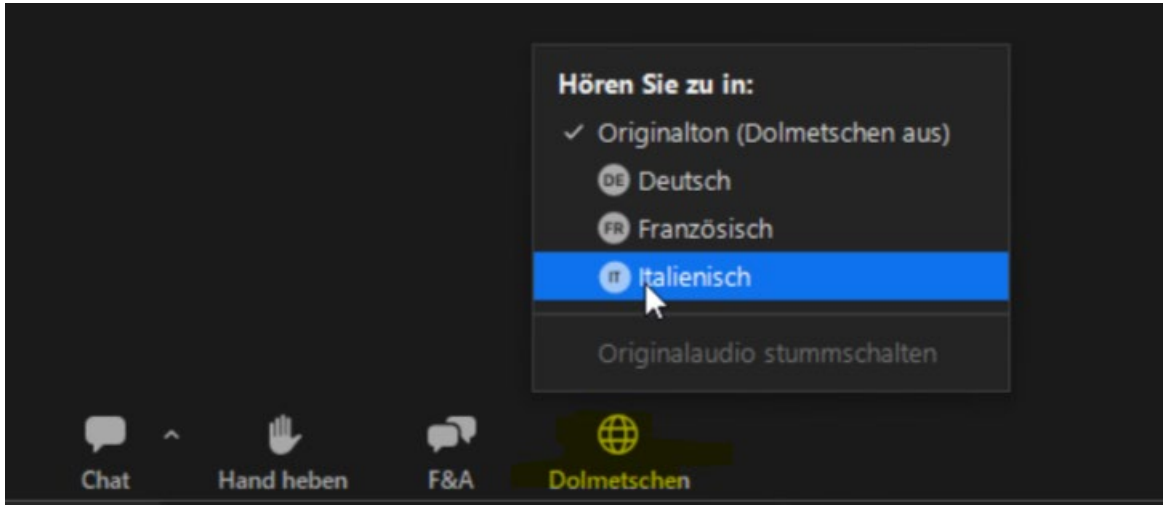
Webinar FMH: la nuova Legge sulla protezione dei dati

Neues Datenschutzgesetz / Nouvelle loi sur la protection des données

Versione tedesca e francese



Relatori e relatrici

Dr. iur. Bruno Baeriswyl
Consulente esterno per la protezione dei dati della FMH

Dr. iur. Iris Herzog-Zwitter
Giurista del Servizio giuridico della FMH

Dr. rer. biol. hum. Reinhold Sojer
Capodivisione Digitalizzazione/eHealth della FMH

Sommario

SOMMARIO	CHI	DURATA (MIN.)
Saluti e introduzione	R. Sojer	5
Obiettivi della LPD rivista	B. Baeriswyl	5
Novità essenziali	I. Herzog-Zwitter	5
Terminologia: nuovi importanti termini della LPD	B. Baeriswyl	5
Dichiarazione di consenso	I. Herzog-Zwitter	5
Disposizioni penali	B. Baeriswyl	10
Trattamento dei dati su incarico (affidamento a un responsabile esterno)	B. Baeriswyl	5
Aspetti giuridici concernenti la responsabilità	I. Herzog-Zwitter	5
Tre importanti novità	B. Baeriswyl	15
Protezione e sicurezza dei dati	R. Sojer	25
Tavola rotonda	Tutti	30
Conclusione	R. Sojer	5

Panoramica degli strumenti ausiliari

Obiettivi della LPD rivista

Legge sulla protezione dei dati (LPD) del 25 settembre 2020

In vigore dal 1° settembre 2023

Obiettivi della Legge sulla protezione dei dati (rivista) (1)

1993 → 2023

Progresso tecnologico

- Trattamento dei dati
  - Senza Internet
  - Senza smartphone
  - Senza cloud
  - ecc.

→ Adeguamento agli sviluppi tecnologici

Evoluzione del diritto europeo

- Protezione delle persone in caso di trattamento automatico dei dati personali
  (Convenzione del Consiglio d'Europa 108+)
- Protezione dei dati nel campo della polizia e della giustizia
  (Direttiva UE 2016/680)
- Diritto generale UE in materia di protezione dei dati
  (Regolamento generale sulla protezione dei dati (RGPD))

→ Adeguamento agli sviluppi giuridici

Obiettivi della Legge sulla protezione dei dati (rivista) (2)

Tematiche principali

Aumento della trasparenza del trattamento dei dati

Chiara definizione delle responsabilità («Accountability»)

Misure di sicurezza dei dati basate sul rischio

Rafforzamento dei diritti degli interessati

Intensificazione del monitoraggio da parte dell'autorità per la protezione dei dati (IFPDT) e sanzioni penali

→ Nessun cambiamento nella concezione di base

Novità essenziali

In vigore dal 1° settembre 2023

La base per tutelarsi a livello legale è il quadro dei dati oggetto di trattamento!

Nella vecchia e nella nuova legge sulla protezione dei dati i principi del trattamento dei dati sono analoghi.

Principi per il trattamento dei dati:
legittimità, il trattamento deve essere effettuato in buona fede e deve essere proporzionato, trattamento vincolato alle finalità, distruzione o anonimizzazione non appena i dati non sono più necessari per gli scopi previsti, correttezza, consenso, sicurezza dei dati

Novità essenziali

1	La definizione di dati personali degni di particolare protezione viene ampliata, includendo i dati genetici e biometrici nella misura in cui identifichino in modo univoco una persona fisica. Dal 1° settembre 2023 le norme riguarderanno solo i dati personali di persone fisiche.
2	A ogni raccolta di dati personali, la persona interessata deve essere informata preventivamente. Il titolare del trattamento informa in modo adeguato la persona interessata in merito alla raccolta dei suoi dati personali.
3	Secondo la LPD, ogni persona può richiedere al titolare del trattamento informazioni sull'eventuale trattamento di dati personali che la riguardano.
4	Il titolare del trattamento è tenuto ad adottare misure tecniche e organizzative atte a garantire che il trattamento dei dati sia conforme alle norme in materia di protezione dei dati.
5	Il titolare e il responsabile del trattamento sono tenuti a garantire un livello di sicurezza dei dati commisurato ai rischi.

Novità essenziali

6	La tenuta di un registro delle attività di trattamento dei dati a determinate condizioni. Il Consiglio federale prevede eccezioni per le aziende con meno di 250 dipendenti e il cui trattamento dei dati comporti un basso rischio di violazioni della personalità delle persone interessate.
7	Lo svolgimento di una valutazione d'impatto sulla protezione dei dati laddove sia previsto un trattamento che possa presumibilmente comportare un rischio elevato per i diritti fondamentali o della personalità della persona interessata. Tale valutazione d'impatto va eseguita solo se i trattamenti di dati effettuati in precedenza vengono modificati dopo il 1° settembre 2023.
8	Obblighi di notifica in caso di violazioni della sicurezza dei dati.
9	Inasprimento delle disposizioni penali: per i privati, la nuova Legge sulla protezione dei dati prevede multe fino a CHF 250'000.-. Sono punibili le azioni intenzionali e le omissioni, ma non la condotta negligente. Reati perseguibili a querela di parte!

Nella misura in cui, fino ad ora, abbiate già attuato nella prassi i requisiti in materia di protezione dei dati, con ogni probabilità siete tutelati da questo punto di vista. In tal caso saranno necessari solo adeguamenti sulla base delle novità essenziali.

Terminologia

Nuovi importanti termini della LPD

Definizioni dei termini

Titolare del trattamento
- Decide in merito agli scopi del trattamento dei dati e ai mezzi per attuarlo

Responsabile del trattamento
- Tratta i dati personali su incarico del titolare del trattamento

Dati personali degni di particolare protezione
- tra l'altro i dati sanitari, ora anche i dati genetici e i dati biometrici

Violazione della sicurezza dei dati
- Perdita, cancellazione, distruzione o alterazione di dati personali, accidentale o illecita, oppure divulgazione dei dati o dati resi accessibili a persone non autorizzate

Consenso

Elemento fondamentale: l’autodeterminazione informativa

Consenso

- Laddove sussistano condizioni legali quadro – come ad esempio nell'assicurazione per l'invalidità o contro gli infortuni –, non è necessario un consenso esplicito in quanto la firma – ad esempio sul modulo di iscrizione all'AI – comporta automaticamente la legittimazione.

- La situazione è diversa nel diritto privato (ad es. contratto di cura) e nel diritto privato delle assicurazioni. In questi casi è necessaria una dichiarazione di esonero o di consenso.

Consenso

- Per il trattamento di dati personali degni di particolare protezione, è necessario l'espresso consenso – orale o scritto – del paziente. Tuttavia, ciò è già previsto dall'attuale Legge sulla protezione dei dati.

Consenso

- Il consenso deve inoltre essere inequivocabile e dalla dichiarazione della persona interessata deve emergere chiaramente la sua volontà.
- Secondo il principio di proporzionalità, il consenso deve essere tanto più inequivocabile quanto più sensibili sono i dati personali in questione.
- In linea di principio il consenso può essere fornito in modo informale e non necessita della forma scritta.

Disposizioni penali

Disposizioni penali (1)

Osservazioni preliminari

La principale disposizione penale riguarda

→ il segreto professionale; l'obbligo del segreto medico (art. 321 CP)

Un confronto errato:

→ nel RGPD della UE le autorità per la protezione dei dati hanno a disposizione ampie opzioni sanzionatorie («multe»). La Svizzera ha invece solo poche disposizioni penali (alcune disposizioni penali erano già presenti nella Legge sulla protezione dei dati attuale). Tuttavia non esistono praticamente condanne sulla base di tali disposizioni).

Disposizioni penali (2)

Presupposti per la punibilità

Fattispecie oggettive

- Violazione degli obblighi di informare, di concedere l'accesso e di collaborare (art. 60 LPD)
- Violazione degli obblighi di diligenza (art. 61 LPD)
- Violazione dell'obbligo del segreto (art. 62 LPD)
- Inosservanza di decisioni (art. 63 LPD)

Fattispecie soggettive

- Dolo (atto compiuto «consapevolmente e volontariamente»)

Querela (eccetto art. 63 LPD)

- entro tre mesi dal momento in cui si viene a conoscenza

Pena prevista

- Multa (max. CHF 250 000) → contravvenzione

Perseguimento penale

- Cantoni

Trattamento dei dati su incarico (affidamento a un responsabile esterno)

Accordo per un trattamento di dati su incarico - Accordo sulla riservatezza

Trattamento dei dati su incarico (affidamento a un responsabile esterno)

Responsabilità

Trattamento da parte di un responsabile
→ ad es. esternalizzazione dell'informatica

La responsabilità della protezione dei dati rimane in capo al *titolare del trattamento*!

- Scelta, istruzione e sorveglianza del responsabile del trattamento incaricato
- Istruzioni al responsabile in relazione al trattamento dei dati
- Il responsabile del trattamento deve essere in grado di garantire la sicurezza dei dati

→**Accordo per un trattamento di dati su incarico**

Comunicazione dei dati
→ ad es. tecnico ortopedico

La responsabilità ai sensi della Legge sulla protezione passa al tecnico ortopedico.

- Il titolare, originariamente responsabile, resta responsabile per la trasmissione sicura dei dati.
- Nella misura in cui il destinatario non sia soggetto al segreto professionale, deve garantire un'adeguata riservatezza.

→ **Accordo sulla riservatezza**

Aspetti giuridici concernenti la responsabilità

Aspetti giuridici concernenti la responsabilità

- Nell’ambito del contratto di cura, il medico è responsabile di qualsiasi violazione dell’obbligo di diligenza.
- Bisogna pertanto basarsi su un’applicazione specifica per la professione dell’obbligo di diligenza per ogni singola azione.
- La diligenza richiesta nell’adempimento del contratto si riferisce alla scelta (cura in eligendo), alle istruzioni (cura in instruendo) e alla sorveglianza (cura in custodiendo).

Aspetti giuridici concernenti la responsabilità

- L’obbligo di diligenza del medico comprende l’equipaggiamento del personale ausiliario con materiale e strumenti idonei, nonché l’organizzazione accurata e appropriata dei processi di lavoro e dell’azienda.

- Per evitare i cosiddetti danni a terzi il medico, se necessario, deve effettuare un controllo finale dei processi di lavoro.

- La prova libera di esonero dalla responsabilità si ha quando si dimostra di aver adottato tutta la diligenza richiesta dalle circostanze per prevenire danni di questo tipo o che il danno si sarebbe comunque verificato anche se fosse stata adottata tale diligenza.

Aspetti giuridici concernenti la responsabilità

Esempi

- Assenza di informazione e conseguente assenza di consenso.
- Gli elenchi di dati richiesti dalla legge devono essere aggiornati e completi.
- In uno studio medico, le competenze e i processi devono essere organizzati.
- La formazione e l’addestramento del personale devono essere garantiti.
- Il soggetto responsabile è la persona responsabile della violazione della Legge sulla protezione dei dati. Secondo il messaggio sulla Legge sulla protezione dei dati rivista, non ci si basa sui responsabili dell'azione, bensì sui responsabili dell’organizzazione.

Tre importanti novità

Registro delle attività di trattamento dei dati
Notifica di violazioni della sicurezza dei dati
Valutazione d’impatto sulla protezione dei dati

Registro delle attività di trattamento dei dati

Documentazione dei processi di trattamento dei dati
→ grande quantità di dati personali degni di particolare protezione (ad es. dati sanitari): nessuna eccezione

Contenuto («informazioni minime»):

- l'identità del titolare del trattamento;
- le finalità del trattamento;
- una descrizione delle categorie di persone interessate e delle categorie di dati personali trattati;
- le categorie di destinatari;
- se possibile, la durata del periodo di conservazione dei dati personali o i criteri per la determinazione di tale durata;
- se possibile, una descrizione generale delle misure adottate per garantire la sicurezza dei dati;
- se i dati vengono inviati all'estero, l'indicazione della nazione e delle relative garanzie.

→ Modello di elenco delle attività di trattamento dei dati

Notifica di violazioni della sicurezza dei dati

Obbligo di notifica in caso di «rischio elevato»

- Ad es. perdita di dati sanitari o accesso non autorizzato

Notifica all'Incaricato federale della protezione dei dati e della trasparenza (IFPDT)
- Notifica online: https://databreach.edoeb.admin.ch/report

Eventuali informazioni alle persone interessate (→ se necessarie per la loro protezione)

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

Valutazione d’impatto sulla protezione dei dati

In caso di nuovi trattamenti di dati
(per i trattamenti di dati già in atto: ulteriori categorie di dati/ulteriori finalità)

Elevato rischio per la personalità o i diritti fondamentali delle persone interessate

- Utilizzo di nuove tecnologie
- Vasto trattamento di dati personali degni di particolare protezione

→ Valutazione dei rischi (e pianificazione di misure tecniche e organizzative adeguate)

Consultazione preventiva dell’IFPDT (art. 23 LPD)

- Elevato rischio nonostante le misure previste
- Nessuna consultazione preventiva se c’è un/una consulente per la protezione dei dati

Termini di conservazione/cancellazione

I dati personali devono essere distrutti o resi anonimi

- Non appena non sono più necessari per le finalità del trattamento

Durata del periodo di conservazione o criteri

- Disposizioni di legge

→ Guida per la conservazione e l'archiviazione

Protezione e sicurezza dei dati

Misure tecniche e organizzative

Sicurezza dei dati

Art. 8 Sicurezza dei dati

[1] Il titolare e il responsabile del trattamento garantiscono, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio.

[2] I provvedimenti devono permettere di evitare violazioni della sicurezza dei dati.

[3] Il Consiglio federale emana disposizioni sui requisiti minimi in materia di sicurezza dei dati.

Sicurezza dei dati

Protezione dei dati sin dalla progettazione

Art. 7 Protezione dei dati personali sin dalla progettazione e per impostazione predefinita

[1] Il titolare del trattamento è tenuto ad adottare i provvedimenti tecnici e organizzativi necessari affinché il trattamento dei dati personali sia conforme alle disposizioni sulla protezione dei dati, in particolare ai principi di cui all'articolo 6. Li adotta sin dalla progettazione.

Sicurezza dei dati

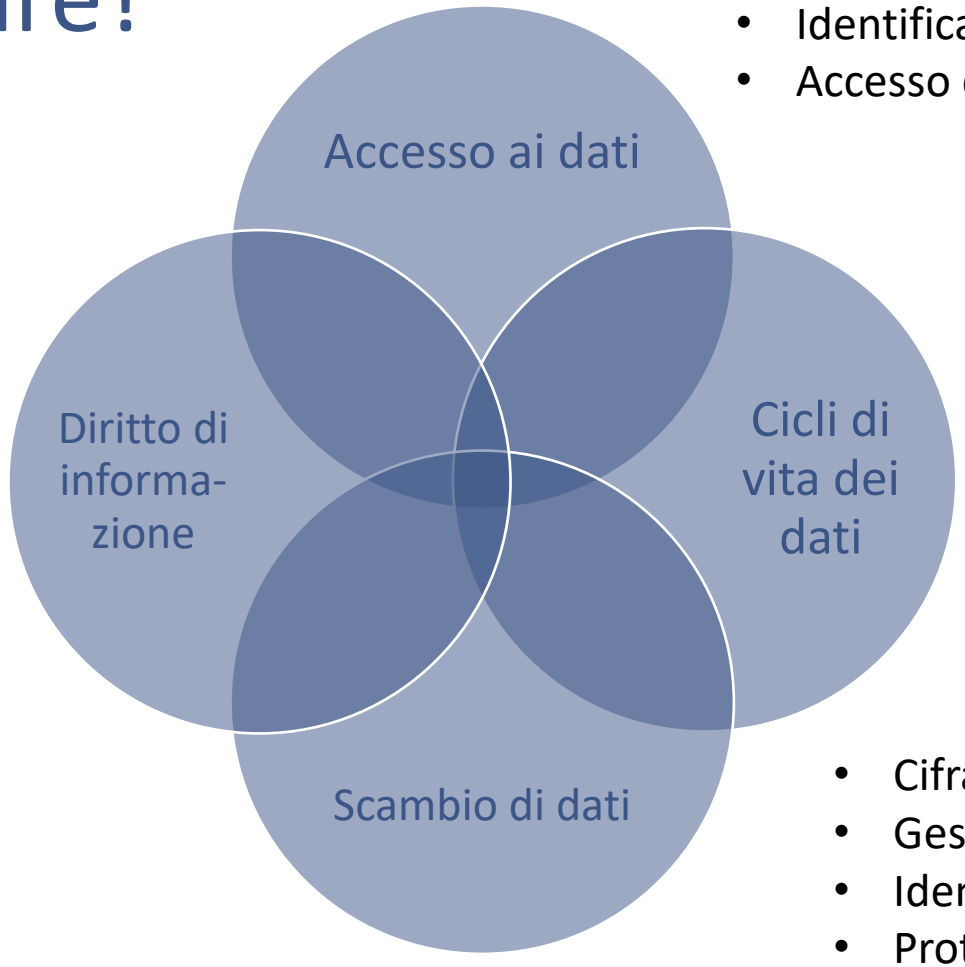
L’art. 7 cpv. 1 stabilisce l’obbligo di diligenza per il titolare del trattamento.
L’art. 8 cpv. 1 assoggetta all’obbligo entrambi, il titolare del trattamento e il responsabile!

«Il titolare del trattamento deve garantire attivamente che il responsabile del trattamento rispetti la legge in misura uguale a lui.»

«Deve pertanto scegliere con cura il responsabile del trattamento, istruirlo in modo adeguato e sorvegliarlo nella misura del necessario.»

Da dove iniziare?

- Sicurezza dei locali, delle sale server e
- delle postazioni di lavoro
- Identificazione e autenticazione
- Accesso dentro e fuori dallo studio medico



- Registrazione e protocollazione
- Anonimizzazione
- Cifratura
- Messa in sicurezza dei dati
- Trattamento dei dati su incarico (ad es.
- Classificazione dei dati

- Processo per le richieste di informazioni
- Cancellazione dei dati
- Protocollazione

- Cifratura del trasporto e del contenuto
- Gestione delle chiavi
- Identità elettronica
- Protocollazione

Raccomandazioni

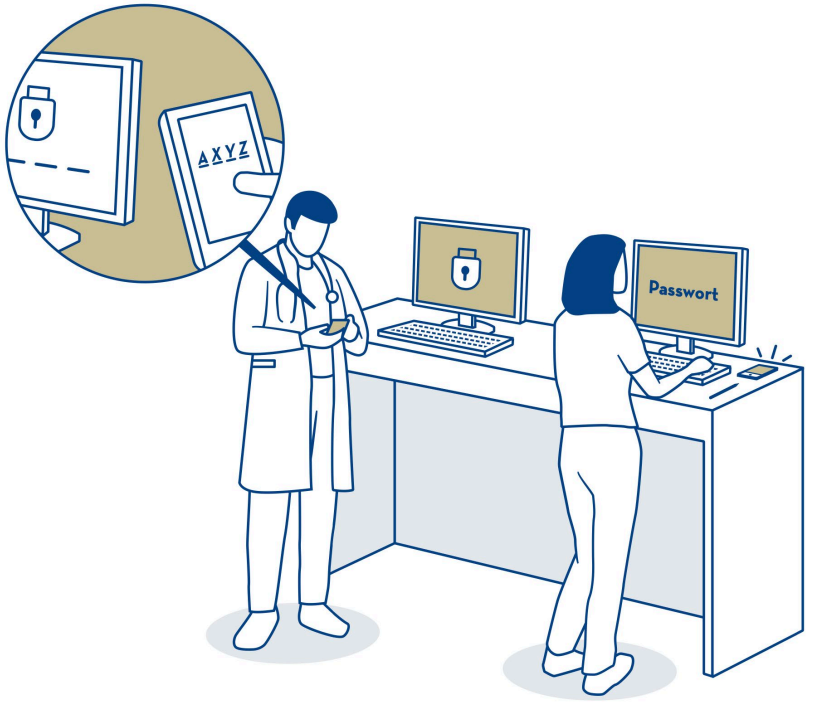
Raccomandazioni dell'IFPDT

Requisiti tecnici e organizzativi per i servizi basati su cloud

Requisiti minimi per la protezione dei sistemi informatici

Esempio: «Regolamentazione della protezione degli accessi»

L’amministrazione centralizzata e l’assegnazione strutturata dei diritti di accesso e di utilizzo, ad esempio mediante Active Directory o servizi di directory alternativi, riduce al minimo i rischi di accessi non autorizzati a dati sensibili da parte di soggetti interni o esterni. L’aggiornamento regolare dei diritti di accesso e di utilizzo consente di rilevare e registrare le entrate e le uscite di collaboratori.

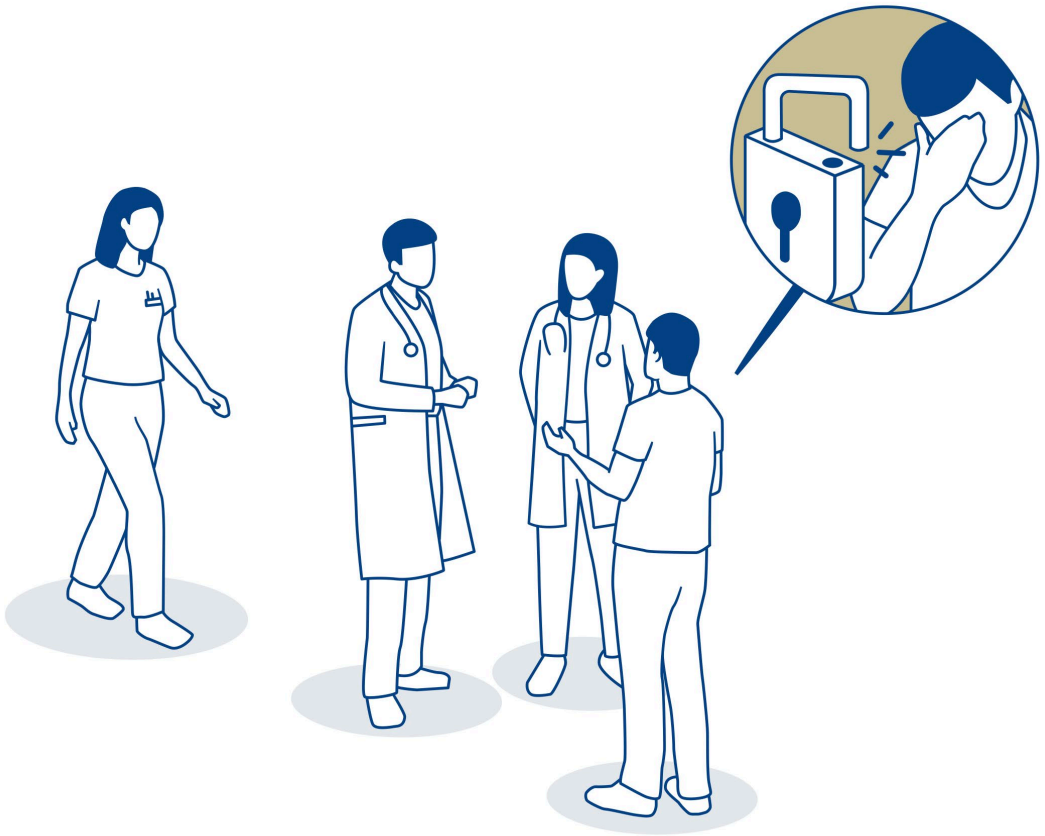


Misure

- Account utente personali per i collaboratori
- Limitazione dei diritti degli utenti (principio del «Need to know
- Accesso alla rete interna dello studio medico con autenticazione forte preventiva
- Cambio della password

Esempio «Sensibilizzare il personale riguardo alla sicurezza dei dati»

I collaboratori di uno studio medico rappresentano un obiettivo apprezzato dagli hacker criminali, i quali spesso cercano di accedere all'ambiente ICT e ai dati mediante attacchi di social engineering. Per impedirlo, è di fondamentale importanza sensibilizzare i responsabili e i collaboratori dello studio medico.

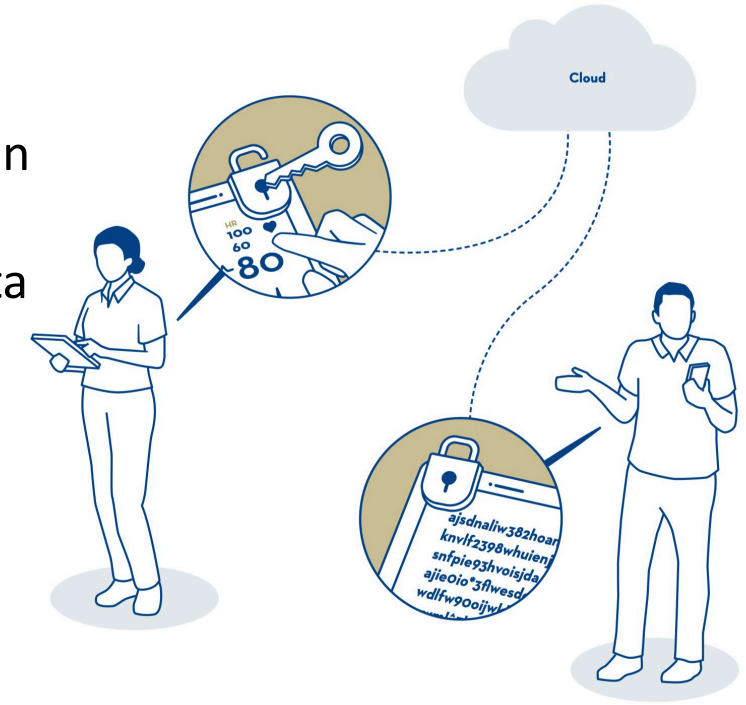


Misure

- Affrontare queste tematiche nelle riunioni (password, classificazione dei dati, gestione delle risorse ICT, trattamento e scambio dei dati, procedure in caso di incidenti relativi alla sicurezza)
- Addestrare i nuovi collaboratori, schede informative
- Utilizzo delle risorse ICT per scopi privati
- …

Esempio «Cifratura e gestione delle chiavi (cloud)»

I dati salvati (Data at Rest) e quelli trasmessi (Data in Transit) devono essere protetti mediante processi crittografici. Allo stesso modo, la comunicazione tramite tutte le connessioni in entrata e in uscita, da e verso l'infrastruttura cloud, ivi incluse le interfacce all'interno dell'infrastruttura cloud, deve essere criptata e soggetta ad autenticazione.



Misure

- Cifratura dei dati salvati in tutti i cicli di vita
- Gestione delle chiavi (gestione efficace del ripristino)
- Cifratura durante il trasporto

Definizione delle responsabilità ed emissione di linee guida

Il titolare del trattamento emette linee guida e definisce processi e controlli interni per la convalida, tra l'altro riguardo a:

- controlli degli accessi;
- inserimento, salvataggio e cancellazione di dati;
- rispetto dei requisiti normativi;
- gestione dei rischi;
- altro

In caso di esternalizzazione del trattamento dei dati nel cloud, la governance resta sempre in capo allo studio medico. La governance non può essere esternalizzata, nemmeno in caso di ricorso a fornitori esterni.

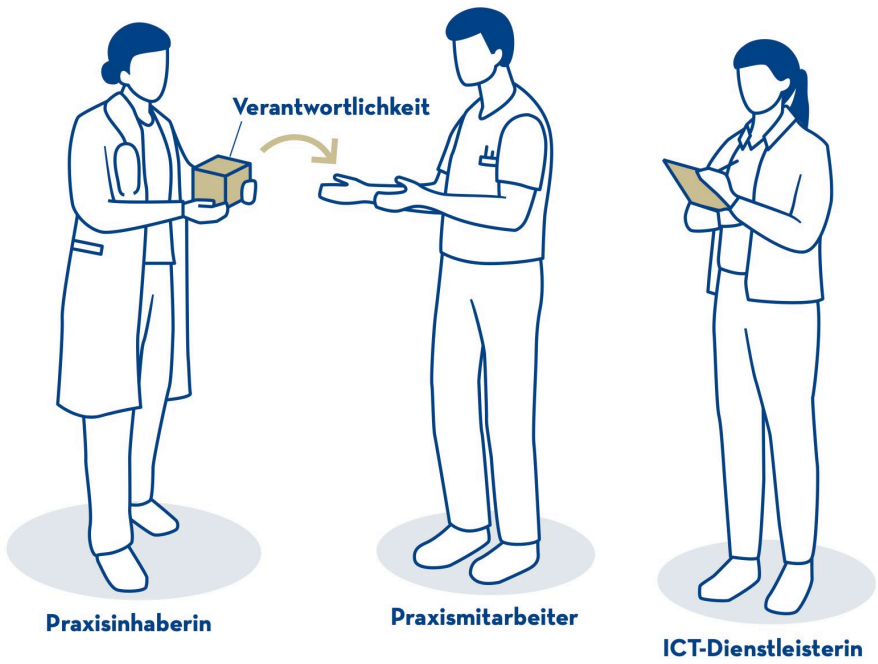


Tavola rotonda

Tavola rotonda

Selezione di domande

Conclusione

Conclusione

- Il webinar sarà registrato: una mail a tutti i partecipanti con link alla registrazione del webinar seguirà la settimana prossima
- Le diapositive della presentazione in italiano, francese e tedesco saranno disponibili in un secondo tempo (informazioni sempre per e-mail)

Grazie per l’attenzione

FMH · Federazione dei medici svizzeri · Verbindung der Schweizer Ärztinnen und Ärzte
Casella postale · CH-3000 Berna 16 · Telefono +41 31 359 11 11
info@fmh.ch · www.fmh.ch