deve prevedere la frequenza di una specifica attività formativa concernente l'illustrazione dei rischi e delle responsabilità derivanti dal trattamento di queste informazioni, le istruzioni da rispettare per la loro custodia e sicurezza, nonché le regole di riservatezza e confidenzialità previste dalle disposizioni normative applicabili e le specifiche precauzioni da utilizzare per tutelare l'identità degli interessati.

¹ Le informative redatte prima del 01/04/2023 riportano come indirizzo di contatto segreteria@fondazionefrom.it

5.7 Ricezione accidentale di dati personali

È possibile che durante uno studio, i dati personali in chiaro dei partecipanti siano accidentalmente comunicati a FROM - E.T.S.; in tal caso, dovrà essere attivato il seguente processo:

- Chiunque tra il personale FROM - E.T.S. identifichi l'invio accidentale di dati personali, deve immediatamente comunicare al referente privacy per valutazione dell'accaduto.
- Tutti i file inviati dalla stessa fonte nello stesso momento devono essere rivisti da chi ha rilevato l'accaduto per vedere se contengono altri dati personali non codificati.
- Tali file devono essere eliminati e rimossi anche dal cestino dei computer personali e aziendali del personale.
- Se i file sono inviati tramite email, il segnalante deve verificare tutti i destinatari delle mail contenenti dati non corretti ai sensi della disciplina privacy e coinvolgere direttamente anche questi ultimi nella risoluzione della problematica. Le email devono essere eliminate e rimosse dal cestino nei computer personali e aziendali del personale coinvolto seguendo le indicazioni dell'RP.
- Chi ha inviato il file deve essere informato per iscritto (tramite canali di comunicazione ufficiali) dell'incidente e delle azioni intraprese per risolverlo.
- Se l'invio accidentale è stato effettuato da persona in forza presso FROM E.T.S. la persona deve essere informata e occorre enfatizzare la serietà dell'accaduto. Occorre inoltre richiedere di esaminare il proprio processo per identificare il motivo dell'accaduto e riportarlo internamente.
- L'incidente e tutte le azioni intraprese devono essere documentati appropriatamente e riportate al personale FROM - E.T.S. coinvolto e al DO. Se i dati personali ricevuti sono considerati un *Data Breach*, il DPO deve essere informato ed attivata la procedura di cui al successivo paragrafo 5.9.

5.8 Violazione dei dati personali (Data Breach)

Per violazione dei dati personali (c.d. *Data Breach*) si intende una 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 (art. 4 par. 12 GDPR).

5.9 Gestione del Data Breach

Il verificarsi di una violazione di dati personali può essere rilevato da qualsiasi soggetto interno (es. personale dipendente, liberi professionisti etc.) o da soggetti esterni (es. pazienti partecipanti agli studi, monitor, etc.). Chiunque riceva notizia di una presunta violazione deve segnalare immediatamente quanto rilevato al Referente Privacy in prima istanza telefonicamente e successivamente per e-mail (privacy@fondazionefrom.it).

Ricevuta l'istanza il Referente Privacy si attiverà per la valutazione della presunta violazione seguendo quanto previsto dalla istruzione operativa "Gestione delle violazioni di dati personali (data breach

1.1.1. Studio clinico con Promotore FROM – E.T.S.

Gli artt. 33 e 34 del Regolamento europeo 679/2016 disciplinano le modalità di gestione del *Data Breach* da parte del Titolare del trattamento e le situazioni in cui risulta necessaria la notifica al Garante di avvenuta violazione.

Nella istruzione operativa IO.GEN06.01/1 "Gestione delle violazioni di dati personali (data breach)" è descritto nel dettaglio il flusso delle attività da svolgere.

La gestione della violazione verrà avviata dal Referente Privacy o, in sua assenza, da un delegato che agiranno secondo le indicazioni del Direttore Operativo.

Quando effettuare la notifica al Garante:

Nel caso in cui la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve notificare l'avvenuta violazione all'autorità di controllo italiana (Garante per la privacy) entro le 72 ore dal momento in cui ne è venuto a conoscenza o comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non venga effettuata entro le 72 ore, il Titolare del trattamento dovrà motivarne il ritardo.

La notifica deve almeno:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notifica di una violazione di dati personali deve essere inviata al Garante tramite apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/>.

a. Quando effettuare la notifica all'interessato:

Il Titolare del trattamento deve notificare agli interessati la violazione dei dati subito nei casi in cui le conseguenze del *Data Breach* siano tali da comportare un rischio elevato per i diritti e le libertà delle persone fisiche; non è richiesta la comunicazione all'interessato qualora sussista una delle ipotesi specificamente disciplinate dal paragrafo 2 dell'art. 34 del GDPR.

b. Tenuta del registro incidenti/violazioni dei dati:

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Dovranno, inoltre, essere conservati i documenti di comunicazione inviati al Garante. Il Referente Privacy attiva la procedura di iscrizione nel registro secondo quanto previsto dalla istruzione operativa "Gestione delle violazioni di dati personali (data breach)".

c. Chiusura processo di incidente/violazioni di dati

Il Referente Privacy aggiorna il DM e il PM dello studio sulle azioni intraprese ed eventualmente ancora da intraprendere.

1.1.2. Studio clinico supportato da FROM - E.T.S. per conto di terzi

FROM – E.T.S. si atterrà alle prescrizioni ricevute nella lettera di nomina a Responsabile al trattamento ex art. 28 GDPR.

Il DO tramite il Referente Privacy informa il Titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione in prima istanza telefonicamente e successivamente via mail ai contatti forniti dal Titolare al trattamento. La comunicazione dovrà contenere almeno i seguenti punti:

- natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del Data Protection Officer o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

6. BIBLIOGRAFIA

- Determina 19 giugno 2015 Determina inerente i requisiti minimi necessari per le strutture sanitarie, che eseguono sperimentazioni di fase I di cui all'articolo 11 del decreto del Presidente della Repubblica 21 settembre 2001, n. 439 e di cui all'articolo 31, comma 3 del decreto legislativo 6 novembre 2007, n. 200 (Determina n. 809/2015);
- D.Lvo n. 196/2003 Codice in materia di protezione dei dati personali;
- D.Lvo n. 101/2018 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);
- Regulation (EU) 2016/679 General Data Protection Regulation (GDPR);
- Regulation (EU) 2014/536 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC
- ICH-E6 (R2): Guideline for good clinical practice - European Medicines Agency, 2017.
- Istruzione operativa "Gestione delle violazioni di dati personali (Data Breach)"

7. ALLEGATI

IO.GEN06.01/1 ISTRUZIONI OPERATIVE GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

IO.GEN06.01.1/1 ISTRUZIONI FLUSSO DATA BREACH

IO.GEN06.01.2/1 DATI DI CONTATTO

8. CRONOLOGIA VERSIONI

| Versione | Data | Cambiamenti introdotti |
|----------|------------|------------------------|
| 1 | 15/09/2023 | Procedura iniziale |