DATA PROTECTION IMPACT ASSESSMENT

PER L'UTILIZZO DELLA PIATTAFORMA PQRST

IPSG SRL

Via Vittor Pisani 28, 20128, Milano (MI)

Nome del DPO/RPD: Simona Giulieri

1. Posizione del DPO/RPD

Il trattamento può essere implementato.

2. Parere del DPO/RPD

Alla luce delle misure tecniche e organizzative adottate o pianificate da IPSG S.r.l. in relazione alla piattaforma PQRST, si ritiene che il trattamento presenti un livello di rischio residuo accettabile per i diritti e le libertà degli interessati, in particolare in merito:

- alla base giuridica chiara e differenziata per ciascuna categoria di dati (sanitari, di contatto, tecnici e di pagamento);
- all'adozione (in corso di perfezionamento) di un sistema di gestione dei rischi privacy e di policy aggiornate per il personale coinvolto;
- all'impegno formale per l'implementazione di misure correttive indicate nel piano d'azione (accessi, logging, segregazione, backup);
- all'impostazione coerente con il principio di privacy by design e alla redazione di una DPIA completa e coerente con i riferimenti normativi (art. 35 GDPR e WP29 Guidelines).

Si raccomanda:

- l'aggiornamento della DPIA, con cadenza annuale o a seguito di modifiche sostanziali del trattamento;
- la formalizzazione di tutti i contratti ex art. 28 GDPR con i professionisti sanitari;
- la verifica periodica delle misure di minimizzazione, integrità e disponibilità dei dati.
- Altre implementazioni tecniche per migliorare la Sicurezza: Abilitazione obbligatoria 2FA (Cellulare o Email), Aggiungere dispositivi affidabili, Abilitazione con PassKey, Limitare i tentativi di login (Rate Limiting) - (3 tentativi/min), Limitare la durata del trusted device -> 90 giorni - massimo consigliabile

3. Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

4. Motivazione della mancata richiesta del parere degli interessati

La natura tecnica e organizzativa del trattamento, nonché il tipo di dati trattati (principalmente per finalità di cura o per l'esecuzione di obblighi contrattuali), non ha reso obbligatorio o utile un coinvolgimento diretto preventivo degli interessati in questa fase di valutazione.

Tuttavia, i diritti degli interessati sono garantiti attraverso:

- una informativa trasparente e aggiornata disponibile sulla piattaforma;
- strumenti digitali di esercizio dei diritti (rettifica, cancellazione, limitazione, opposizione);
- un canale diretto di contatto con il DPO, indicato nell'informativa.

Sezione 1

Panoramica del trattamento

5. Qual è il trattamento in considerazione?

Il trattamento in esame riguarda l'utilizzo della piattaforma digitale PQRST, gestita da IPSG Srl, per l'erogazione di servizi di telerefertazione medica a distanza, attraverso il caricamento di documentazione sanitaria da parte di un medico inviante e la successiva refertazione da parte di un medico refertatore.

Finalità del trattamento:

- Garantire la corretta esecuzione della prestazione sanitaria a favore del paziente (finalità di cura);
- Consentire l'accesso, la trasmissione e la conservazione di referti medici in ambiente digitale sicuro;
- Supportare la gestione organizzativa, tecnica e documentale del servizio da parte della piattaforma.

Contesto di utilizzo:

- Piattaforma cloud-based accessibile via web;
- Utenti della piattaforma: medici regolarmente abilitati (in qualità di titolari autonomi del trattamento per finalità di cura);
- IPSG agisce come responsabile del trattamento per conto dei medici in relazione alla gestione tecnico-infrastrutturale (hosting, archiviazione, sicurezza, logging).

Risultati attesi:

- Refertazione efficace, sicura e tracciabile;
- Conservazione digitale conforme dei referti;
- Riduzione degli errori operativi nella trasmissione e gestione dei documenti;
- Trasparenza nei ruoli privacy, nel rispetto del Regolamento UE 2016/679.

6. Quali sono le responsabilità connesse al trattamento?

A. **Responsabilità di IPSG come TITOLARE (per dati dei medici utenti della piattaforma)**

Responsabilità principali:

- Informare i medici utenti sulla raccolta dei loro dati (art. 13 GDPR).
- Stipulare contratti con i medici per definire le finalità del trattamento (creazione account, gestione accessi, supporto).
- Gestire i dati di navigazione e comunicazione (cookie, e-mail, log).
- Proteggere i sistemi e le credenziali di accesso.
- Designare un DPO
- Predisporre procedure in caso di data breach.

Rischi:

- Uso illecito dei dati per finalità non previste (es. marketing non autorizzato)
- Violazioni informatiche (es. attacchi ai server)
- Responsabilità verso l'autorità garante in caso di inadempienze

B. **Responsabilità di IPSG come RESPONSABILE del trattamento (per dati dei pazienti)**

Responsabilità principali (ex art. 28.3 GDPR):

- Trattare i dati solo su istruzioni documentate del medico.
- Implementare misure tecniche e organizzative adeguate (art. 32 GDPR).
- Evitare qualsiasi uso autonomo dei dati.
- Garantire la riservatezza del personale autorizzato al trattamento.
- Collaborare con il medico in caso di ispezioni o richieste degli interessati.
- Notificare al medico ogni *data breach* che coinvolga dati trattati per suo conto.
- Fornire garanzie documentate (audit, log, procedure).
- Consentire e agevolare ispezioni da parte del titolare (medico).

Rischi:

- Superamento del perimetro di responsabilità (uso improprio dei dati)
- Inadeguatezza tecnica nel trattamento (es. backup insufficienti, mancata cifratura)
- Responsabilità solidale con il medico in caso di danni al paziente

C. **Responsabilità del medico (TITOLARE del trattamento per finalità di cura)**

Responsabilità principali:

- Informare i pazienti ai sensi dell'art. 13 GDPR (tramite informativa specifica).
- Raccogliere e documentare il consenso informato alla prestazione sanitaria (non al trattamento).
- Trattare i dati solo per finalità sanitarie lecite e proporzionate (cura, diagnosi).
- Garantire la sicurezza e riservatezza dei dati (art. 32 GDPR).
- Registrare i trattamenti nel proprio registro (art. 30 GDPR).
- Gestire le richieste di esercizio dei diritti da parte dei pazienti (accesso, rettifica, cancellazione, ecc.).
- Valutare i fornitori (es. la piattaforma) e stipulare un contratto conforme all'art. 28 GDPR se usano IPSG per attività delegate.

Rischi:

- Violazione della riservatezza dei dati sensibili
- Responsabilità civile in caso di trattamento scorretto o dannoso
- Mancato rispetto dei diritti del paziente
- Responsabilità penale e disciplinare (art. 75 ss. Codice Privacy, deontologia medica)

7. Ci sono standard applicabili al trattamento?

Linee guida del Garante Privacy (marzo 2024): *"Compendio sul trattamento dei dati personali attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari"*

Dati, processi e risorse di supporto

8. Quali sono i dati trattati?

1. **Dati identificativi degli Utenti Medici (caricatori e refertatori):**
   - Nome, cognome, codice fiscale, e-mail, indirizzo di residenza o studio, numero di iscrizione all'Ordine.
   - **Finalità:** registrazione, gestione contrattuale, fatturazione, accesso alla piattaforma.
   - **Periodo di conservazione:** 10 anni dalla cessazione del rapporto.
   - **Accesso:** personale autorizzato IPSG, amministratori di sistema, provider cloud.
2. **Dati identificativi dei Pazienti:**
   - Nome, cognome, codice fiscale, data di nascita, sesso.
   - **Finalità:** identificazione del paziente per finalità di cura.
   - **Periodo di conservazione:** sino al termine del rapporto contrattuale con il medico (salvo diverse istruzioni del medico titolare)
   - **Accesso:** medico refertatore, medico inviante, IPSG (come responsabile tecnico su istruzione), provider cloud.
3. **Dati sulla salute del Paziente:**
   - Documentazione sanitaria, immagini diagnostiche, referti, eventuali note mediche.
   - **Finalità:** refertazione medica per finalità di diagnosi e cura.
   - **Periodo di conservazione:** sino al termine del rapporto contrattuale con il medico (salvo diverse istruzioni del medico titolare)
   - **Accesso:** medico refertatore, medico inviante, IPSG per mera conservazione tecnica (responsabile), provider cloud.
4. **Log di accesso e dati tecnici di navigazione:**

   Accesso: personale IT autorizzato IPSG, provider cloud.

   A) Log di Autenticazione e Sicurezza

   Categoria di dati:

   Accessi: Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Metodo di login (password, OTP, MFA), Esito (successo/fallito), Motivo fallimento (es. credenziali errate, OTP scaduta, utente disabilitato)

   Sessioni (Timestamp, Creazione della sessione, Durata sessione, Logout manuale o scadenza automatica)

   Protezione account (Timestamp, Reset password richiesto/completato, Modifica email/telefono 2FA, Notifica se un dispositivo viene rimosso, Log di sicurezza con IP e device name, Controllo per Brute-force (Es. login da Paesi non abituali), Motivo Blocco IP (es. credenziali errate, OTP scaduta, utente disabilitato)

Finalità: garantire la sicurezza della piattaforma e dei dati trattati, prevenire e rilevare accessi non autorizzati o utilizzi illeciti, assicurare l'integrità dei sistemi informativi, (security monitoring & incident response) ai sensi dell'art. 32 GDPR e del Considerando 49.
Base giuridica: legittimo interesse del titolare/responsabile alla sicurezza delle reti e dei sistemi; adempimento degli obblighi di sicurezza previsti dal GDPR.
Tempo di conservazione: 12 mesi dalla registrazione, fatti salvi ulteriori periodi di conservazione in caso di incidenti di sicurezza o contenzioso, per il tempo strettamente necessario alla relativa gestione.

B) Log di Creazione dei Dati (Caricamento)

Caricamento file (Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Nome file caricato, Dispositivo utilizzato (browser/app)

C) Log di Creazione / Cancellazione dei Referti

Creazione referto (Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Medico responsabile, Paziente, Dispositivo utilizzato (browser/app)

D) Firma / Firma Digitale (Timestamp, Firma digitale, ID utente (medico, infermiere, centro, admin), IP di origine, Esito (successo/fallito), Motivo fallimento (es. credenziali errate, OTP scaduta, utente disabilitato)

E) Cancellazione (Timestamp, Utente che ha Eliminato il File, ID utente (medico, infermiere, studio, centro), IP di origine, motivazione)

Finalità: documentare la tracciabilità completa del processo di refertazione, garantire l'integrità e l'autenticità dei referti e delle firme apposte, consentire a IPSG di accertare le responsabilità in caso di errori (ad es. caricamento di un referto non corrispondente al tracciato originario) e di difendersi in sede giudiziaria.

Base giuridica: esecuzione del rapporto contrattuale tra IPSG e i professionisti coinvolti nella refertazione, legittimo interesse del titolare/responsabile (art. 6, par. 1, lett. f GDPR) alla tutela dei propri diritti in caso di contestazioni, art. 9, par. 2, lett. f GDPR (accertamento, esercizio o difesa di un diritto in sede giudiziaria).

Tempo di conservazione: 10 anni dalla data dell'operazione, fatti salvi ulteriori periodi di conservazione in caso di incidenti di sicurezza o contenzioso.

9. Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

1. Raccolta (Collect)

Chi raccoglie:

- *Medico titolare* → raccoglie i dati sanitari del paziente
- *IPSG (PQRST)* → raccoglie dati personali per creazione account medico (es. e-mail, nome, ruolo)

Dati raccolti:

- *Dati sanitari del paziente* (referti, immagini, diagnosi)
- *Dati identificativi del medico*

2. Archiviazione (Store)

Chi conserva:

- *IPSG* (Responsabile del trattamento per i dati sanitari; Titolare per i dati degli utenti/medici)

Dove:

- Cloud/server (specificare nel registro dei trattamenti) La piattaforma è ubicata su server situato presso AWS EC2, nel data center di Francoforte (Germania).Il Backup automatico settimanale e mensile in cloud viene eseguito su server ubicati in Germania e di proprietà di Hetzner.

Dati conservati:

- Referti sanitari, account medici

3. Utilizzo (Use / Process)

Chi utilizza:

- *Medico titolare* → per leggere, analizzare, refertare
- *IPSG* → per gestire la piattaforma, assegnare referti, inviare notifiche

Operazioni:

- Refertazione
- Consultazione dei documenti
- Comunicazioni operative tra medici
- Notifiche all'utente

4. Trasferimento (Transfer)

Chi trasferisce:
Medico refertatore → carica il referto sulla piattaforma, rendendolo accessibile al medico caricatore;

Medico caricatore → carica i dati sanitari del paziente per la refertazione;

IPSG → fornisce l'infrastruttura tecnologica che consente il trasferimento dei dati tra gli utenti abilitati (senza accedere direttamente ai contenuti).

Dati trasferiti:

- Immagini diagnostiche, Referti PDF.

Destinatari:

- Altro medico (invio peer-to-peer)
- Paziente (tramite il medico)

5. Cancellazione (Delete)

Chi cancella:

- *IPSG* su richiesta o decorrenza termini
- *Medico* su richiesta o secondo le regole deontologiche della propria professione

Dati cancellati:

- Referti e documenti scaduti o non più necessari
- Account inattivi su richiesta

10. Quali sono le risorse di supporto ai dati?

I dati personali trattati tramite la piattaforma PQRST sono supportati dalle seguenti risorse:

- **Server cloud dedicati** localizzati nell'Unione Europea, dotati di backup periodici e crittografia a riposo e in transito;
- **Software di gestione piattaforma PQRST**, sviluppato su architettura web-based con accesso riservato tramite credenziali personali e tracciamento degli accessi;
- **Database relazionali** gestiti attraverso sistemi di gestione (DBMS) sicuri e aggiornati, protetti da firewall e meccanismi di controllo accessi;
- **Sistemi operativi** (Linux) configurati secondo best practice di sicurezza (patch management, account privilegiati separati);
- **Rete HTTPS** cifrata con certificati SSL/TLS per tutte le comunicazioni tra client e server;
- **Personale autorizzato**: solo il personale tecnico di IPSG (in qualità di responsabile del trattamento) e i medici utenti della piattaforma (titolari del trattamento) possono accedere ai dati, nei limiti delle rispettive autorizzazioni;
- **Procedure organizzative** per il controllo accessi, la gestione dei ruoli e la minimizzazione dei dati;
- **Supporti digitali**: non è previsto l'uso di supporti cartacei per la gestione ordinaria dei dati trattati dalla piattaforma.

Sezione II

Principi Fondamentali

Proporzionalità e necessità

11. Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono **specifici, espliciti e legittimi**, in conformità agli articoli 5 e 6 del Regolamento (UE) 2016/679 (GDPR). In particolare:

- Il trattamento è finalizzato alla **prestazione di servizi sanitari da parte di professionisti abilitati**, attraverso l'uso della piattaforma digitale PQRST, con modalità di telerefertazione e gestione dei referti.
- Le finalità sono **esplicitamente indicate** nelle Condizioni Generali d'Uso e nell'Informativa Privacy, accessibili e accettate dall'utente all'atto della registrazione.
- **Il trattamento per finalità di cura** da parte dei medici è fondato sull'art. 9.2.h del GDPR, e quindi **non richiede consenso**, rientrando tra le basi giuridiche legittime e necessarie.
- **Il trattamento effettuato da IPSG** (in qualità di **responsabile del trattamento**) è finalizzato esclusivamente all'**erogazione del servizio tecnico e amministrativo**, secondo le istruzioni fornite dai medici titolari.
- I dati non sono trattati per finalità ulteriori incompatibili con quelle dichiarate.

12. Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento dei dati personali svolto tramite la piattaforma PQRST si fonda su diverse basi giuridiche previste dagli articoli 6 e 9 del Regolamento (UE) 2016/679 (GDPR), a seconda della tipologia di dati e dei soggetti coinvolti:

1. Trattamento dati comuni (utente medico):

- **Art. 6, par. 1, lett. b)** GDPR: **esecuzione di un contratto** di servizi digitali tra IPSG e l'utente registrato (medico inviante o refertatore).
- **Art. 6, par. 1, lett. c)** GDPR: **adempimento di obblighi legali**, come obblighi fiscali e di conservazione dei dati.
- **Art. 6, par. 1, lett. f)** GDPR: **legittimo interesse del titolare** per garantire il corretto funzionamento della piattaforma e la sicurezza dei dati.

2. Trattamento dati sanitari (pazienti):

- **Art. 9, par. 2, lett. h)** GDPR: **finalità di cura medica** da parte di professionisti sanitari soggetti al segreto professionale. In questo caso, il medico agisce come titolare autonomo del trattamento e non è richiesto il consenso.
- IPSG, che supporta il medico nella **gestione tecnica e amministrativa dei dati sanitari** (es. conservazione, accesso, organizzazione), agisce come **responsabile del trattamento** ai sensi dell'art. 28 GDPR.

13. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

I dati raccolti sono adeguati, pertinenti e limitati rispetto alle finalità per cui sono trattati, in conformità al principio di minimizzazione di cui all'art. 5, par. 1, lett. c) GDPR.

Nel dettaglio:

Dati dei medici (utenti registrati)

- Dati identificativi e di contatto (es. nome, cognome, email, numero di iscrizione all'Albo): necessari per l'esecuzione del contratto di servizi digitali, la corretta identificazione professionale, le comunicazioni e l'accesso alla piattaforma.
- Dati fiscali (es. P. IVA, codice fiscale): richiesti per l'emissione di fatture e adempimenti di legge.
- Documentazione professionale (es. certificazioni, abilitazioni): raccolta necessaria per validare la qualifica professionale e garantire la sicurezza e affidabilità dei servizi erogati tramite la piattaforma.

Dati dei pazienti (oggetto di refertazione)

- Dati identificativi e anagrafici: necessari per associare correttamente il referto alla persona interessata e per l'esecuzione della prestazione medica.
- Dati sanitari (es. immagini diagnostiche, sintomatologia, anamnesi): raccolti e trattati unicamente per finalità di diagnosi e cura, nel rispetto del principio di necessità, e solo per le informazioni indispensabili alla prestazione richiesta.

Dati di utilizzo della piattaforma

- Dati di accesso/log di sistema: raccolti per garantire la sicurezza informatica, la tracciabilità delle operazioni e la corretta erogazione del servizio.

Nessun dato superfluo o non pertinente viene raccolto o conservato oltre il tempo necessario per le finalità dichiarate.

14. I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati.
Le misure previste per garantire l'esattezza e l'aggiornamento dei dati includono:

- Responsabilità diretta del medico titolare del trattamento nell'inserimento corretto e nella verifica delle informazioni sanitarie dei pazienti, in conformità alle proprie obbligazioni professionali.
- Controlli tecnici della piattaforma, che impediscono l'uso di formati errati o l'invio di documenti incompleti.
- Possibilità di richiesta di rettifica da parte dell'interessato, secondo quanto previsto dagli artt. 16 e 19 GDPR.

15. Qual è il periodo di conservazione dei dati?

5. **Dati identificativi degli Utenti Medici (caricatori e refertatori):**
   - Nome, cognome, codice fiscale, e-mail, indirizzo di residenza o studio, numero di iscrizione all'Ordine.
   - **Finalità:** registrazione, gestione contrattuale, fatturazione, accesso alla piattaforma.
   - **Periodo di conservazione:** 10 anni dalla cessazione del rapporto.
   - **Accesso:** personale autorizzato IPSG, amministratori di sistema, provider cloud.
6. **Dati identificativi dei Pazienti:**
   - Nome, cognome, codice fiscale, data di nascita, sesso.
   - **Finalità:** identificazione del paziente per finalità di cura.
   - **Periodo di conservazione:** sino al termine del rapporto contrattuale con il medico (salvo diverse istruzioni del medico titolare)
   - **Accesso:** medico refertatore, medico inviante, IPSG (come responsabile tecnico su istruzione), provider cloud.
7. **Dati sulla salute del Paziente:**
   - Documentazione sanitaria, immagini diagnostiche, referti, eventuali note mediche.
   - **Finalità:** refertazione medica per finalità di diagnosi e cura.
   - **Periodo di conservazione:** sino al termine del rapporto contrattuale con il medico (salvo diverse istruzioni del medico titolare)
   - **Accesso:** medico refertatore, medico inviante, IPSG per mera conservazione tecnica (responsabile), provider cloud.
8. **Log di accesso e dati tecnici di navigazione:**

   Accesso: personale IT autorizzato IPSG, provider cloud.

   A) Log di Autenticazione e Sicurezza

   Categoria di dati:

   Accessi: Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Metodo di login (password, OTP, MFA), Esito (successo/fallito), Motivo fallimento (es. credenziali errate, OTP scaduta, utente disabilitato)

   Sessioni (Timestamp, