DATA PROTECTION IMPACT ASSESSENT (DPIA)

IPSG S.R.L

Via Carlo Carrà, 5

20900, Monza (MB)

C.F.- P.I. 09338750962

DATA PROTECTION IMPACT ASSESSENT (DPIA)

1. PREMESSA

Il presente documento viene redatto a cura della Società IPSG srl allo scopo di ottemperare a quanto stabilito dall'Art. 35 del Regolamento Europeo in materia di protezione dei dati personali 2016/679 (da qui GDPR).

Nell'ambito del contesto sopra descritto, il presente documento ha come obiettivo quello di fornire una guida metodologica per lo svolgimento del Risk Assessment (analisi del rischio) sui trattamenti 1 WP 248, rev. 01 "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del Regolamento (UE) 2016/679, Working Party 29 versione 4/10/2017."

Il menzionato articolo del GDPR stabilisce quanto segue:

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

A seguito dell'identificazione dei trattamenti a rischio elevato per i diritti e le libertà degli interessati, il presente documento fornisce, altresì, la guida metodologica per la conduzione del processo di Data Protection Impact Assessment (da qui DPIA) su tali trattamenti.

In base alle peculiarità allo scopo di dare evidenza dell'applicazione della normativa sulla protezione dei dati fin dalle prime fasi di attività, secondo quanto previsto dal principio della privacy by design.

Il documento è frutto delle analisi e del confronto che IPSG ha realizzato con la collaborazione delle seguenti figure di cui si avvale:

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

- Consulente in ambito Privacy;

1.1 Termini e definizioni

➢ **Titolare del trattamento** (Art. 4, n. 7, del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

➢ **Responsabile del trattamento** (Art. 4, n. 8, del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Interessato: la persona fisica identificata o identificabile (Art. 4, n. 1, del GDPR) a cui si riferisce il dato personale oggetto di trattamento.

➢ **Dato personale** (Art. 4, n. 1, del GDPR): qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

➢ **Trattamento** (Art. 4, n. 2, del GDPR): qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

➢ **Impatto**: indicazione della gravità di un incidente che può compromettere la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa privacy.

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

➢ **WP29** (Article 29 Working Party o Gruppo di Lavoro Articolo 29 per la protezione dei dati): il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Dal 25 maggio 2018 è stato sostituito dal Comitato europeo per la protezione dei dati (EDPB).

➢ **WP 248**, rev. 01: "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

2. ANALISI PRELIMINARE E SPECIFICHE OPERATIVE DELLA PIATTAFORMA

Come descritto nei punti successivi la Piattaforma avente lo scopo di gestire e conservare referti medici è stata considerata soggetto all'esecuzione della presente DPIA per le seguenti motivazioni:

- Impiego di dati relativi a persone fisiche classificati dal GDPR come dati particolari in quanto afferenti allo stato di salute di una persona.

- Impiego di nuove tecnologie in quanto il progetto si basa sull'impiego di una piattaforma tecnologica.

La piattaforma utilizzata è PQRST, strumento creato per il salvataggio e la condivisione di referti medici, principalmente cardiologici. Gli esami che possono essere salvati sulla piattaforma sono: ecg, holter, MAP, spirometrie e altri esami a patto che siano in formato .pdf o dicom.

PQRST offre agli utenti uno spazio sicuro in cloud accessibile da qualunque dispositivo con collegamento internet, tramite tutti i browser disponibili. Una volta iniziato l'abbonamento l'utente potrà accedere al suo spazio tramite e-mail e password e avrà a disposizione uno spazio illimitato per il salvataggio dei suoi referti. PQRST oltre al servizio di storage offre anche un servizio di condivisione fra medici. L'utente infatti potrà invitare a collaborare al suo spazio altri medici che riceveranno quindi l'accesso alla piattaforma, sempre tramite e-mail e password, e potranno vedere in automatico eventuali esami che l'utente condividerà con loro. In questo caso l'utente che è stato invitato sarà un utente con ruolo di "refertatore".

Quando un file viene caricato sulla piattaforma PQRST dall'utente il file stesso verrà salvato con uno specifico "stato" ovvero stato "caricato", se l'utente decide di condividere l'esame con il suo utente refertatore lo stato dell'esame diventerà "in attesa" e questo stato sarà visibile anche dal refertatore.

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

Quando il refertatore procede all'apertura dell'esame con il tool interno alla piattaforma oppure lo scarica, lo stato dell'esame diventa "in lavorazione" sia per l'utente che per il refertatore, una volta che il refertatore ha analizzato l'esame e lo ha nuovamente ricaricato con diagnosi e firma in formato .zip (lo zip si crea automaticamente) lo stato diventa "firmato" sia per il refertatore che per l'utente.

A questo punto l'esame rimane disponibile sempre per il download per l'utente, il refertatore invece vedrà la riga dell'esame nella sua lista ma non potrà più scaricarlo. Poiché è possibile per un utente aggiungere più refertatori dopo che il primo refertatore avrà aperto un esame gli altri non potranno più farlo, per evitare doppie refertazioni. Gli utenti "refertatori" hanno un tempo di 24h per referatare: nel caso in cui il tempo non sia sufficiente, un altro utente "refertatore" può accedere allo stesso file.

PQRST può essere gestita da un singolo medico che sarà l'unico a poter caricare gli esami oppure potrà essere uno spazio multiutente, in questo caso la piattaforma avrà un singolo amministratore che potrà aggiungere più utenti in grado di caricare gli esami, questi utenti vedranno solo gli esami caricati da loro e non quelli caricati dagli altri utenti, solo l'amministratore potrà vedere tutti i file.

3. ATTORI COINVOLTI NEL PROGETTO

Gli attori coinvolti sono i seguenti:

- Personale medico ed infermieri
- IPSG srl quale provider di servizio che sovraintende la realizzazione della piattaforma, la gestisce e ne monitorizza l'utilizzo.
- Pazienti quali soggetti interessati.

In regime di totale trasparenza si precisa che la IPSG srl, non potrà accedere alla piattaforma né in alcun modo ai dati personali e sanitari dei soggetti coinvolti direttamente o indirettamente, ma avrà il ruolo di Responsabile del trattamento ex art. 28 GDPR con funzione di Amministratore di sistema all'interno del processo privacy, intervenendo solo ove fosse necessario per aspetti di carattere esclusivamente tecnico.

4. IDENTIFICAZIONE DEI RUOLI DEGLI ATTORI IN BASE ALLA DATA PROTECTION

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

In relazione agli attori mappati al Punto precedente IPSG srl ha operato una serie di valutazioni allo scopo di configurare correttamente non solo il proprio ruolo in relazione alla piattaforma ma anche il ruolo degli ulteriori attori coinvolti.

In considerazione del fatto che è presente un coinvolgimento diretto di medici specializzati e di infermieri, che nell'ambito privacy sono Titolari del Trattamento, ad esso afferenti in quanto (come meglio dettagliato successivamente) saranno i Medici ad utilizzare la piattaforma inserendo una serie di informazioni sul paziente di carattere sanitario.

La valutazione a cui si è giunti è stata quella relativa ad un rapporto tra Titolare (medici o infermieri) e del responsabile quale amministratore di sistema per la società IPSG srl, pertanto il personale sanitario che decide di usufruire della piattaforma decide in piena autonomia le finalità ed i mezzi del trattamento.

La responsabilità della gestione del dato sulla piattaforma resta quindi in capo al personale sanitario mentre IPSG srl, in quanto provider di servizio, si occuperà di intervenire in via esclusiva per aspetti prettamente tecnici ed informatici relativi alla piattaforma utilizzata per le presenti attività.

I medici e gli infermieri avranno dunque l'obbligo di predisporre apposita informativa ex artt. 13 e 14 del GDPR al fine di richiedere specifico consenso ai pazienti per accedere alla piattaforma.

5. TIPOLOGIA DI DATI COINVOLTI

L'accesso alla piattaforma comporta il trattamento dei seguenti dati:

Dati personali dei Pazienti

- non vengono tracciati dati personali del paziente

Dati "particolari" dei Pazienti

- referto medico quale a titolo esemplificativo ma non esaustivo elettrocardiogrammi

Dati personale sanitario (Medici ed infermieri)

- Non vengono tracciati dati del personale sanitario, può accedervi alla piattaforma un solo soggetto munito di specifica password.

6. L'ATTIVITÀ DI RISK ASSESSMENT – (ANALISI DEI RISCHI)

Documento di valutazione rischi (DPIA) di utilizzo esclusivo della IPSG SRL

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

L’attività di Risk Assessment si sviluppa sulla base dei seguenti step metodologici:

- Step 1: Definizione del valore di criticità dei trattamenti.
- Step 2: Identificazione trattamenti critici. Nei paragrafi successivi è riportato il dettaglio degli step metodologici previsti ai fini dello svolgimento del Risk Assessment.

Definizione del valore di criticità dei trattamenti:

La definizione del valore di criticità dei trattamenti è effettuata partendo dalla mappatura dei trattamenti dei dati personali effettuati dall’Azienda e tracciati all'interno del "Registro delle attività di Trattamento" aziendale.

Nel dettaglio, il contenuto informativo riguarda gli ambiti:

- ID Trattamento
- Direzione/Unità Organizzativa
- Finalità del trattamento
- Base giuridica del trattamento
- Categorie interessati
- Categorie dati personali
- Categoria destinatari a cui i dati personali sono stati o saranno comunicati
- Termine cancellazione dati
- Applicativo o banca dati (cartaceo o elettronico)
- Misure di sicurezza tecniche ed organizzative
- Trattamento verso paese terzo (se previsto)
- Paese o organizzazione a cui si invia
- Trattamento verso paese terzo (se previsto)

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

– Garanzie Per ognuno dei trattamenti mappati.

il Titolare del trattamento procede con la valorizzazione qualitativa (SI; NO) delle specifiche variabili utili per la definizione del livello di criticità dei trattamenti.

Livelli di criticità delle variabili		
Livello di criticità	**Peso delle variabili**	**Descrizione**
ALTO	3	Variabile che può determinare un alto livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un alto impatto sui diritti e sulle libertà delle persone fisiche
MEDIO	2	Variabile che può determinare un medio livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un medio impatto sui diritti e sulle libertà delle persone fisiche
BASSO	1	Variabile che può determinare un basso livello di criticità in termini di accessi non autorizzati, di modifica / cancellazione / furto / e diffusione di dati personali, determinando un basso impatto sui diritti esulle libertà delle persone fisiche

Il valore di criticità del trattamento è ottenuto come somma del peso delle variabili valorizzate con"Sì".

6.1 Identificazione trattamenti critici:

Sulla base del valore di criticità determinato, i trattamenti sono classificati in funzione del rispettivo livello di criticità.

Un trattamento è valutato come “critico” nel caso in cui il Livello di Criticità del Trattamento risulti uguale ad "ALTO".

Per i trattamenti critici identificati, il Titolare del trattamento, effettua la valutazione del rischio per i diritti e le libertà delle persone fisiche scaturente dal trattamento nei seguenti due momenti:

- Valutazione del Rischio Inerente sulla base di criteri di impatto e probabilità;
- Valutazione del Rischio Residuo a seguito della valutazione dei controlli posti in essere ai fini della mitigazione del rischio e corrispondenti al sistema di prevenzione e protezione dei dati personali in essere.

6.2 L’ATTIVITÀ DI DATA PROTECTION IMPACT ASSESSMENT:

L’attività di Data Protection Impact Assessment (DPIA) si sviluppa sulla base dei seguenti step metodologici:

Step 1: Valutazione del livello di Rischio Inerente

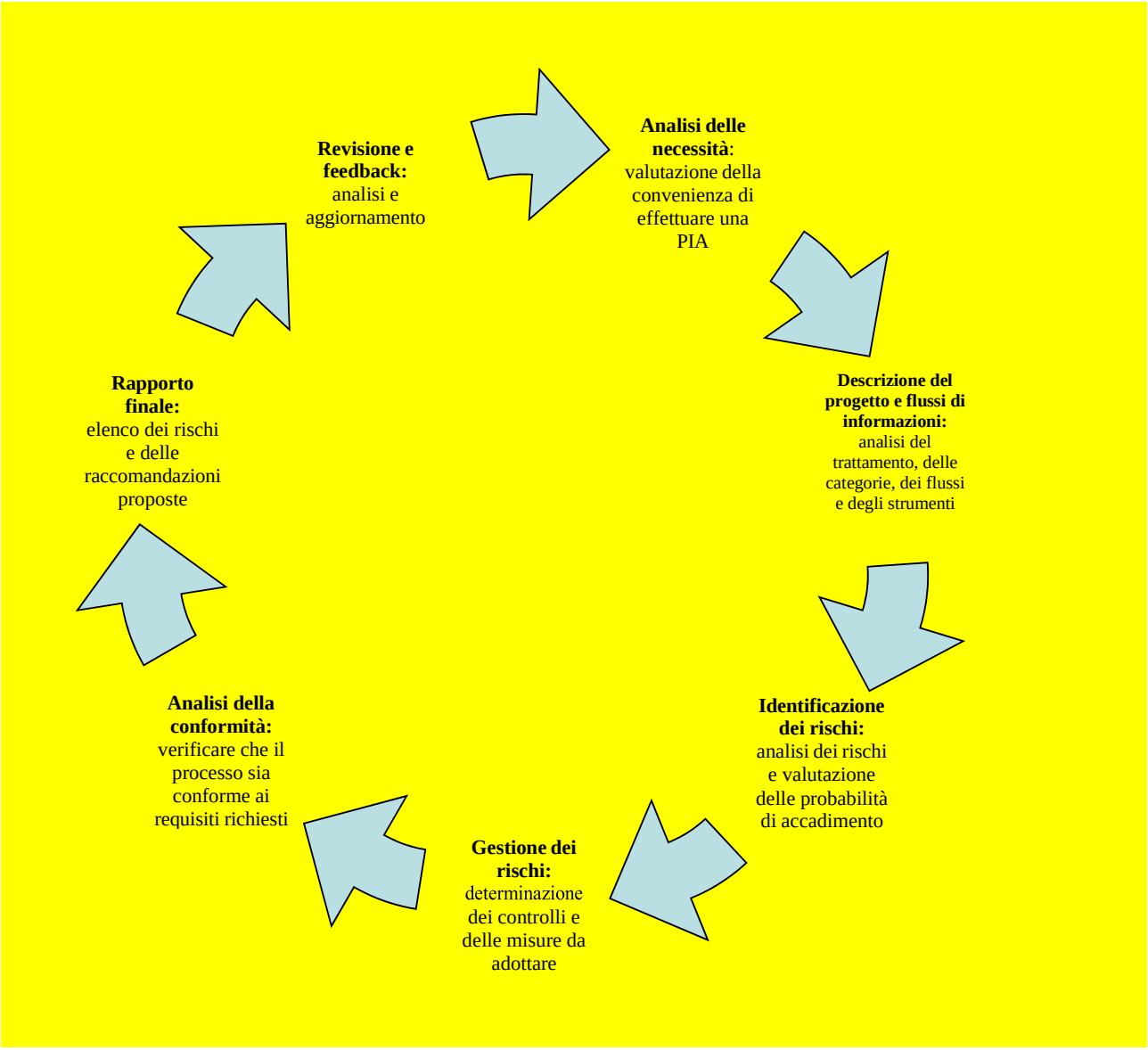
Step 2: Identificazione tipologia di trattamento

Step 3: Valutazione controlli

Step 4: Definizione del livello di Rischio Residuo

Step 5: Identificazione trattamenti rischiosi

DATA PROTECTION IMPACT ASSESSENT (DPIA)



6.3 VALUTAZIONE DEL LIVELLO DI RISCHIO INERENTE

Il Data Protection Impact Assessment inizia con la valutazione del Rischio Inerente, attraverso il quale viene identificato il rischio del trattamento, senza considerare gli eventuali presidi di controllo posti in essere dall'Azienda per la sua mitigazione, combinando, sulla base di metriche predefinite, le seguenti due dimensioni:

- Impatto, ovvero il possibile effetto che la diffusione dei dati potrebbe avere per l'interessato;
- Probabilità di accadimento, ovvero la frequenza con cui il trattamento è effettuato.

Il Titolare del trattamento, valuta qualitativamente l'impatto e la probabilità connessi a ciascun trattamento sulla base dell'applicazione di specifiche scale di valutazione adottate per le valutazioni inerenti l'impatto.

I valori di Impatto e Probabilità attribuiti sono tradotti quantitativamente su una scala da 1 a 4, dove 1 corrisponde al valore minimo (es. Impatto = Trascurabile; Probabilità = Evento raro) e 4 corrisponde al valore massimo (es. Impatto = Massimo; Probabilità = Evento probabile).

7. TIPOLOGIA DI INTERESSATI

Come indicato ai Punti precedenti gli interessati sono:

- i pazienti;
- i medici ed infermieri che utilizzano la piattaforma.

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

8. DESCRIZIONE DEI TRATTAMENTI AFFERENTI ALLA PIATTAFORMA

Le attività si basano sull'utilizzo di un sistema di telerefertazione che viene realizzato tramite la piattaforma digitale messa a disposizione da IPSG srl accessibile tramite password:

Modalità di raccolta dei dati:

I dati relativi ai pazienti vengono raccolti a cura del personale sanitario che acquista il servizio. Tali dati si riferiscono ai pazienti, ai quali è stata consegnata specifica informativa ex artt.13 e 14 del Gdpr.

Attività afferenti all'area sanitaria svolte a cura di personale medico:

- caricamento del referto

I dati relativi al Paziente vengono inseriti a cura del personale medico all'interno della piattaforma;

Archiviazione, aggiornamento ed eliminazione dei dati

Le operazioni aventi ad oggetto i dati particolari dei pazienti avvengono esclusivamente a cura del personale sanitario ed archiviati sulla piattaforma per tempo illimitato, sarà la società IPSG srl che in caso di mancato rinnovo del servizio da parte del personale sanitario potrà provvedere alla cancellazione.

9. TECNOLOGIA IMPIEGATA E TRASFERIMENTO DI DATI ALL'ESTERO

L'utilizzo della piattaforma si compone delle seguenti specifiche tecnologiche a tutela dei dati particolari dei pazienti inerenti i referti.

I dati non vengano trasferiti all'estero visto che:

il server è situato in Italia presso Register.it - i dati sono conservati e garantiti seguendo i loro standard di sicurezza: Data Center allineato Tier 3+, Monitoraggio Infrastruttura 24/7/365,

L'Aggiornamento di virtualizzazione della piattaforma avviene in modo costante, avendo programmato un supporto di emergenza notturno e festivo, consultabile al seguente sito: www.register.it/server/vps/

9.1 GESTIONE SICUREZZA ED ACCESSO PIATTAFORMA

La piattaforma utilizza la massima protezione dei dati personali e particolari che su di essa vengono caricati e monitorati, la sicurezza è il punto principale ed il più importante su quale verte il sistema di gestione delle informazioni acquisite.

A) il flusso delle informazioni viene gestito nel seguente modo:

I) I files vengono caricati dall'utente/utenti in una cartella "temporanea" dove successivamente un "Agente" legato ad un CronJob (attività programmata), una volta fatte le opportune verifiche, provvede a spostarli in una cartella dell'utente all'interno del server.

II) Successivamente gli utenti "che hanno refertato il paziente" collegati ad utenti caricatori possono accedere al file per consultazione web con il Tool di Refertazione o effettuare il Download. Gli utenti che hanno provveduto a refertare il paziente possono vedere il record del file, ma solo il primo refertatore può prenderlo in carico e solo lui riesce a vedere il file, nel caso il cui un altro refertatore possa accedere al file si deve di nuovo cambiare lo stato al file originario.

Gli utenti "refertatori" hanno un tempo di 24h per refertare: nel caso in cui il tempo non sia sufficiente, un altro utente "refertatore" può accedere allo stesso file.

III) Alla fine del processo, gli utenti "refertatori" possono caricare il referto, o refertarlo utilizzando il Tool di Refertazione web: l'applicazione crea uno .zip

IV) Gli Utenti caricatori possono scaricare il file .zip generato.

B) il sistema di protezione dati è stato impostato come di seguito specificato:

I dati vengono caricati dall'utente in una cartella "temporanea" dove successivamente un CronJob (attività programmata), una volta fatte le opportune verifiche, sposta in una cartella dedicata dell'utente all'interno del server. A tale cartella non è possibile accedervi direttamente, tranne se non si è autenticati secondo i protocolli di Laravel.

Alla cartella dell'utente non si può accedere direttamente in nessun modo, l'utente che è proprietario del file può scaricare il file, ma richiesta e download passano sempre dal server, dunque si può scaricaresolo con l'autenticazione di laravel e tutti i sistemi di sicurezza di cui è provvisto.

Sistema di autenticazione Laravel:

Laravel dispone già di un robusto processo di autenticazione dell'utente con il codice boilerplate associato disponibile nello scaffolding.

Laravel utilizza "provider" e "guardie" per facilitare il processo di autenticazione. Le guardie autenticano gli utenti per ogni richiesta che fanno, mentre i "provider" facilitano il recupero degli utenti dal database.

I files, quando vengono caricati/salvati non possono essere distinti tra loro, perché vengono registrati con nomi criptati tramite Hash, e dunque per poter accedere ai medesimi files si deve chiamare il Database per poterli individuare.

Le chiamate che si fanno dal Browser al Server vengono protette dai sistemi Laravel che prevedono la protezione contro l'impersonificazione degli utenti.

Laravel è fornito di un'interfaccia per crittografare e decrittografare il testo tramite OpenSSL, utilizzando la crittografia AES-256 e AES-128.

Tutti i valori crittografati di Laravel sono firmati con un codice di autenticazione dei messaggi (MAC), in modo che il valore sottostante non possa essere modificato o manomesso una volta crittografato.

Laravel è un framework PHP per applicazioni web che viene utilizzato per sviluppo Backend.

Tale utilizzo gli garantisce un enorme affidabilità e sicurezza poiché fornisce tutte le funzionalità necessarie “lato server”.

Gestione delle password: Laravel Hash fornisce un hashing sicuro Bcrypt e Argon2 per la memorizzazione delle password degli utenti.

C) l’accesso al gestionale avviene tramite e-mail e password robuste Per aumentare il livello di sicurezza delle autenticazioni è stata definita una scadenza periodica dellepassword che avviene ogni 90 giorni. Gli utenti della Piattaforma dovranno comporre password robuste, come richiesto dalla piattaformadella pw robuste composte da caratteri alfanumerici, caratteri speciali e lettere maiuscole e minuscole e con lunghezza minima di 8 caratteri al fine di tutelare i dati da loro inseriti.

La piattaforma utilizzata è PQRST che garantisce un elevato livello di sicurezza dei dati grazie alla protezione dei server e alle procedure di contrasto all'intrusione descritte in questo documento.

Il primo sistema di protezione riguarda l'autenticazione dei pazienti e dei medici che seguono i pazienti che hanno aderito al progetto. Tramite L'autenticazione si può verificare l'identità di un utente e determinare se ha diritto ad accedere in piattaforma. L'accesso avviene in via esclusiva mediante delle credenziali di accesso (username e password).

10. GIUSTIFICAZIONE PER L'UTILIZZO DELLA PIATTAFORMA

Si riportano qui di seguito obiettivi e vantaggi che possono essere perseguiti grazie alle attività svolte con la piattaforma PQRST.

Obiettivi e Vantaggi per il personale sanitario, riguarda un facile accesso ai referti caricati in piattaforma, evitando la gestione cartacea dei documenti, e permettendo una facile fruibilità dei documenti sanitari dei pazienti.

Lo scopo di utilizzare tale piattaforma è quello di avere i dati sempre a portata di mano accelerando e monitorando i tempi di diagnosi e trattamento.

In questo quadro verranno ottimizzati i tempi e la qualità delle prestazioni ed il paziente, risulterà più tutelato consentendogli una formulazione immediata del trattamento ideale, evitando così di incorrere in maggiori complicazioni in futuro.

11. FINALITA' DEL TRATTAMENTO

I trattamenti di dati necessari all'esecuzione delle attività sanitarie trovano la loro finalità nell'esecuzione delle attività terapeutiche come descritto ai punti precedenti utilizzando i dati personali e particolari dei pazienti.

12. MINIMIZZAZIONE DEI DATI

I dati inserti nella Piattaforma sono esclusivamente quelli necessari per l'esecuzione delle attività descritte ai punti precedenti a cura del personale sanitario.

VALUTAZIONE DEL RISCHIO

Accesso illegittimo

Probabilità: Bassa Gravità: Alta

Misure di mitigazione: l'accesso ai dati avviene a cura di personale medico che utilizza specifiche credenziali (username password).

Modifiche indesiderate dei dati

Probabilità: Bassa Gravità: Alta

Misure di mitigazione: l'accesso ai dati avviene a cura del personale medico che utilizza specifiche credenziali (username password).

Perdita dei dati

Probabilità: Bassa Gravità: Alta

Misure di mitigazione: viene garantito il costante backup dei dati.

Rischi legati alla riservatezza dei dati

Il trattamento riguarda i dati personali e particolari relativi ai pazienti; non vengono utilizzati per ulteriori finalità rispetto a quelle specificate nella relativa informativa che viene sottoposta ai pazienti quale condizione di liceità del trattamento.

Rischi legati all'integrità dei dati

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

Probabilità: Bassa Gravità: Alta

I dati vengono costantemente aggiornati a cura esclusivamente del personale medico.

Rischi legati alla perdita di disponibilità dei dati

Probabilità: Bassa Gravità: Alta

L'accesso ai dati avviene tramite le specifiche credenziali di autenticazione soggette a modifica periodica esclusivamente a cura del personale medico.

Sui server è attivo un sistema di backup e di recovery realizzato con sistemi ridondanti.

Eventuali difficoltà di mal funzionamento vengono risolte grazie all'intervento del gestore dell'applicazione.

VALUTAZIONE DEGLI IMPATTI PER GLI INTERESSATI

IMPATTO PER GLI INTERESSATI DETTAGLIO

GRAVITA' DELL'IMPATTO

Perdita del controllo dei dati personali

I dati trattati sono monitorati dal personale medico in modo costante grazie alle funzionalità della piattaforma;

Medio

Limitazione dei diritti L'utilizzo della piattaforma non limita in alcun modo i diritti degli interessati che in ogni momento possono rivolgersi al proprio medico refertatore per esercitare i diritti di cui agli Artt.

15-22 del GDPR

Basso

Discriminazione

I dati coinvolti non espongono gli interessati ad atteggiamenti discriminatori

Medio

Furto o usurpazione d'identità Il furto o l'usurpazione di identità

in relazione ai dati dei pazienti non comporterebbe alcun vantaggio

Basso

Pregiudizio alla reputazione

Basso

I dati coinvolti nel Progetto sono di natura sia personale sia di natura particolare (inerenti allo stato di

salute); il pregiudizio non può essere escluso.

Medio

Perdita di riservatezza dei dati personali protetti da segreto professionale

Il trattamento avviene a cura di personale medico soggetto al segreto professionale oltre che agli obblighi stabiliti dalla normativa in materia di protezione dei dati.

Basso

Conoscenza da parte di terzi non autorizzati

Eventuali terzi coinvolti (il cui numero è volutamente ristretto al fornitore della piattaforma tecnologica) sono soggetti a specifici vincoli di protezione dei dati da parte del personale sanitario

Basso

ASPETTI DEFINITIVI DEI RISCHI

Quali sono i principali fattori di rischio per la società?

I principali fattori di rischio per il Titolare e il Responsabile del trattamento derivanti dalle attività di gestione di **della Piattaforma PQRST** sono:

- Rischi sull'integrità dei dati;
- Rischi sulla riservatezza dei dati;
- Rischi sulla disponibilità dei dati;
- Rischi di trattamento non conforme alle finalità della raccolta;

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

- Rischio reputazionale;
- Rischio finanziario;
- Rischio legale e di conformità.

- MISURE PREVISTE O ESISTENTI

Elenco dei controlli di sicurezza fisica e informatica, e dei controlli organizzativi implementati dal Responsabile

	Controlli di sicurezza fisica e informatica
☒	**Protezione da virus, malware o altri software dannosi** La Piattaforma PQRST, è protetta da firewall. I dati presenti sono accessibili solo da personale che accede con specifiche credenziali. La piattaforma applicativa gira su infrastruttura in cloud che adotta un firewall applicativo; l'infrastruttura virtuale Microsoft è, inoltre, costantemente aggiornata nell'ambito del servizio PAAS.
☒	**Vulnerabilità** Il Responsabile svolge test periodici di vulnerabilità (vulnerability assessment) al fine di testare, verificare e valutare le vulnerabilità del sistema, garantire la sicurezza del trattamento e mitigare i rischi che insistono sui dati.
☒	**Contratti di nomina dei responsabili del trattamento dei dati presenti** Presenti.
☒	**Controllo degli accessi logici all'applicativo** L'applicativo prevede un sistema di autenticazione degli accessi.
☒	**Gestione dei pc** È previsto il meccanismo di autenticazione con inserimento di Username, Password personale. La password è modificata ogni 90 giorni
☒	**Backup** È previsto processo di backup quotidiano sull'applicativo

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

☒	**Minimizzazione dei dati** La minimizzazione dei dati è realizzata sin dalla fase di progettazione: vengono trattenute solo le informazioni ritenute funzionali a perseguire lo scopo del trattamento, escludendo quelle ininfluenti.
☒	**Sicurezza hardware** La società ha implementato una prassi operativa relativa alla dismissione dell'hardware per garantire la sicurezza dei dati.
☒	**Tracciabilità (log)** Il sistema di autenticazione previsto nell'uso dell'applicativo garantisce il logging degli accessi. I log sono protetti da modifiche non autorizzate da parte degli Amministratori e dall'accesso non autorizzato agli stessi**.**
☒	**Sicurezza dei siti web** La società ha implementato un sistema di monitoraggio continuativo della sicurezza dei propri sistemi.

	Controlli organizzativi
☒	**Procedure in caso di data breach** Il Responsabile del trattamento ha attuato una Policy sulla gestione dei Data Breach: Policy Data Breach.
☒	**Funzione privacy all'interno della società** Il Responsabile ha strutturato uno specifico Team deputato alla gestione di tutti gli adempimenti in materia di protezione dei dati personali, oltre che alla mitigazione dei relativi rischi.
☒	**Gestione del personale, formazione e sensibilizzazione** La Società sta formalizzando un plan periodico di formazione e sensibilizzazione in materia di protezione dei dati personali rivolto al personale coinvolto nelle attività di trattamento
☒	**Relazione con terze parti**

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

	Ciascun soggetto esterno che ha o potrebbe avere accesso ai dati personali del Titolare del trattamento è stato nominato Responsabile del trattamento ai sensi dell'art. 28 del GDPR.

- ACCESSO NON AUTORIZZATO AI DATI PERSONALI

1. **Quale sarebbe l'impatto principale sugli interessati se il rischio di accesso non autorizzato ai dati personali si verificasse?**

Un accesso non autorizzato ai dati personali potrebbe tradursi in un rischio per i diritti e le libertà degli interessati. La società ottiene "notizie di reato" tramite sistemi di alert, di log con continui miglioramenti sul piano della sicurezza cyber.
L'eventuale accesso ai dati presenti a sistema si potrebbero concretizzare in: esposizioni a ricatti e diffamazione, discriminazione, danni reputazionali, danni psicologici, danno molto significativo e noto sia all'interno che all'esterno del perimetro aziendale.

2. **Quali sono le principali fonti di rischio e minacce che potrebbero tradursi in fattori di rischio?**

Attacchi malevoli (malware, phishing, social engineering), minacce interne intenzionali: atti volontari commessi da soggetti interni alla società volti ad accedere ai sistemi informativi senza esserne autorizzati.

3. **Quali tra i controlli identificati contribuiscono a mitigare i rischi di accesso non autorizzato?**

	Controlli di sicurezza fisica e informatica
☒	Archiviazione
☒	Protezione da virus, malware o altri software dannosi
☒	Vulnerabilità
☒	Contratti di nomina dei responsabili del trattamento dei dati presenti
☒	Controllo degli accessi logici
☒	Gestione dei pc
☒	Backup
☒	Minimizzazione dei dati
☒	Sicurezza hardware
☒	Tracciabilità (log)

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

☒	Rischi ambientali
☒	Sicurezza siti web

	Controlli organizzativi
☒	Integrazione della funzione privacy nel progetto relativo alle attività di trattamento
☒	Procedure in caso di data breach
☒	Funzione privacy all'interno della società
☒	Gestione personale, formazione e sensibilizzazione
☒	Relazione con terze parti

4. C**on riguardo agli impatti principali e ai controlli pianificati?**

Importante

Motivi della valutazione della gravità: La gravità del rischio di accesso non autorizzato ai dati personali è stata ritenuta importante poiché potrebbero essere rivelate condotte e comportamenti degli interessati potenzialmente suscettibili di ledere i diritti e le libertà degli stessi.

5. **Come è valutata la probabilità dei rischi di accesso non autorizzato ai dati personali, in particolare in relazione a minacce, fonti di rischio e controlli pianificati?**

Limitata

Motivi della valutazione della probabilità: La probabilità di accesso non autorizzato è stata ritenuta limitata poiché le misure di sicurezza tecniche e organizzative adottate dal Responsabile del trattamento sono adeguate a mitigare tale rischio.

- MODIFICAZIONE INDESIDERATA DEI DATI PERSONALI

1. **Quale sarebbe l'impatto principale sugli interessati del trattamento se il rischio di modificazione indesiderata dei dati personali si verificasse?**

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

Esporrebbe gli interessati al rischio di esposizioni a ricatti e diffamazione, discriminazione, danni reputazionali, danni psicologici, danno molto significativo e noto sia all'interno che all'esterno del perimetro aziendale.

2. **Quali sono le principali fonti di rischio e minacce che potrebbero tradursi in fattori di rischio?**

- Minacce esterne non intenzionali: attacchi malevoli (malware, phishing, social engineering) o malfunzionamenti dei sistemi;
- Minacce interne non intenzionali: imperizia, negligenza imprudenza di dipendenti.

3. **Quali tra i controlli identificati contribuiscono a mitigare i rischi di modificazione indesiderata?**

	Controlli di sicurezza fisica e informatica
☒	Archiviazione
☒	Protezione da virus, malware o altri software dannosi
☒	Vulnerabilità
☒	Contratti di nomina dei responsabili del trattamento dei dati presenti
☒	Controllo degli accessi logici
☒	Gestione dei pc
☒	Backup
☒	Minimizzazione dei dati
☒	Sicurezza hardware
☒	Tracciabilità (log)
☒	Rischi ambientali
☒	Sicurezza siti web

	Controlli organizzativi
☒	Integrazione della funzione privacy nel progetto relativo alle attività di trattamento
☒	Procedure in caso di data breach

DATA PROTECTION IMPACT ASSESSENT (DPIA)

☒	Funzione privacy all'interno della società
☒	Gestione personale, formazione e sensibilizzazione
☒	Relazione con terze parti

4. **Come è valutata la gravità dei rischi di modificazione indesiderata dei dati personali, in particolare con riguardo agli impatti principali e ai controlli pianificati?**

Limitata.

Motivi della valutazione della gravità:
La probabilità di modifica indesiderata dei dati personali è stata ritenuta limitata poiché le misure di sicurezza tecniche e organizzative adottate dal Responsabile del trattamento sono adeguate a mitigare tale rischio.

5. **Come valuta la probabilità dei rischi di modificazione indesiderata, in particolare in relazione a minacce, fonti di rischio e controlli pianificati?**

Limitata.

Motivi della valutazione della probabilità:
La probabilità di modificazione indesiderata dei dati è stata ritenuta limitata in virtù delle misure di sicurezza tecniche ed organizzative adottate dal Responsabile .

- PERDITA DI DATI

1. **Quale sarebbe l'impatto principale per gli interessati qualora il rischio di perdita di dati si manifestasse?**

La perdita dei dati personali potrebbe tradursi nell'incapacità del Titolare e del Responsabile di aver contezza di situazioni che abbiano potuto mettere in pericolo la sicurezza di persone o beni.

2. **Quali sono le principali fonti di rischio e minacce che potrebbero tradursi in fattori di rischio?**

- Minacce esterne non intenzionali: modificazione dei dati dovuta al danneggiamento involontario dei sistemi su cui risiedono i dati personali.
- Minacce esterne intenzionali: tentativi deliberati da parte di soggetti esterni di cancellare o copiare i dati che risiedono sui sistemi del Titolare e del Responsabile.
- Minacce interne non intenzionali: atti accidentali compiuti da soggetti interni alla società che potrebbero cancellare i dati della società a causa di negligenza o errore umano.

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

- Minacce interne intenzionali: atti volontari commessi da soggetti interni alla società volti ad accedere ai sistemi per procedere alla successiva cancellazione o copia dei dati personali presenti sugli stessi.

3. **Quali tra i controlli identificati contribuiscono a mitigare tali rischi?**

	Controlli di sicurezza fisica e informatica
☒	Archiviazione
☒	Protezione da virus, malware o altri software dannosi
☒	Vulnerabilità
☒	Contratti di nomina dei responsabili del trattamento dei dati presenti
☒	Controllo degli accessi logici
☒	Gestione dei pc
☒	Backup
☒	Minimizzazione dei dati
☒	Sicurezza hardware
☒	Tracciabilità (log)
☒	Rischi ambientali
☒	Sicurezza siti web

	Controlli organizzativi
☒	Integrazione della funzione privacy nel progetto relativo alle attività di trattamento
☒	Procedure in caso di data breach
☒	Funzione privacy all'interno della società
☒	Gestione personale, formazione e sensibilizzazione
☒	Relazione con terze parti

4. **Come è valutata la gravità dei rischi, in particolare con riguardo agli impatti principali e ai controlli pianificati?**

IPSG S.r.l.	**DATA PROTECTION IMPACT ASSESSENT (DPIA)**

Limitata

Motivi della valutazione della gravità: La gravità del rischio di perdita dei dati personali è stata ritenuta limitata poiché le conseguenze da essa derivanti non sono tali da ledere gravemente i diritti e le libertà degli interessati. In aggiunta, il recupero della struttura dell'applicativo essendo oggetto di backup, è di facile esecuzione

5. **Come valuta la probabilità del rischio, in particolare in relazione a minacce, fonti di rischio e controlli pianificati?**

Limitata

Motivi della valutazione della probabilità: La probabilità di perdita dei dati personali è stata ritenuta limitata poiché le misure di sicurezza tecniche e organizzative adottate dal Responsabile del trattamento sono adeguate a mitigare tale rischio.

RISK OVERVIEW

RISK OVERVIEW
Complessivamente si ritiene che i rischi per i diritti e le libertà degli interessati siano mitigati in misura adeguata dalle misure di sicurezza tecniche e organizzative messe in atto dal Responsabile del trattamento.

Valutazione complessiva delle risultanze della Valutazione di Impatto sul Programma
Buon livello di adeguatezza