Azienda Provinciale per i Servizi Sanitari
Provincia Autonoma di Trento

Valutazione di impatto sulla protezione dei dati personali

(estratto)

relativa al trattamento

"TreC Mamma - Progetto 1000 giorni" - ricerca interventi comportamentali digitali

redatta ai sensi dell'art. 35 del Reg. UE 679/2016 (GDPR)
e sulla base delle Linee Guida del 4/10/2017 del Working Party Art. 29

1. Sommario

2. Obiettivo e organizzazione del documento

Il presente documento, redatto ai sensi dell'art. 35 del Reg. UE 2016/679 ("GDPR") e sulla base delle Linee Guida del 4 ottobre 2017 del Working Party Art. 29, ha lo scopo di valutare l'impatto sui diritti e le libertà delle persone fisiche con riferimento al trattamento dei dati effettuato nell'ambito del trattamento analizzato.

Ai sensi dell'art. 35 del GDPR la valutazione di impatto (o "DPIA") deve essere effettuata quando un'attività di trattamento di dati personali è in grado di determinare un rischio elevato per i diritti e le libertà delle persone fisiche alle quali i dati si riferiscono (interessati).

La Valutazione di Impatto deve essere effettuata **prima** di mettere in atto il trattamento dei dati personali ([1]), coerentemente con il principio di privacy by design e privacy by default ([2]) per individuare la necessità di implementare misure di sicurezza ulteriori rispetto a quelle già in atto e finalizzate a mitigare i rischi.

Nel valutare l'impatto del trattamento effettuato dai titolari o responsabili, sono tenute in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'art. 40 del GDPR e le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, raccolte laddove possibile.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Nel rispetto dei principi di cui all'art. 35 GDPR e Linee guida applicabili, la presente valutazione d'impatto è elaborata seguendo gli step sotto riportati.

1. Definizione del contesto in cui avviene l'attività di trattamento
2. Descrizione sistematica dell'attività di trattamento, con particolare attenzione al flusso dei dati
3. Indicazione delle modalità di rispetto dei principi applicabili al trattamento dei dati personali ([3])
4. Indicazione delle modalità di gestione dei diritti degli interessati ([4])
5. Indicazione del rispetto degli adempimenti relativi ai responsabili del trattamento ([5]) e degli autorizzati al trattamento ([6])

[1] Considerando 90 e 93, art. 35, parr. 2 e 10, GDPR.

[2] Considerando 78, art. 25 GDPR.

[3] Art. 5 GDPR.

[4] Artt. 15-22 GDPR.

6. Definizione dei meccanismi dell'eventuale trasferimento dei dati in Paesi extra UE ([7]);
7. Calcolo del rischio relativo al trattamento
8. Indicazione delle minacce a cui è esposta l'attività di trattamento, calcolo del rischio inerente (probabilità e impatto), indicazione delle misure in atto, calcolo del rischio residuo, individuazione delle eventuali contromisure di mitigazione, valutazione dell'accettabilità del rischio residuo per verificare se mettere in atto il trattamento o ricorrere allo strumento della consultazione preventiva al Garante per la protezione dei dati personali ([8]).

La metodologia seguita per la redazione della DPIA soddisfa gli standard richiesti dal GDPR in quanto conforme ai criteri previsti dall' "Allegato 2 – Criteri per una DPIA ammissibile" alle Linee guida sulla Valutazione d'Impatto nella protezione dei dati (DPIA) e stabilire se il trattamento "può comportare un rischio elevato" ai sensi del regolamento 2016/679 (WP 248 rev.01).

[5] Art. 28 GDPR

[6] Art. 29 GDPR e art. 2-*quaterdecies* D. Lgs. 196/2003 (Codice Privacy).

[7] Capo V GDPR.

[8] Art. 36 GDPR.

3. Definizione del contesto.

In questa sezione è analizzata nel dettaglio e sotto diversi punti di vista l'attività di trattamento da sottoporre a valutazione.

Il presente documento ha l'obiettivo di descrivere i risultati della valutazione d'impatto con riferimento al Progetto "TreC Mamma - Progetto 1000 giorni" nella sua componente relativa alle sperimentazioni di ricerca inerenti alla realizzazione di interventi comportamentali digitali per la promozione del benessere.

