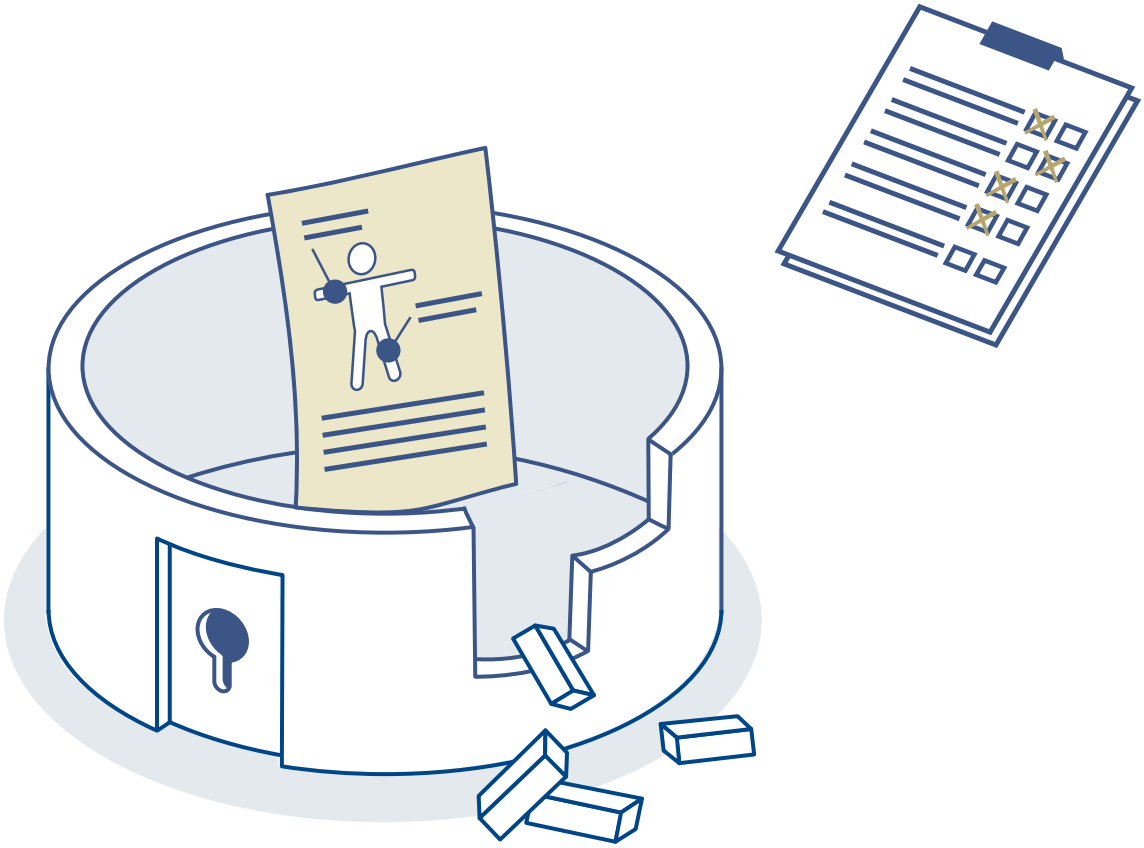
Check-list e procedura in caso di violazioni della protezione dei dati



Versione 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Sommario

1 Aspetti generali

Il presente documento si propone di fornire supporto per prepararsi ad affrontare e gestire eventuali violazioni della sicurezza dei dati, garantendo il rispetto dei requisiti di legge. Oltre alla definizione di violazione e all'obbligo di notifica, il documento include una check-list per la preparazione e una procedura per la gestione degli eventi.

Per gli argomenti riguardo ai quali la legge non prevede norme specifiche, sono state formulate raccomandazioni per un possibile modo di procedere. Per evitare ridondanze rispetto ai Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio, che prevedono raccomandazioni e misure in caso di incidenti relativi alla sicurezza, si rinvia in parte alle singole raccomandazioni (E) e misure (M-10.XX) della protezione di base IT.

1.1 Definizione di violazione della sicurezza dei dati

Analogamente agli obiettivi concernenti la sicurezza delle informazioni, anche l'obiettivo della sicurezza dei dati consiste nella protezione dei dati personali da perdite di riservatezza, integrità o disponibilità, mediante adozione di misure adeguate.

Ai sensi della Legge sulla protezione dei dati, sussiste una violazione della sicurezza dei dati

— se dati personali vengono persi, cancellati, distrutti o modificati involontariamente o illecitamente oppure vengono rivelati o resi accessibili a persone non autorizzate, ad es. in caso di perdita di un supporto dati come laptop, CD, chiavette USB ecc., di distruzione di dati a causa di eventi naturali come ad es. inondazioni, incendi oppure di attacchi di phishing.

Indizi di una possibile violazione della sicurezza dei dati sono ad esempio:

— irruzione nello studio medico mediante effrazione;
— incendio.

1.2 Obbligo di notifica

Se la violazione della sicurezza dei dati comporta un elevato rischio per le persone interessate, deve essere notificata all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) . Secondo la legge, sussiste un rischio elevato se la violazione della sicurezza dei dati può presumibilmente mettere in pericolo i diritti fondamentali o i diritti della personalità di singole persone interessate.

Possibili esempi di rischio elevato possono essere i seguenti:

— si verifica un attacco ai server dello studio medico e si suppone che l'autore abbia avuto accesso a tutti i dati sanitari dei pazienti;
— a causa di un'anomalia tecnica, i dati sanitari dei pazienti vengono cancellati e non è possibile ripristinarli mediante il backup;
— i dati dei pazienti vengono trasmessi per e-mail a terzi senza consenso e in formato non criptato.

[1] https://www.edoeb.admin.ch/edoeb/it/home.html

1.3 Check-list

La seguente check-list ha lo scopo di fornire aiuto per l'individuazione dei punti da definire preventivamente. In tal modo, in caso di (presunta) violazione della sicurezza dei dati, alcune importanti fasi della procedura e le relative decisioni da prendere sono già definite.

Definizione di persona responsabile (responsabile della sicurezza dei dati)

In caso di violazioni della sicurezza dei dati, soprattutto se è previsto l'obbligo di notifica ai sensi del punto 1.2, deve essere informato immediatamente il titolare dello studio medico, al fine di adottare insieme a lui le misure necessarie.

Analogamente alla misura M-10.01 dei Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio-D3, deve essere definita una persona che sia responsabile per quanto concerne le violazioni della sicurezza dei dati (di seguito detta Responsabile della sicurezza dei dati). Si può trattare della stessa persona già nominata responsabile degli incidenti concernenti la sicurezza secondo la protezione di base IT (cfr. anche E1 dei Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio-D3).

Documento informativo sulle violazioni della sicurezza dei dati

Si raccomanda di redigere preventivamente un documento informativo che fornisca supporto al personale per l'individuazione di eventuali violazioni della sicurezza dei dati. Come ulteriore aiuto, potrebbero essere inseriti nel documento informativo esempi di possibili indizi di una violazione della sicurezza dei dati. A titolo orientativo può essere utilizzato l'elenco riportato sopra al punto 1.1 Definizione di violazione della sicurezza dei dati.

Si raccomanda inoltre di definire nel documento informativo istruzioni concrete per il personale su come agire, sensibilizzando inoltre i collaboratori (cfr. il punto 2 Procedura in caso di violazioni della sicurezza dei dati).

Documentazione

La Legge sulla protezione dei dati prevede che le violazioni della sicurezza dei dati debbano essere documentate dalla persona responsabile della sicurezza dei dati nella misura in cui siano soggette all'obbligo di notifica.

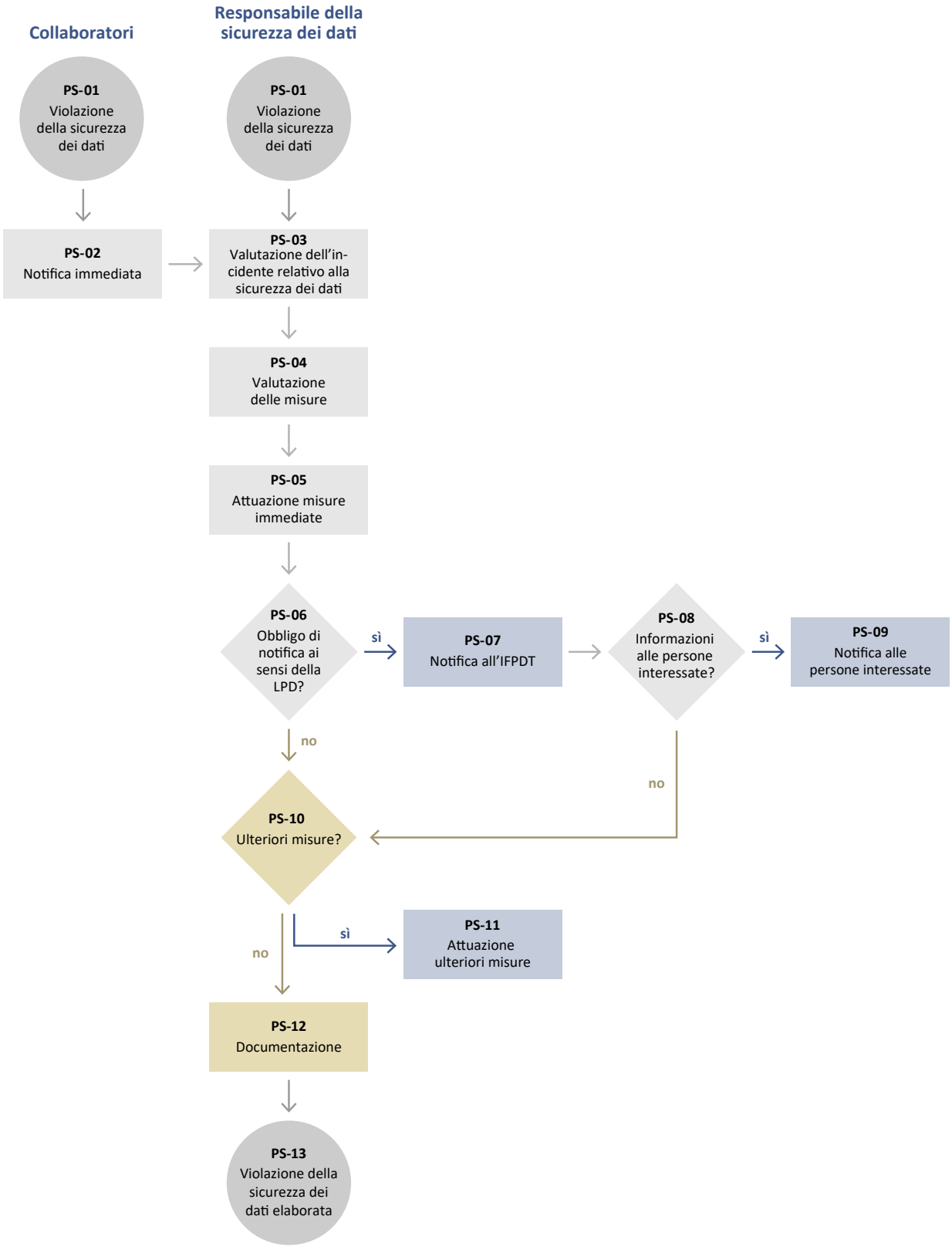
La documentazione deve contenere almeno:

- tutti i fatti inerenti alla violazione della sicurezza dei dati (cfr anche sotto il punto 2 Procedura in caso di violazioni della sicurezza dei dati passaggio «PS-07, notifica all'IFPDT»),
- gli effetti della violazione della sicurezza dei dati e
- le misure adottate per contenere o porre rimedio alla violazione della sicurezza dei dati.

Se la violazione della sicurezza dei dati non è soggetta all'obbligo di notifica, si raccomanda di documentare comunque il motivo della rinuncia alla notifica.

La documentazione ai sensi dell'Ordinanza sulla protezione dei dati, deve essere conservata per un periodo di almeno due anni a decorrere dalla data della violazione della sicurezza dei dati.

2 Procedura in caso di violazioni della sicurezza dei dati



Passaggio della procedura	Attività	Descrizione dell'attività
PS-01	Violazione della sicurezza dei dati	Si è verificata una violazione della sicurezza dei dati che è stata individuata dalla persona responsabile della sicurezza dei dati o da un/una collaboratore/trice (cfr. sopra il punto 1.1 Definizione di violazione della sicurezza dei dati).
PS-02	Notifica immediata	Se il personale ha individuato una (potenziale) violazione della sicurezza dei dati, ne deve essere informata immediatamente la persona responsabile della sicurezza dei dati (cfr. sopra il punto 1.3 Check-list paragrafo «Definizione di persona responsabile»).
PS-03	Valutazione della violazione della sicurezza dei dati	La persona responsabile della sicurezza dei dati valuta la notifica o la presunta violazione della sicurezza dei dati. Per la valutazione è possibile ricorrere alla misura M-10.03 dei Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio.
PS-04	Valutazione delle misure	La persona responsabile della sicurezza dei dati valuta la violazione della sicurezza dei dati sulla base del rischio atteso e stabilisce se sia necessario adottare misure per gestire la violazione e quali. In fase di definizione delle misure, è possibile fare distinzione tra misure immediate per contenere gli effetti dell'incidente e misure per individuarne la causa e gestire l'incidente a lungo termine.
PS-05	Attuazione delle misure immediate	Se nel passaggio PS-04 sono state definite misure immediate, esse devono essere attuate direttamente al fine di ridurre al minimo l'entità della violazione della sicurezza dei dati (ad es. isolamento o disattivazione di singoli servizi o sistemi).
PS-06	Obbligo di notifica ai sensi della LPD?	In un passaggio successivo, la persona responsabile della sicurezza dei dati verifica se la violazione della sicurezza dei dati possa comportare un rischio elevato per le persone interessate (cfr. sopra il punto 1.2 Obbligo di notifica) e se pertanto sussista un obbligo di notifica all'IFPDT.
PS-07	Notifica all'IFPDT	Se sussiste l'obbligo di notifica, deve essere preparato il testo della notifica all'IFPDT. La Legge sulla protezione dei dati prevede che la notifica all'IFPDT della violazione della sicurezza dei dati debba contenere almeno i seguenti punti: — tipo di violazione della sicurezza dei dati (ad es. distruzione dei dati, furto di dati ecc.); — se note, data, ora e durata della violazione; — per quanto possibile, le categorie di dati personali e il quantitativo approssimativo di dati personali interessati; — per quanto possibile, le categorie di persone interessate e il loro numero approssimativo; — conseguenze della violazione della sicurezza dei dati, ivi inclusi gli eventuali rischi per le persone interessate (ad es. impossibilità di accedere alle cartelle cliniche e quindi ricostruibilità solo parziale del trattamento, con possibili conseguenti rischi per la salute delle persone interessate; pubblicazione delle cartelle cliniche sul «dark Web» con conseguenti rischi di violazioni dei diritti della personalità delle persone interessate); — misure adottate o previste per rimediare al problema o ridurne le conseguenze (ad es. ripristino dei dati da backup nel caso di dati digitali); e — nome e dati di contatto di un/una referente. Se non è possibile comunicare tutte le informazioni allo stesso tempo, le informazioni mancanti possono essere messe a disposizione dell'IFPDT progressivamente entro un termine ragionevole. **Avvertenza:** per determinare quali categorie di persone interessate e di dati sono coinvolte dalla violazione della sicurezza dei dati, potrebbe risultare utile un registro delle attività di trattamento redatto precedentemente (cfr. al riguardo il documento Modello di registro delle attività di trattamento dei dati e relativa guida).

PS-08	Informazioni alle persone interessate?	Il responsabile della sicurezza dei dati valuta se debbano essere informate della violazione della sicurezza dei dati le persone interessate. Le persone interessate devono essere informate se: — è necessario adottare misure di protezione (ad es. modifica di dati di accesso come password) oppure — l'IFPDT lo richiede. La persona responsabile della sicurezza dei dati può limitare o rinviare l'invio di informazioni alle persone interessate oppure rinunciarvi del tutto se: — ciò è necessario sulla base di un interesse preponderante; — l'invio di informazioni è vietato ai sensi di un obbligo di riservatezza previsto dalla legge; — l'invio di informazioni non è possibile o comporterebbe oneri sproporzionati; oppure — la comunicazione delle informazioni alle persone interessate è comunque garantita in modo equiparabile tramite un avviso pubblico.
PS-09	Notifica alle persone interessate	Se il risultato di PS-08 è stato che è necessario informare le persone interessate, deve essere predisposta una notifica in merito alla violazione della sicurezza dei dati. La notifica deve contenere almeno le seguenti informazioni: — tipo di violazione della sicurezza dei dati (ad es. distruzione dei dati, furto di dati ecc.); — conseguenze della violazione della sicurezza, ivi inclusi gli eventuali rischi per le persone interessate (ad es. impossibilità di accedere alle cartelle cliniche e quindi ricostruibilità solo parziale del trattamento, con possibili conseguenti rischi per la salute delle persone interessate; pubblicazione delle cartelle cliniche sul «dark Web» con conseguenti rischi di violazioni dei diritti della personalità delle persone interessate); — misure adottate o previste per rimediare al problema o ridurne le conseguenze (ad es. ripristino dei dati da backup in caso di perdita di dati digitali); — nome e dati di contatto di un/una referente.
PS-10	Ulteriori misure?	Una volta attuate le misure immediate, verificata la sussistenza dell'obbligo di notifica all'IFPDT nonché alle persone interessate ed inviate le eventuali notifiche e informazioni, occorre stabilire se sono necessarie ulteriori misure. Potrebbero infatti essere necessarie ulteriori misure attuabili tuttavia solo a medio-lungo termine (vedi anche PS-04).
PS-11	Attuazione delle ulteriori misure	Se è stata rilevata la necessità di adottare ulteriori misure, si può passare alla loro attuazione (cfr. anche M-10.07 e M-10-08 dei Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio).
PS-12	Documentazione	La persona responsabile della sicurezza dei dati deve documentare in ogni caso la violazione della sicurezza dei dati (cfr. sopra il punto 1.3 Check-list paragrafo «Documentazione»).
PS-13	Violazione della sicurezza dei dati elaborata	Una volta attuate le misure necessarie, effettuata l'eventuale notifica ed effettuata la documentazione della violazione della sicurezza dei dati, la procedura per la gestione dell'incidente è conclusa.

Colophon
Editrice: FMH Federazione die medici svizzeri
Pubblicazione: marzo 2023
www.fmh.ch