1 Spiegazioni sull'esecuzione della DPIA

1.1 Svolgimento della DPIA

1.1.1 Descrizione sistematica delle procedure di trattamento dei dati

In primo luogo, è necessario predisporre una descrizione sistematica delle procedure di trattamento dei dati rilevanti. Laddove la stessa sia già stata presentata nel quadro della definizione dei valori soglia, è possibile farvi riferimento.

Occorre altresì valutare la necessità e la proporzionalità del trattamento dei dati. Al riguardo, si pone la domanda se la finalità del trattamento dei dati non possa essere raggiunta con dei mezzi meno impattanti (ad es. minimizzando i dati o scartando quelli più sensibili).

Le misure di sicurezza attuate devono essere debitamente descritte.

1.1.2 Valutazione del rischio

Il contesto della valutazione del rischio deve definire i rischi a cui va incontro la persona interessata. La gestione del rischio prevede il seguente iter documentato:

- attribuire al rischio un livello in base al quale classificare sia l'impatto che le probabilità di accadimento;
- delineare le misure correttive attuate per minimizzare o eliminare il rischio;
- valutare il rischio ancora una volta alla luce delle misure correttive adottate;
- all'occorrenza consultare l'IFPDT.

1.2 Spiegazioni sulla valutazione del rischio

1.2.1 Identificazione e classificazione dei rischi

L'identificazione dei rischi avviene sulla base dei possibili rischi individuati nella definizione dei valori soglia.

La valutazione è finalizzata a determinare la probabilità di accadimento del rischio, nonché l'impatto che la sua concretizzazione può avere per la persona interessata.

L'impatto e la probabilità di accadimento devono essere classificati secondo i livelli BASSO, MODERATO o ELEVATO, a loro volta corrispondenti alle seguenti categorie descrittive:

	Livello di impatto	Probabilità di accadimento
Basso	La persona interessata può subire dei disagi che, tuttavia, riesce a superare con poche difficoltà.	Stando alla fonte del rischio è alquanto inverosimile che la vulnerabilità possa essere sfruttata in modo tale da costituire una minaccia.
Moderato	La persona interessata può subire dei disagi anche notevoli che riesce a superare con alcune difficoltà.	Stando alla fonte del rischio è poco probabile che la vulnerabilità possa essere sfruttata in modo tale da costituire una minaccia.
Elevato	La persona interessata può subire delle conseguenze irrevocabili o comunque dei disagi talmente importanti da riuscire a superarli solo con estrema difficoltà.	Stando alla fonte del rischio è probabile o persino facile che la vulnerabilità possa essere sfruttata in modo tale da costituire una minaccia.

In linea di massima, l'accadimento di un rischio può avere un impatto fisico, materiale e/o morale sulla persona interessata.1

La seguente tabella di classificazione offre un esempio di come quantificare il livello d'impatto di un rischio:

	Basso	Moderato	Elevato
Esempi di impatto materiale	Pubblicità mirata per i normali beni di consumo	Obblighi di pagamento imprevisti	Debiti importanti
Esempi di impatto morale	Leggero disappunto Sensazione di violazione della sfera privata in assenza di danno reale o oggettivo	Violazione della sfera privata senza danni permanenti	Sensazione di violazione della sfera privata con danni irreversibili Sensazione di vulnerabilità dopo un invito a comparire in tribunale

La scala della probabilità di accadimento del rischio deve inoltre prevedere i livelli di ipotesi e le categorie descrittive seguenti:

	Probabilità di accadimento
Basso	Stando alle conoscenze attuali, l'evento potrebbe verificarsi al massimo ogni dieci anni
Moderato	L'evento si verifica da un minimo di una volta ogni cinque anni a un massimo di una volta all'anno
Elevato	L'evento si verifica da un minimo di una volta all'anno a un massimo di una volta al mese

1.2.2 Analisi del livello di rischio

Dopo la classificazione del rischio e della probabilità di accadimento, la seguente matrice consente di effettuare una stima del livello di rischio:

[1] Cfr. l'allegato al documento «Risk Assessment & Datenschutz-Folgenabschätzung» di Bitkom, p. 50 ss.

Impatto dal punto di vista della persona interessata	Elevato	Lieve	Moderato	Elevato
	Moderato	Lieve	Moderato	Moderato
	Basso	Lieve	Lieve	Lieve
		Basso	Moderato	Elevato
		Probabilità di accadimento		

Categoria	Descrizione
Verde (lieve)	Non occorre intervenire in tempi rapidi. Definire le misure preventive in virtù dei costi e dello stato dell'arte.
Giallo (moderato)	Necessità di intervento di seconda priorità. Le misure preventive devono essere definite.
Rosso (elevato)	Rischio intollerabile per la persona interessata e/o l'azienda. Necessità di intervento di prima priorità. Le misure preventive devono essere definite (ad es. il piano di emergenza).

1.2.3 Misure correttive

Se il livello di rischio è ELEVATO, occorre predisporre delle misure correttive per minimizzarlo e, se possibile, eliminarlo. Le misure correttive possono essere di natura organizzativa o tecnica.

Laddove possibile, è consentito fare riferimento alla misure tecniche e organizzative (TOM) già documentate o ad altro materiale aggiuntivo.

1.2.4 Nuova valutazione del rischio

In virtù delle misure correttive adottate è possibile stabilire un nuovo livello di rischio.

1.3 Consultazione dell'IFPDT

Qualora dalla nuova valutazione del rischio ai sensi del punto 1.2.4 risulti che, nonostante l'adozione di misure correttive, il rischio per la persona interessata continua a essere elevato (cfr. matrice di rischio) e che non esistono ulteriori misure idonee a minimizzarlo, occorre consultare l'IFPDT per ottenere un parere in merito.

Le eventuali ulteriori misure correttive proposte dall'IFPDT devono essere attuate.

2 Descrizione e valutazione delle procedure di trattamento dei dati

2.1 Descrizione sistematica

[inserire qui la descrizione]

Registrazione di dati personali e dati sanitari (dati personali degni di particolare protezione) nella gestione dell'anamnesi della/del paziente. In particolare, si rilevano le procedure terapeutiche, le diagnosi mediche, i dati di contatto della/del paziente (cognome, nome, indirizzo) e altri dati relativi alla persona (data di nascita).

2.2 Valutazione della necessità e della proporzionalità

[inserire qui la valutazione]

In base ai dati forniti in primo luogo dal medico prescrittore possiamo intanto predisporre la terapia più adatta alla/al paziente. La gestione della cartella pazienti è necessaria ai fini di ottemperare agli obblighi legali.

Sono raccolti soltanto i dati sanitari indispensabili al trattamento.

3 Valutazione del rischio

Si prega di compilare la seguente valutazione del rischio (colonna destra).

Rischio 1

Valutazione	
Descrizione del rischio	**Virus o attacco hacker** Perdita dei dati
Probabilità di accadimento	**Bassa** I sistemi sono protetti da un antivirus e da Firewall.
Impatto	**Bassa** La/il paziente può non gradire la divulgazione pubblica del proprio quadro clinico causata da un attacco hacker. Tuttavia, visto che non si trattano dei quadri clinici stigmatizzanti, i disagi sono contenuti.
Livello di rischio	Lieve
Misure correttive	
Descrizione della misura	-
Documentazione della misura	-
Nuova valutazione del rischio	
Probabilità di accadimento (in considerazione delle misure correttive)	-
Impatto (in considerazione delle misure correttive)	-
Livello di rischio (in considerazione delle misure correttive)	-
Occorre consultare l'IFPDT?	No

Rischio 2

Valutazione	
Descrizione del rischio	**Perdita dei dati per interruzione dell'IT e/o backup** La perdita dei dati influisce sull'attività operativa. Tuttavia, i dati possono essere in parte recuperati rivolgendosi alla persona interessata o al medico prescrittore.
Probabilità di accadimento	**Bassa** L'infrastruttura risulta protetta da misure tecniche.
Impatto	**Basso** A parte dover nuovamente indicare i dati, la persona interessata non subisce alcun impatto.
Livello di rischio	LIEVE
Misure correttive	
Descrizione della misura	-
Documentazione della misura	-
Nuova valutazione del rischio	
Probabilità di accadimento (in considerazione delle misure correttive)	-
Impatto (in considerazione delle misure correttive)	-
Livello di rischio (in considerazione delle misure correttive)	-
Occorre consultare l'IFPDT?	No

Rischio 3

Valutazione	
Descrizione del rischio	**Trattamento di dati falsi**
Probabilità di accadimento	**Lieve** I dati delle/dei pazienti sono assegnati alla relativa cartella pazienti e conservati separatamente sia in modo fisico che digitale.
Impatto	**Elevato** Il trattamento di dati falsi può essere la causa di una prescrizione di terapia errata, con conseguenti danni per la salute della/del paziente.
Livello di rischio	*Lieve*
Misure correttive	
Descrizione della misura	-
Documentazione della misura	-
Nuova valutazione del rischio	
Probabilità di accadimento (in considerazione delle misure correttive)	-
Impatto (in considerazione delle misure correttive)	-
Livello di rischio (in considerazione delle misure correttive)	-
Occorre consultare l'IFPDT?	**No**

Rischio 4

Valutazione	
Descrizione del rischio	**Violazione della protezione dei dati da parte di un partner in outsourcing** Comunicazione a terzi non autorizzati e modificazione dei dati da parte dei dipendenti di un partner in outsourcing.
Probabilità di accadimento	**Lieve** Gli accessi sono limitati allo stretto necessario. I partner in outsourcing e i loro dipendenti sono vincolati ad accordi sul trattamento dei dati e a dichiarazioni di riservatezza, in base ai quali sono tenuti a trattare i dati conformemente a quanto prescritto in materia di protezione dei dati e esclusivamente nel rispetto delle finalità da noi prestabilite.
Impatto	**Lieve** L'impatto della violazione sulla personalità del singolo è lieve in quanto il trattamento di malattie stigmatizzanti è ridotto.
Livello di rischio	*Lieve*
Misure correttive	
Descrizione della misura	-
Documentazione della misura	-
Nuova valutazione del rischio	
Probabilità di accadimento (in considerazione delle misure correttive)	-
Impatto (in considerazione delle misure correttive)	-
Livello di rischio (in considerazione delle misure correttive)	-

Occorre consultare l'IFPDT?	**No**

Titolare del trattamento dei dati: _____

Data: _____

Firma: _____

***Nota**: La presente valutazione d'impatto sulla protezione dei dati si basa sull'esempio di una DPIA relativa alla videosorveglianza eseguita da privacyofficers.at (Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter), nonché sulla guida «Risk Assessment & Datenschutz-Folgenabschätzung» di Bitkom (associazione registrata). Il documento è da intendersi quale supporto accuratamente predisposto e reso disponibile da IT & Law Consulting GmbH in base al testo definitivo della revisione della legge sulla protezione dei dati e al corrispondente messaggio. In considerazione della letteratura e della giurisprudenza attuali possono esservi delle deviazioni che richiedono di modificare la lista di controllo. L'azienda che utilizza questo modello è individualmente responsabile dell'ottemperanza alle disposizioni di legge.*