Il Progetto è effettuato in contitolarità dall'Azienda Provinciale per i Servizi Sanitari di Trento (di seguito "APSS")" e dalla Fondazione Bruno Kessler (di seguito "FBK") in un contesto di sanità pubblica e di innovazione del servizio sanitario locale, per la promozione della salute e la prevenzione primaria e secondaria e per lo svolgimento di attività di ricerca, approvato tramite accordo di collaborazione sottoscritto dalle Parti in data 28/11/2024 (Protocollo: APSS.28/11/2024.0214970).
Il progetto consiste nella realizzazione e validazione di un ecosistema di interventi di sanità digitale per accompagnare e supportare la donna, il bambino e la famiglia nei primi 1000 giorni di vita, da erogare tramite l'app TreC Mamma.
Le attività di ricerca prevedono il coinvolgimento dei professionisti sanitari di APSS, dei ricercatori di FBK e delle donne e famiglie attraverso il "patto con il cittadino".
Il presente progetto rappresenta un progetto bandiera del Centro di Competenza Trentino Salute S4.0, nello specifico del Centro Digital Health&Wellbeing di FBK per gli aspetti di ricerca in AI definito e concordato con APSS e approvato dal Comitato Esecutivo di TS4.0.

Il Progetto ricomprende diverse progettualità con differenti obiettivi e finalità, ma con simili scenari. Ai sensi dell'art. 35 del GDPR "una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi". I fattori di rischio possono essere così sintetizzati: i trattamenti concernono dati particolari relativi a soggetti assistiti dal Servizio Sanitario Provinciale; i trattamenti di dati relativi alla salute comportano dei rischi per gli interessati in quanto soggetti vulnerabili.

Il presente documento si applica per le attività inerenti la ricerca sia ad APSS che ad FBK in qualità di Contitolari del trattamento.

Le attività di ricerca sono svolte con l'ausilio della app TreC Mamma e prevedono la raccolta di dati comuni, categorie particolari di dati personali (es. dati relativi alla salute, dati idonei a rivelare l'origine razziale o etnica), dati da device (wearable, dispositivi indossabili).
APSS e FBK collaborano nella realizzazione e definizione dei contenuti erogati e delle funzionalità utili per la ricerca. FBK fornisce inoltre supporto nell'area di data analytics, di design, implementazione delle soluzioni di digital health concordate e valutazione degli interventi.

L'utilizzo di TreC mamma per lo sviluppo di attività di ricerca possono riguardare:

- raccolta di dati in forma aggregata per finalità epidemiologiche, socio-economiche ed organizzative, anche volte a misurare il gradimento e la soddisfazione dei servizi forniti dall'Azienda al fine di migliorare la qualità dell'assistenza erogata;
- progettazione, sviluppo, sperimentazione, validazione di applicazioni/soluzioni di e/mHealth e di modelli diagnostico-predittivi basati su tecniche di Intelligenza Artificiale, nello specifico si fa riferimento ai progetti già approvati dal Comitato Etico Territoriale della Provincia Autonoma di

Trento per le sperimentazioni cliniche (DEMETRA - Un coach virtuale per migliorare la dieta e l'attività fisica delle donne sovrappeso in gravidanza: studio pilota di fattibilità, REA - Un coach virtuale per promuovere il benessere psicologico e prevenire il disagio post partum nelle donne in gravidanza: studio pilota di fattibilità, MAIA - Un coach virtuale di accompagnamento alle donne in gravidanza per promuovere il benessere psicologico: studio pilota di fattibilità, ALBA - Un coach virtuale per promuovere il benessere psicologico e prevenire lo stress nelle donne in gravidanza: studio pilota di fattibilità, Intervento educativo e motivazionale sugli stili di vita di bambini a rischio sovrappeso o con sovrappeso-obesità ai 24 mesi di età);

- progetti specifici in ambito socio-sanitario-assistenziale (nello specifico si fa riferimento al progetto già approvato dal Comitato Etico Territoriale della Provincia Autonoma di Trento per le sperimentazioni cliniche: Sviluppo di un modello predittivo per la predizione dell'insorgenza di emorragia nel post partum (EPP)).

I dati raccolti e utilizzati sono sia dati identificativi che particolari ai sensi dell'art. 9, par. 1, del GDPR, dati sensibili o dati aventi carattere estremamente personale, dati riguardanti soggetti interessati vulnerabili (pazienti) nonché trattamenti effettuati attraverso l'uso di tecnologie innovative (app, assistenti virtuali). Per queste ragioni appare necessario svolgere una valutazione di impatto dei trattamenti dei dati.

3.1 Elementi di fatto

L'Azienda Provinciale per i Servizi Sanitari (di seguito "APSS") è l'ente strumentale della Provincia Autonoma di Trento preposto alla gestione coordinata delle attività sanitarie e socio-sanitarie per l'intero territorio provinciale.

La presente DPIA valuta il trattamento dei dati personali nell'ambito del trattamento ***"TreC Mamma - Progetto 1000 giorni" - ricerca interventi comportamentali digitali***

In particolare, il trattamento di dati personali per ogni attività di ricerca svolta viene esplicitato nelle specifiche schede presenti al seguente punto 3.4.

3.2 Ruoli privacy

Sono di seguito riportati i riferimenti dei soggetti che rivestono dei ruoli privacy nell'ambito delle attività del trattamento.

a) Contitolari del trattamento

CONTITOLARI DEL TRATTAMENTO		
	CONTITOLARE 1	**CONTITOLARE 2**
RAGIONE SOCIALE	Azienda Provinciale per i Servizi Sanitari	Fondazione Bruno Kessler C.F. e P.IVA 02003000227
SEDE LEGALE	Via Degasperi 79 Trento	Via Santa Croce, n. 77 – Trento
INDIRIZZO MAIL	dirgen@apss.tn.it	privacy@fbk.eu
INDIRIZZO PEC	apss@pec.apss.tn.it	privacy@pec.fbk.eu
DPO	Avv. Silvia Stefanelli	dott.ssa Anna Benedetti

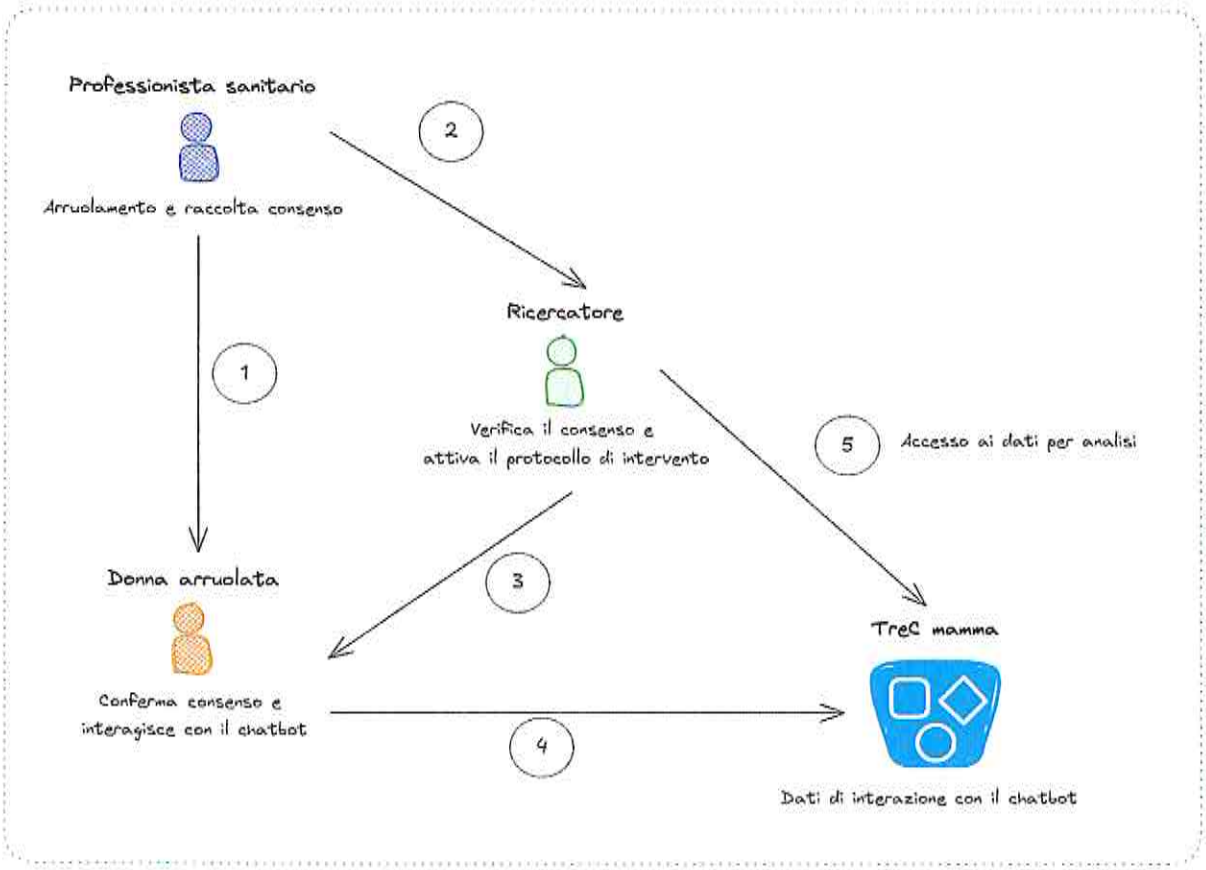
3.3 Descrizione generale dell'attività di trattamento

In questo paragrafo sono individuate le caratteristiche generali del trattamento.
Il trattamento di dati personali ha finalità di ricerca scientifica in ambito medico, attraverso la piattaforma prototipale TreC Mamma. Il consenso dell'interessata viene raccolto al momento del coinvolgimento e previa comunicazione dell'informativa. Sia il consenso che l'informativa sono somministrati in formato cartaceo dagli operatori di APSS. Oltre al consenso cartaceo, è prevista tramite la piattaforma la possibilità per l'utente di confermare la partecipazione allo studio selezionando le apposite spunte sulla piattaforma. L'informativa è sempre disponibile all'interno della piattaforma. Il consenso dell'interessata viene raccolto nelle stesse modalità di consegna dell'informativa, ossia in modalità cartacea per l'accettazione ad essere arruolata e per fornire i dati di contatto al ricercatore, così come il consenso ad essere ricontattata al termine dello studio, e in modalità digitale per acconsentire all'avvio dell'intervento di ricerca.

(Omissis)

4. Rappresentazione del ciclo di vita dei dati

Segue l'immagine che rappresenta il ciclo di vita dei dati, suddiviso in quattro fasi che comprendono le operazioni elencate nell'art. 4, 2 del GDPR e riguardano tutte le specifiche attività di trattamento elencate al precedente punto 3.4.



Il ciclo di vita del trattamento Dati prevede i seguenti passi:

RACCOLTA DEL DATO	- I dati relativi al consenso sono raccolti in forma cartacea al momento dell'arruolamento da parte dei professionisti sanitari (v. grafico punto 1) e successivamente confermati attraverso l'app TreC mamma a seguito dell'inserimento nella piattaforma da parte del

	ricercatore. (Di persona - v. grafico punto 2 e 3) - La raccolta dati relativa allo svolgimento dell'interazione prevista con l'assistente virtuale avviene tramite l'app TreC mamma. (Parte tecnologica - v. grafico punto 4) - A conclusione dello studio le interviste qualitative verranno audio-registrate dal ricercatore. (Di persona)
SALVATAGGIO/ARCHIVIAZIONE DEL DATO	I dati sono salvati nei database della piattaforma TreC Mamma all'interno dell'infrastruttura tecnologica di FBK e APSS; nessun dato viene condiviso con altri enti all'esterno di APSS e FBK.
ACCESSO AL DATO	Gli autorizzati al trattamento (ricercatori) possono accedere ai dati raccolti tramite cruscotto web previa autenticazione (v. grafico punto 5). Gli amministratori di sistema nominati da APSS e FBK possono accedere ai dati per operazioni di manutenzione e aggiornamento, creazione e gestione utenti. Il personale di sviluppo, appositamente incaricato da FBK, può avere accesso ai dati per operazioni di manutenzione del software.
ELABORAZIONE DEL DATO	L'analisi del dato viene effettuata dai ricercatori utilizzando software statistici.
CONSERVAZIONE DEL DATO	I Dati raccolti attraverso l'app TreC Mamma rimangono nei database e nei file di backup della piattaforma fino a conclusione del progetto. I Dati raccolti e gli output elaborati saranno conservati in FBK, secondo le normative, per 3 anni dalla chiusura del progetto per consentire la pubblicazione dei risultati. Alla conclusione del progetto di ricerca, i dati verranno sottoposti ad una procedura di anonimizzazione, ovvero verranno rimossi tutti gli elementi identificativi che possono far risalire all'identità dell'interessata.

(Omissis)

6. Tabelle di calcolo del rischio e valutazione dell'impatto sugli interessati.

In questa sezione del documento è dettagliata l'analisi del rischio del trattamento oggetto della valutazione d'impatto.

La definizione di rischio è la seguente:

il rischio è l'eventualità di subire un danno in conseguenza di un'azione compiuta o subita, e si calcola ricorrendo alla formula **R=P*I**, in cui **P** è la probabilità di accadimento delle minacce, e **I** è l'impatto o danno conseguente.[9]

Alla luce della definizione di cui sopra, l'analisi del rischio viene svolta nel seguente modo:

- prima vengono analizzate le minacce e la probabilità di accadimento delle minacce;
- poi viene analizzato **l'impatto** o danno conseguente in caso di accadimento;
- tenuto conto poi delle minacce e del possibile impatto, viene valutato il **rischio**.

Tale rischio è denominato **rischio inerente:** vale a dire il rischio connaturato nell'attività svolta dall'organizzazione prima dell'adozione di misure volte a contenerlo o controllarlo.
In sostanza, si opera una valutazione dei rischi intrinseci cui è esposta l'organizzazione senza che si operi un controllo sugli stessi[10].

Valutato il rischio inerente si andranno ad analizzare le misure di sicurezza implementate o che si reputa opportuno implementare per valutare il rischio residuo.
Il **rischio residuo** è il rischio che permane dopo aver implementato le misure di sicurezza sul rischio inerente[11].
Infine:

- Se il rischio residuo viene valutato come **accettabile**, potrà procedersi con l'attività di trattamento dei dati.
- Se il rischio residuo viene invece valutato come **non accettabile** (in quanto continui ad essere elevato nonostante le misure di sicurezza adottate), sarà necessario svolgere la Consultazione preventiva dinanzi l'Autorità Garante ai sensi dell'art. 36 GDPR.

---

[9] Guida ISO/IEC 73/2009, 3.6.1.8: il rischio può esser definito come la combinazione delle probabilità di un evento e delle sue conseguenze;

[10] Guida ISO/IEC 73/2009, 3.6.1.8: L'identificazione del rischio comporta l'individuazione delle fonti di rischio (3.5.1.2), degli eventi (3.5.1.3), delle loro cause e delle loro potenziali conseguenze (3.6.1.3). L'identificazione del rischio può coinvolgere dati storici, analisi teoriche, opinioni informate ed esperte e le esigenze delle parti interessate.

[11] Guida ISO/IEC 73/2009: 3.8.1.6 rischio residuo: rischio (1.1) rimanente dopo il trattamento del rischio (3.8.1)

NB: La compilazione delle tabelle riportate ai successivi paragrafi 4.1., 4.2. e 4.3. deve seguire le istruzioni riportate nell'Allegato 1.

6.1. Perdita di riservatezza

Perdita di riservatezza	La perdita di riservatezza dei dati ha impatto sui diritti e le libertà degli interessati? X SI > compilare il paragrafo 6.1 ☐ NO > passare al paragrafo 6.2

Divulgazione/ accesso non autorizzato o accidentale

1. Quali sono le potenziali minacce alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	X Accesso abusivo da parte di persone non autorizzate ai luoghi in cui si svolge il trattamento (es. sala CED, archivio dei documenti, uffici con computer, laboratori ecc.) ☐ Sottrazione da parte di soggetti interni o esterni alla struttura di documenti cartacei o di strumenti elettronici (pc) X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransomware, etc.) ☐ Intercettazione del traffico Ethernet; acquisizione dei dati inviati su una rete Wi-Fi, X Condivisione dei dati con soggetti non autorizzati ☐ _____

2. Quali sono le principali vulnerabilità rilevate?	☐ Salvataggio dei dati su chiavette USB o dischi esterni personali ☐ Inefficacia delle tecniche di pseudonimizzazione o crittografia X Mancata formazione del personale o formazione risalente ☐ Locali non protetti da accessi esterni ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ _____	
3.Conseguenze per gli interessati della perdita di riservatezza dei dati:	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di riservatezza dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
X Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
X Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale	Rivelazione del segreto professionale (art. 622 c.p.)	
X Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	☐ Improbabile 1 X Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4	
5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4	

6. **Rischio inerente** (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	X 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	X medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	X crittografia [descrizione delle tecniche di crittografia: i dati sono crittografati a livello dei DB PostGres e MongoDB, connessione crittografata TLS tra database e piattaforma applicativa (micro-servizi), connessione via VPN con servizi APSS] ☐ pseudonimizzazione X limitazione degli accessi X misure di protezione dagli attacchi informatici X Adozione di una policy per il corretto utilizzo degli strumenti informatici X Formazione del personale ☐ _____

8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. **Stima del rischio residuo**

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
I	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8

	Basso	X 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. Modalità di mitigazione del rischio per gestire il rischio residuo	X nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali misure ulteriori di sicurezza contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• sicurezza dei canali informatici, accesso solo dal sito aziendale (tramite VPN), lotta contro il malware, sicurezza dell'hardware, manutenzione, backup, gestione dei terzi che accedono ai dati, controllo accessi logici e accessi fisici
12. Priorità degli interventi di attuazione delle ulteriori misure di sicurezza	X Interventi già in essere ☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	1. Misure di sicurezza già implementate dalla Fondazione Bruno Kessler

14. Rischio residuo	X accettabile (1-6)	☐ non accettabile (8-16)
	✓ attuazione del trattamento	⚠ consultazione preventiva

6.2. Perdita di integrità

Perdita di integrità	La perdita di integrità dei dati ha impatto sui diritti e le libertà degli interessati? X SI > compilare il paragrafo 6.2 ☐ NO > passare al paragrafo 6.3

Divulgazione/accesso non autorizzato o accidentale

1. Quali sono le potenziali minacce alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	X Malfunzionamento dell'hardware X Malfunzionamento del software ☐ Deterioramento degli strumenti informatici ☐ Errore umano nell'inserimento dei dati X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransomware, etc.)
2. Quali sono le principali vulnerabilità rilevate?	☐ Mancanza di regolarità nella manutenzione dell'hardware ☐ Mancanza di regolarità nell'aggiornamento del software ☐ Strumenti non protetti da attacchi informatici ☐ Mancata adozione di una policy per il corretto utilizzo degli strumenti informatici ☐ Mancata formazione del personale X Phishing_____

3.Conseguenze per gli interessati della perdita di integrità dei dati:	Impatto sui **diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di integrità dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
X Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
X Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	
☐ Perdite finanziarie	Diritti patrimoniali	
X Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	

4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	X Improbabile 1 ☐ Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4
5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4

6. Rischio inerente (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	X Regolare manutenzione dell'hardware X Software aggiornato regolarmente X Adozione di una policy per il corretto utilizzo degli strumenti informatici X Formazione del personale ☐ Doppio controllo nell'inserire i dati nella eCFR

8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. Stima del rischio residuo

	Misure di sicurezza				
R		Adeguate	Minime	Insufficienti	Inesistenti
	Molto	☐ 4	☐ 8	☐ 12	☐ 16

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. Modalità di mitigazione del rischio per gestire il rischio residuo	X nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali misure ulteriori di sicurezza contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• sicurezza dei canali informatici, accesso solo dal sito aziendale (tramite VPN), lotta contro il malware, sicurezza dell'hardware, manutenzione, backup, gestione dei terzi che accedono ai dati, controllo accessi logici e accessi fisici
12. Priorità degli interventi di attuazione delle ulteriori misure di sicurezza	X Interventi già in essere ☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	1. Misure già implementate dalla Fondazione Bruno Kessler

14. **Rischio residuo**	X accettabile (1-6)	☐ non accettabile (8-16)
	✓ attuazione del trattamento	⚠ consultazione preventiva

6.3. Perdita di disponibilità

Perdita di disponibilità	La perdita di disponibilità dei dati ha impatto sui diritti e le libertà degli interessati? X SI > compilare il paragrafo 6.3 ☐ NO > passare al paragrafo successivo.

Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale

1. Quali sono le potenziali minacce alle quali sono esposte le aree ad accesso ristretto in cui si svolge il trattamento dei dati?	X Infezione del sistema tramite software nocivi diffusi via mail o attraverso internet (es. trojan horse, malware, spyware, cryptolocker, ransmoware, etc.) X Catastrofi naturali (incendi, allagamenti, terremoti) X Eliminazione accidentale dei dati ☐ _____	
2. Quali sono le principali vulnerabilità rilevate?	☐ Assenza di impianto antincendio ☐ Conservazione dei dati in locali seminterrati o vicino a tubature ☐ Zona sismica ☐ Strumenti non protetti da attacchi informatici ☐ Mancata formazione del personale X indisponibilità della rete_____	
3.Conseguenze per gli interessati della perdita di disponibilità dei dati:	**Impatto sui diritti e le libertà** degli interessati:	**Livello di impatto** della perdita di disponibilità dei dati:
☐ Morte	Diritto alla vita (art. 2 Cost.)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4 ☐ La perdita di disponibilità non è configurabile
☐ Danni all'integrità fisica	Diritto alla salute (art. 32 Cost.)	
☐ Furto o usurpazione d'identità	Diritto all'identità personale (art. 2 Cost.)	
☐ Discriminazioni	Diritto all'uguaglianza (art. 3 Cost.)	
☐ Pregiudizio alla reputazione	Diritto alla protezione della reputazione (art. 10 CEDU)	

☐ Perdite finanziarie	Diritti patrimoniali	
X Perdita del controllo sui propri dati personali	Diritto alla protezione dei dati personali (Reg. UE 679/2016)	
☐ altro_____	_____	
4. Stima della probabilità di accadimento delle minacce (fattore P della formula di calcolo del Rischio)	☐ Improbabile 1 X Poco probabile 2 ☐ Probabile 3 ☐ Molto probabile 4	
5. Stima dell'impatto (fattore I della formula di calcolo del Rischio)	☐ Lieve 1 X Medio 2 ☐ Grave 3 ☐ Gravissimo 4	

6. Rischio inerente (R = P x I)

		P			
		Improbabile	Poco probabile	Probabile	Molto probabile
I	Gravissimo	☐ 4	☐ 8	☐ 12	☐ 16
	Grave	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	X 4	☐ 6	☐ 8
	Lieve	☐ 1	☐ 2	☐ 3	☐ 4

Rischio inerente:	☐ basso (1-3)	X medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

7. Quali misure di sicurezza già in atto contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	X Misure di protezione dagli attacchi informatici [descrizione delle misure: aggiornamento costante dei software, programmi di protezione anti-malware e anti-intrusione,procedure di autenticazione e policy di autorizzazione di accesso ai dati] X Backup [descrizione delle modalità di backup: backup dei dati (giornalieri per l'ultima settimana, mensile per l'ultimo anno, annuale per gli ultimi due anni), mantenimento dei backup dei log per un mese, storico delle serie temporali dei software di log] X Cloud [descrizione del cloud: descrizione del cloud: Cloud

		Computing Service Microsoft Azure AKS; Azure Database for PostgreSQL; Database MongoDB as a service] X Formazione del personale ☐ _____		
8. Misure di sicurezza:	X adeguate	☐ minime	☐ insufficienti	☐ inesistenti

9. Stima del rischio residuo

		Misure di sicurezza			
		Adeguate	Minime	Insufficienti	Inesistenti
R i	Molto alto	☐ 4	☐ 8	☐ 12	☐ 16
	Alto	☐ 3	☐ 6	☐ 9	☐ 12
	Medio	☐ 2	☐ 4	☐ 6	☐ 8
	Basso	X 1	☐ 2	☐ 3	☐ 4

Rischio residuo:	X basso (1-3)	☐ medio (4-6)	☐ alto (8-9)	☐ molto alto (12-16)

10. Modalità di mitigazione del rischio per gestire il rischio residuo	X nessuna: accettazione del rischio (1-6) ☐ trasferimento del rischio (outsourcing) ☐ trasferimento del rischio (polizza assicurativa) ☐ adozione di ulteriori misure di sicurezza ☐ altro _____
11. Quali misure ulteriori di sicurezza contribuiscono a ridurre la probabilità e l'impatto di un evento negativo?	• _Non applicabili____
12. Priorità degli interventi di attuazione delle ulteriori misure di sicurezza	☐ secondo normativa/scadenza indicata (1) ☐ entro 3 mesi (2-3) ☐ entro 2 mesi (4-5) ☐ entro 1 mese (6-8) ☐ immediata (9-16)
13. Responsabile/i dell'attuazione delle ulteriori misure di sicurezza	1. 2.

14. Rischio residuo	X accettabile (1-6)	☐ non accettabile (8-16)
	✓ attuazione del trattamento	⚠ consultazione preventiva

6.4 Rischio residuo

Il rischio residuo viene valutato come **accettabile**, si potrà pertanto procedere con l'attività di trattamento dei dati personali oggetto della presente DPIA.

7. CONCLUSIONI

7.1 Valutazioni finali

7.1.1 Validazione della DPIA

Validazione dei Contitolari del trattamento

La DPIA diventa effettiva con la conferma di validazione da parte dei Titolari di trattamento. Alla luce della DPIA si ritiene non necessario inviare il presente documento per la condivisione con l'Autorità Garante.

Il presente documento è stato condiviso con il gruppo privacy, il dipartimento tecnologie e il servizio governance clinica di APSS, il Direttore del Centro Digital Health and Wellbeing di FBK, il Responsabile dell'Unità Digital Health Research di FBK, il Responsabile dell'Unità Digital Health Innovation Lab di FBK e con i DPO di APSS e di FBK. La DPIA a questo punto richiede la documentazione delle decisioni prese durante il processo di valutazione e validazione da parte dei rispettivi DPO e Titolari. Ciò consentirà di dimostrare la conformità del trattamento rispetto alle normative sulla protezione dei dati e di rendere trasparenti le decisioni intraprese dagli attori interessati.

Parere in merito alla valutazione d'impatto da parte dei DPO

Ai sensi dell'art. 39 par 1, lettera c) del GDPR il DPO ha il compito di *"fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35"*.

Parere del DPO APSS: Il DPO ha esaminato e valutato i contenuti della DPIA e l'ha ritenuta conforme all'art. 35 GDPR e alle Linee guida del Gruppo di lavoro ex art. 29.
Dalle valutazioni svolte è risultato che l'Azienda - tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche - mette in atto misure tecniche e organizzative che sono ritenute adeguate a garantire che il trattamento è effettuato conformemente al Regolamento UE 2016/679.

Dalla presente DPIA non si rilevano condizioni di rischio residuo elevato e, pertanto, non è necessario consultare l'Autorità garante ai sensi dell'art. 36 del GDPR.

Si raccomanda di riesaminare periodicamente e ad aggiornare, se necessario, la presente valutazione d'impatto.

Parere del DPO FBK:

Le attività di trattamento dei dati personali sono state implementate secondo i principi della privacy by design e della privacy by default. Tutti i rischi per i diritti e le libertà delle persone fisiche sono stati valutati in termini di probabilità e gravità del danno e sono considerati accettabili.

Si suggerisce di tenere sotto costante monitoraggio il trattamento dei dati personali, in particolare per quanto riguarda eventuali raccolte aggiuntive e/o trattamenti diversi che potrebbero proposti nel corso del Progetto, man mano che questo si evolve, in quanto deve sempre essere possibile dimostrare che le misure sono effettivamente e correttamente implementate.

Sulla base di tutte le informazioni raccolte durante questo processo, la DPO FBK approva ufficialmente questa DPIA.

Sottoscrizione per approvazione:

Data:

Firma: Il delegato al trattamento dati APSS:

Dott. Emanuele Torri

Data:

Firma Direttore del Centro Digital Health and Wellbeing FBK: