Guida per la conservazione e l’archiviazione

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 Fondamenti giuridici per la cancellazione

1.1 Aspetti generali

Il presente documento fornisce indicazioni sui casi in cui i dati personali possono o devono essere cancellati o distrutti e su quali aspetti devono essere considerati a tale riguardo.

Il trattamento dei dati personali è consentito solo per un determinato scopo specifico e nella misura in cui essi siano idonei e necessari a tale scopo. Non appena i dati non sono più necessari ai fini del trattamento previsto, devono essere cancellati, distrutti o resi anonimi.

Nella misura in cui non sussista più alcun motivo che ne giustifichi il trattamento, le persone interessate hanno inoltre il diritto di richiedere la cancellazione dei dati personali trattati che le riguardano. Possibili giustificazioni sono i termini di prescrizione e di conservazione dei dati che sono disciplinati in modo differente a seconda del caso.

Avvertenza: per quanto concerne i termini di conservazione previsti dalla legge può essere utile l'apposito riepilogo dei termini di conservazione di legge messo a disposizione dalla FMH [Rechtliche Grundlagen im medizinischen Alltag].

1.2 Diritto di cancellazione della persona interessata

In caso di richiesta di cancellazione è necessario osservare i seguenti punti:

— la persona richiedente deve essere identificata;
— va verificato se sussistono obblighi di conservazione di legge o altri motivi cogenti che impediscano la cancellazione o la distruzione dei dati. Se non sussistono motivi di questo tipo, i dati personali devono essere cancellati o distrutti;
— deve essere inviata alla persona richiedente una comunicazione in merito all'avvenuta cancellazione dei suoi dati. Se i dati non sono stati cancellati, la persona richiedente ne deve essere informata indicandone i motivi.

2 Requisiti giuridici per la conservazione e l'archiviazione

2.1 Termini di conservazione previsti dalla legge (situazione al 31.10.2022)

Nelle strutture sanitarie viene prodotta quotidianamente documentazione che include informazioni (dati personali) su pazienti e collaboratori della struttura stessa o di fornitori di servizi. Il periodo di conservazione di tale documentazione si basa sul principio di proporzionalità. I dati personali possono quindi essere conservati per il tempo necessario e opportuno per l'adempimento del compito. Le leggi federali e i decreti cantonali stabiliscono inoltre termini di conservazione concreti. Oltre a ciò, uno scopo della conservazione può consistere anche nella tracciabilità di un trattamento medico oppure nella valutazione di una prestazione o di fatti per scopi probatori.

I dati aziendali che non contengono dati personali possono in linea di principio essere conservati a tempo indeterminato. Devono comunque essere conservati come minimo per il tempo previsto dai termini di conservazione di legge.

A titolo indicativo, le seguenti tabelle contengono un riepilogo dei requisiti previsti dalla legge per il tipo e la durata della conservazione. Se non sussistono regolamentazioni per la conservazione, la Legge sulla protezione dei dati richiede che vengano stabiliti come minimo i relativi criteri (art. 12 LPD).

Dato che durante l'intero periodo di conservazione bisogna fare in modo che la protezione e la sicurezza dei dati siano sempre garantite, nell'ultimo capitolo del presente documento è disponibile anche una check-list che indica alcune possibili misure tecniche e organizzative per preservare la sicurezza dei dati.

Excursus: cessione/cessazione dell'attività – Obbligo di conservazione delle cartelle cliniche

In linea di principio, in caso di cessazione o cessione dell'attività, l'obbligo di conservazione delle cartelle cliniche permane. A tale proposito va fatta distinzione riguardo al soggetto con il quale i pazienti hanno stipulato un contratto di trattamento. Ciò significa che se il contratto di trattamento è stato stipulato con uno studio medico di gruppo (SA o Sagl), l'obbligo di conservazione resta in capo allo studio medico. Se invece il contratto di trattamento è stato stipulato con il medico, è quest'ultimo a dover garantire un'adeguata conservazione dei dati.

Se lo studio medico o l'ulteriore trattamento medico dei pazienti viene rilevato da un successore (una persona fisica o giuridica), ciò non significa automaticamente che le cartelle cliniche gli possano essere consegnate o che ne possa prendere visione. Il successore potrà prendere visione delle cartelle cliniche solo in presenza del consenso da parte del/della paziente. Se il/la paziente non ha (ancora) dato il proprio consenso, può essere applicato il cosiddetto «principio dei due armadi». Ciò significa che in un armadio verranno tenute le cartelle cliniche per le quali i pazienti hanno dato il consenso al trattamento da parte del successore e nel secondo armadio quelle per le quali invece non è stato (ancora) ottenuto il consenso alla consultazione. In caso di gestione delle cartelle cliniche in formato elettronico si applica in linea di principio la stessa regolamentazione.

In caso di cessazione dell'attività, i medici sono comunque tenuti a fornire ai pazienti informazioni sulla loro cartella clinica entro il termine prescritto dalla legge. Di conseguenza, il medico deve provvedere affinché le cartelle cliniche vengano conservate in modo adeguato e siano protette da accessi non autorizzati. Le può ad esempio conservare privatamente oppure può delegarne la conservazione a terzi.

Avvertenza: occorre consultare anche le eventuali disposizioni cantonali applicabili (leggi sanitarie cantonali o leggi sui pazienti), in quanto possono prevedere periodi di conservazione più lunghi o particolari forme di conservazione.

2.2 Riepilogo dei periodi di conservazione previsti dalla legge

Dati sanitari/documentazione del paziente		
Tipo di documentazione	**Tipo e durata della conservazione**	**Fondamenti giuridici**
Cartella clinica	A causa del termine di prescrizione previsto dalle norme sulla responsabilità civile, le cartelle cliniche devono essere conservate per **20 anni** dopo la fine delle cure. Inoltre, possono essere conservate solo con il consenso delle persone interessate. *Per quanto concerne gli obblighi applicabili in materia di tipo e durata della conservazione, occorre consultare le leggi sanitarie cantonali applicabili al luogo in cui ha sede lo studio medico. Per le cartelle cliniche, le disposizioni cantonali prevedono come minimo un periodo di conservazione di **10 anni**. Tuttavia, alcuni Cantoni prevedono un obbligo di conservazione di **20 anni** in casi specifici. Alcuni (pochi) decreti cantonali prescrivono la distruzione della documentazione dopo 20 anni qualora non vi siano interessi preponderanti che vi si oppongono.*	Art. 60 cpv. 1bis e 2 Codice delle Obbligazioni (CO)/ Art. 128a CO Art. 12 Codice deontologico della FMH Leggi sanitarie cantonali (in base all'ubicazione dello studio medico)
Documentazione delle applicazioni radiologiche e del grado di occupazione dell'impianto	I dati devono essere conservati secondo le disposizioni applicabili alle cartelle cliniche. Tuttavia, il termine di **20 anni** si applica ai parametri di esposizione per impianti a raggi X per uso terapeutico, nonché ai dati che vengono raccolti in relazione ai sistemi a raggi X per il controllo del posizionamento, la pianificazione e la simulazione nella radioterapia. I dati raccolti nell'ambito di applicazioni di dose media e forte e per la mammografia devono essere conservati per **10 anni**.	Art. 20 cpv. 5 lett. a Ordinanza sui raggi X (OrX) Art. 20 cpv. 5 lett. b OrX
Documentazione dell'utilizzo di sangue e suoi derivati	Se, ai sensi Legge sugli agenti terapeutici, insorge un obbligo di conservazione della documentazione relativa all'utilizzo di sangue e suoi derivati (ad es. prelievo di sangue), tale documentazione deve essere conservata per **30 anni**. ***Avvertenza:** sono previste disposizioni speciali in caso di cessazione dell'attività prima della scadenza del termine di conservazione.*	Artt. 39 e 40 Legge federale sui medicamenti e i dispositivi medici (Legge sugli agenti terapeutici, LATer)
Documentazione del trattamento di organi, tessuti o cellule	Se, ai sensi Legge sul trapianto di organi, tessuti e cellule insorge un obbligo di conservazione della documentazione relativa al trattamento di organi, tessuti o cellule, tale documentazione deve essere conservata per **20 anni**.	Artt. 34 e 35 Legge federale sul trapianto di organi, tessuti e cellule (Legge sui trapianti)
Documenti inerenti alla medicina del lavoro	**40 anni** per i documenti inerenti alla medicina del lavoro.	Art. 8 allegato 4 al Codice deontologico della FMH

Risultati di esami genetici presintomatici	Se, ai sensi Legge sul trapianto di organi, tessuti e cellule insorge un obbligo di conservazione della documentazione relativa al trattamento di organi, tessuti o cellule, tale documentazione deve essere conservata per 20 anni.	Art. 28 Legge federale sugli esami genetici sull'essere umano (LEGU)
Documentazione delle informazioni fornite ai donatori viventi di organi, tessuti o cellule	I medici che prelevano organi, tessuti o cellule devono, prima del prelievo, informare il potenziale donatore in modo esauriente e comprensibile, per scritto e oralmente. La documentazione relativa alle informazioni al donatore vivente deve essere conservata, **separatamente** dalla cartella clinica, **per un periodo di 10 anni**.	Art. 9 cpv. 4 e art. 10 cpv. 2 Ordinanza concernente il trapianto di organi, tessuti e cellule umani (Ordinanza sui trapianti)
Obbligo di documentazione giustificativa per le sostanze controllate ai sensi dell'Ordinanza sul controllo degli stupefacenti	I documenti giustificativi, i dati e i supporti di dati concernenti la prescrizione e il commercio di sostanze controllate ai sensi dell'Ordinanza sul controllo degli stupefacenti devono essere conservati per un periodo di **10 anni**.	Art. 62 Ordinanza sul controllo degli stupefacenti (OCStup)

Documentazione sui collaboratori		
Tipo di documentazione	**Tipo e durata della conservazione**	**Fondamenti giuridici**
Dossier personale (contratti di lavoro, dossier personali incluse le valutazioni, certificati di lavoro, attestati, note nel dossier, disdetta, ecc.)	**5 anni** a decorrere dalla data di uscita del collaboratore, in formato cartaceo (analogico) o elettronico (digitale), in modo che i fatti possano essere dimostrati e resi nuovamente leggibili in qualsiasi momento.	Art. 330a CO in combinato disposto con l'art. 128 CO/Art. 46 Legge sul lavoro (LL) e art. 73 Ordinanza 1 concernente la legge sul lavoro (OLL 1)
Salari (certificati salariali, conteggi, assicurazioni sociali e cassa pensioni)	**5 anni** a decorrere dalla data di uscita del collaboratore, in formato cartaceo (analogico) o elettronico (digitale), in modo che i fatti possano essere dimostrati e resi nuovamente leggibili in qualsiasi momento.	Art. 128 cpv. 3 CO
Registrazione dell'orario di lavoro (orari di lavoro inseriti in un apposito sistema di registrazione)	**5 anni** a decorrere dalla data di uscita del collaboratore, in formato cartaceo (analogico) o elettronico (digitale), in modo che i fatti possano essere dimostrati e resi nuovamente leggibili in qualsiasi momento.	Art. 46 Legge sul lavoro (LL) e art. 73 Ordinanza 1 concernente la legge sul lavoro (OLL 1)

Documenti aziendali		
Tipo di documentazione	**Tipo e durata della conservazione**	**Fondamenti giuridici**
Fatture (debitori, creditori, chiusure annuali ivi inclusi i rapporti di revisione)	**10 anni** a decorrere dalla fine dell'esercizio, in formato cartaceo (analogico), elettronico (digitale) o in modo equivalente, affinché i fatti possano essere dimostrati e resi nuovamente leggibili in qualsiasi momento.	Artt. 958 e 958f CO
Documentazione fiscale (tutti i documenti relativi alle imposte)		
Spesen (giustificativi delle spese e tutti i documenti relativi alle spese)		

Altre documentazioni		
Tipo di documentazione	**Tipo e durata della conservazione**	**Fondamenti giuridici**
Verbalizzazione in caso di trattamento automatizzato di dati personali degni di particolare protezione/Profilazione	Nella misura in cui lo studio medico tratti, in modo automatizzato o digitalizzato, dati personali degni di particolare protezione e le misure impiegate non garantiscano una sufficiente protezione dei dati, lo studio medico è tenuto a verbalizzare il trattamento. I verbali devono essere conservati per **un anno** con modalità adatte alla revisione.	Art. 4 Ordinanza sulla protezione dei dati (OPDa)
Valutazione d'impatto sulla protezione dei dati (tutti i documenti rilevanti nell'ambito della valutazione d'impatto sulla protezione dei dati)	Almeno **2 anni** dalla fine del trattamento dei dati. ***Avvertenza:*** *sussiste l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati se vengono trattati dati personali che, in caso di eventuale violazione della riservatezza o dell'integrità dei dati oppure in caso di abusi, comporterebbero un elevato rischio elevato per la personalità o i diritti fondamentali della persona interessata.* *Sono esclusi dall'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati i responsabili del trattamento privati che sono tenuti a trattare i dati per legge. Ciò significa che le strutture sanitarie di diritto privato con l'obbligo di legge di tenere una cartella clinica non sono tenute a effettuare una valutazione d'impatto sulla protezione dei dati. Ciò vale solo per l'obbligo di tenere la cartella clinica prescritto dalla legge. Qualora in strutture sanitarie vengano ad esempio utilizzati prodotti basati su cloud, potrebbe invece rendersi necessario effettuare una valutazione d'impatto sulla protezione dei dati in quanto l'utilizzo del cloud non è prescritto dalla legge.*	Art. 14 OPDa
Documentazione relativa a violazioni della sicurezza dei dati (tutti i documenti rilevanti in relazione alla notifica di una violazione della sicurezza dei dati)	Almeno **2 anni** a partire dal momento della notifica di una violazione della sicurezza dei dati.	Art. 15 OPDa

2.3 Check-list per la conservazione e l'archiviazione di dati personali

Se i dati devono essere conservati per uno o più motivi sopraccitati o per altri motivi, occorre fare in modo che la sicurezza dei dati sia garantita anche durante il periodo di conservazione. Le seguenti check-list possono essere utilizzate come aiuto per garantire la sicurezza dei dati durante la conservazione.

Avvertenza: *la check-list «Cancellazione» fornisce aiuto in relazione alla questione se e in che modo sia consentito cancellare i dati personali.*

Ulteriori raccomandazioni sui requisiti di sicurezza negli studi medici sono disponibili nel documento Requisiti minimi per la protezione di base IT per assistenti di studio medico e medici titolari di studio.

Luogo		
Misura	**Spiegazione/avvertenze**	**Check**
Gestione degli accessi	I supporti dati contenenti dati personali devono essere conservati in un luogo al quale abbia accesso solo una cerchia di persone selezionata. Ad esempio in schedari, archivi o locali chiudibili a chiave o dotati di un sistema di accesso basato su badge ecc. per i quali solo le persone autorizzate siano in possesso delle chiavi o di un badge.	☐
Protezione da eventi ambientali	I supporti dati devono essere conservati in modo tale che non possano essere distrutti da allagamenti, incendi o altri eventi ambientali.	☐

Formato		
Misura	**Spiegazione/avvertenze**	**Check**
Protezione da corrosione/ decadimento della carta	I supporti dati devono essere conservati in modo tale che non possano essere distrutti da corrosione (supporti dati digitali) o dal deterioramento della carta (supporti dati fisici).	☐
Formati attuali	I dati digitali devono essere salvati in un formato che possa essere letto a lungo termine. Se ciò non è possibile, occorre garantire che i dati vengano convertiti tempestivamente in un formato attuale. I formati qui di seguito elencati sono adatti all'archiviazione:	☐

Campo di applicazione	**Formati adatti all'archiviazione**
Documenti di Office (Word, Excel, Power-Point, Outlook)	PDF/A
Testo (non formattato)	TXT
Fogli di lavoro	CSV
Banche dati	SIARD
Immagini digitali	TIFF o PDF/A
Audio	WAVE
Video	MPEG-4

Avvertenza: *La trasmissione di dati in un altro formato può alterare i dati e causare altre compromissioni.*

Accesso		
Misura	**Spiegazione/avvertenze**	**Check**
Autorizzazioni all'accesso	Devono essere autorizzate ad accedere ai dati solo le persone che ne hanno effettivamente necessità (ad es. per scopi probatori nel contesto di pretese di responsabilità, per garantirne la leggibilità ecc.). Il numero delle persone autorizzate ad accedere ai dati deve essere limitato allo stretto necessario (ad es. limitazione a una o due persone). Occorre garantire che le autorizzazioni possano essere adeguate alle circostanze (ad es. mutazioni, sostituzioni ecc.).	☐
Protezione dei mezzi di autenticazione	Occorre garantire che i mezzi di autenticazione (ad es. nome utente/password, chiavi, badge) siano disponibili per tutto il periodo di conservazione, ma siano protetti da accessi da parte di persone non autorizzate.	☐
Tecnologie di crittografia attuali	Occorre garantire che vengano utilizzate tecnologie di crittografia tali da consentire la decodifica durante l'intero periodo di conservazione. Nella misura in cui le tecnologie subiscano cambiamenti durante il periodo di conservazione, i dati devono essere tempestivamente criptati con una nuova tecnologia.	☐
Backup	Se i dati vengono conservati sotto forma di backup digitale, la possibilità di ripristinarli da backup deve essere testata periodicamente (si raccomanda una volta all'anno). ***Avvertenza:*** *la raccomandazione numero 8 dei Requisiti minimi per la protezione di base IT della FMH contiene ulteriori aspetti da osservare in relazione alla creazione di backup.*	☐

Tracciabilità		
Misura	**Spiegazione/avvertenze**	**Check**
Protezione contro le modifiche non autorizzate	Occorre garantire che le modifiche ai dati conservati siano visibili e tracciabili. — Documenti cartacei e supporti dati rimovibili: ad es. verbale delle modifiche creato mediante registrazioni manuali — Supporti dati digitali: ad es. verbalizzazione delle modifiche (logging) anche durante la conservazione.	☐
Protezione dei verbali	I sistemi di verbalizzazione e i verbali devono essere protetti da accessi non autorizzati.	☐

Collaborazione con terzi		
Misura	**Spiegazione/avvertenze**	**Check**
Disposizioni contrattuali	Se vi sono terzi coinvolti nella conservazione dei dati, occorre garantire che siano stati concordati requisiti contrattuali per la conservazione e che il loro rispetto sia documentato. ***Avvertenza:*** *quando si ricorre a fornitori di servizi per la conservazione, occorre garantire che questi ultimi siano selezionati con cura e istruiti in merito ai loro obblighi, il cui rispetto deve essere verificato con regolarità. Si raccomanda di far firmare ai fornitori di servizi un accordo sulla riservatezza. Qui è possibile scaricare il relativo modello.*	☐
Gestione in caso di violazione della sicurezza dei dati	Se vi sono terzi coinvolti nella conservazione dei dati, occorre garantire che sia stata definita una procedura in caso di violazione della sicurezza dei dati. ***Avvertenza:*** *a tale proposito può essere utile la raccomandazione numero 10 dei Requisiti minimi per la protezione di base IT della FMH (Misure preventive per la gestione violazioni della sicurezza dei dati).*	☐
Consegna contrattualmente concordata	Se vi sono terzi coinvolti nella conservazione dei dati, occorre garantire che al termine della collaborazione abbia luogo la riconsegna dei dati.	☐

Adempimento degli obblighi		
Misura	**Spiegazione/avvertenze**	**Check**
Controllo dei termini di conservazione	I termini di conservazione sono garantiti e, una volta scaduto il termine, i dati personali vengono cancellati o distrutti senza indugio e irrevocabilmente. ***Avvertenza:*** *Per quanto concerne la cancellazione/distruzione dei dati personali è possibile utilizzare come aiuto la check-list «Cancellazione».*	☐
Documentazione	I termini di conservazione e la successiva cancellazione/distruzione devono essere documentati.	☐

3 Requisiti tecnici per la cancellazione

3.1 Definizione di cancellazione/distruzione

Ai sensi della Legge sulla protezione dei dati, con il termine distruzione dei dati ci si riferisce alla distruzione fisica di dati o alla cancellazione irrevocabile dei dati in formato digitale. Mentre per distruzione fisica si intende la distruzione di un supporto dati (documenti cartacei, chiavette USB, CD ecc.), il termine cancellazione si riferisce all'atto di rendere i dati salvati irriconoscibili in modo che non possano essere recuperati. Diversamente dalla distruzione, con la cancellazione il supporto dati non viene distrutto.

Anche la cifratura dei dati può essere sostanzialmente considerata come un'operazione che rende irriconoscibili i dati se le chiavi ad essa associate e necessarie per decifrare i dati vengono eliminate.

3.2 Aspetti organizzativi

Per una cancellazione tempestiva si raccomanda di elaborare una procedura o un processo che definisca che cosa deve essere cancellato/distrutto, quando e a quali condizioni. A questo proposito può essere utile il registro delle attività di trattamento dei dati, che offre una panoramica di quali dati devono essere conservati e per quanto tempo (cfr. il modello di registro delle attività). Nella misura in cui sussista un motivo che giustifichi la conservazione dei dati, non bisogna procedere alla loro cancellazione. Un motivo giustificativo sarebbe ad esempio il consenso del paziente a un'ulteriore conservazione.

3.3 Considerazione dei casi speciali

I dati personali devono essere cancellati in modo irrevocabile o distrutti, tenendo in considerazione i termini di conservazione e di prescrizione previsti dalla legge, in sequenza dopo la scadenza del termine specifico. I dati conservati in archivi, copie di backup o in e-mail non sono esclusi da questa normativa. Qui di seguito sono indicati, a titolo di aiuto, i punti da osservare e alcune procedure esemplificative.

3.3.1 Archivi

I dati o gli interi database che dovrebbero o devono essere disponibili a lungo termine, ma che non devono più essere modificati, vengono spesso spostati in archivi interni. Nella misura in cui non sussista alcun motivo giustificativo per un'ulteriore conservazione, i dati archiviati devono essere distrutti secondo i termini prescritti dalla legge.

Al fine di poter garantire una distruzione tempestiva è consigliabile, ad esempio, definire un processo di selezione annuale. Inoltre, se i dati vengono chiaramente contrassegnati prima di essere spostati nell'archivio (ad es. indicando l'anno spostamento e il termine di conservazione), si facilita la loro progressiva eliminazione.

3.3.2 Backup

È obbligatorio installare un sistema di backup per proteggersi dalle perdite di dati. I backup con cicli brevi (ad es. quotidiani o settimanali) prevedono una sovrascrittura frequente dei dati salvati. Se i dati originali presenti nel sistema vengono cancellati, anche le copie di sicurezza di tali dati spariscono rapidamente al momento del backup successivo.

Invece, con backup a cicli lunghi (ad es. mensili o annuali), le copie di sicurezza continuano a essere disponibili per un periodo più lungo. Così, in caso di ripristino, tali dati verrebbero ricostruiti, annullando la loro cancellazione.

Al fine di garantire che i dati cancellati restino tali anche dopo il ripristino di un backup, si consiglia di impostare un processo di verifica. È possibile, ad esempio, tenere un elenco contenente dati pseudonimizzati (ad es. il codice del paziente) nel quale sia indicato quali dati sono stati cancellati. Se viene effettuato un ripristino da backup, mediante tale elenco sarà possibile verificare se sono stati ripristinati anche record di dati cancellati. In tal caso, i dati possono essere di nuovo immediatamente cancellati dal sistema in uso. Se nell'elenco viene indicata anche la data della cancellazione originaria, la registrazione potrebbe essere nuovamente eliminata dopo l'ultimo backup a lungo termine.

In aggiunta a un processo di verifica di questo tipo, bisogna garantire tramite misure tecniche e organizzative che vengano verificati anche i diritti di accesso ai dati ripristinati.

3.3.3 E-mail

Nella misura in cui delle e-mail contengano dati di un singolo paziente, tali dati devono essere archiviati nella relativa cartella clinica. Se la cartella clinica viene cancellata in conformità ai termini di conservazione prescritti dalla legge, bisogna garantire che vengano cancellate anche le e-mail ad essa associate.

3.4 Requisiti di sicurezza per la cancellazione

I metodi di cancellazione e distruzione devono garantire la cancellazione definitiva. Ciò significa che deve essere scelto un metodo che renda impossibile il ripristino dei dati personali cancellati. I metodi che consentono il ripristino dei dati personali non sono conformi alle norme in materia di protezione dei dati (ad es. semplice smaltimento dei dati personali in sacchi della spazzatura/container di rifiuti oppure spostamento virtuale nel cestino della carta sul desktop/nel cloud).

La seguente tabella mostra i possibili metodi in grado di garantire una cancellazione sicura. Le spiegazioni si basano anche, in particolare, su un foglio informativo per la distruzione di dati in formato elettronico [1] che è stato pubblicato dall'Incaricato per la protezione dei dati del Canton Zurigo.

[1] https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_vernichten_elektronischer_daten.pdf

Tipo di distruzione	Descrizione	Valutazione
Distruzione fisica	Distruzione meccanica di un supporto dati (triturazione, fusione, ecc.). Sono considerati supporti dati ad esempio CD, chiavette USB, dischetti, ma anche carta ecc. ***Avvertenza:*** *se per la cancellazione/distruzione si ricorre a fornitori di servizi esterni, occorre garantire che il processo sia sufficientemente sicuro e tracciabile e che non sia possibile un ulteriore utilizzo dei supporti dati. Il processo deve essere oggetto di verifiche regolari. Lo studio medico ne resta responsabile.*	In linea di principio deve essere garantita una cancellazione conforme alle norme in materia di protezione dei dati.
Cancellazione magnetica	Speciali dispositivi di cancellazione consentono di cancellare le informazioni di interi dischi rigidi mediante una magnetizzazione specifica, in modo tale che la riproduzione dei dati diventi impossibile o molto difficoltosa. Tali dispositivi per la cancellazione possono essere utilizzati efficacemente anche su dischi rigidi difettosi. Questa procedura è adatta ai supporti dati magnetici come dischi rigidi e carte o nastri magnetici (LTO, DLT, DAT, cassette audio, videocassette).	L'irrevocabilità della cancellazione è garantita. Tuttavia, il processo rende inutilizzabili i supporti dati.
Sovrascrittura tecnica (wiping)	I singoli file o addirittura interi supporti di archiviazione riscrivibili possono essere cancellati in modo permanente sovrascrivendoli più volte con stringhe casuali (wiping). Questo metodo non è adatto ai sistemi moderni con supporti elettronici di memorizzazione volatili (Solid State Disk o SSD).	L'irrevocabilità della distruzione è garantita.
Cancellazione di dati su supporti dati elettronici non volatili (Solide State Disk)	In genere, i supporti di memorizzazione elettronici sono dotati di comandi di cancellazione (ad es. ATA Secure Erase). Se il supporto di memorizzazione non dispone di un comando di cancellazione, si consiglia di criptare prima i dati e cancellare la chiave.	L'irrevocabilità della distruzione è parzialmente garantita.

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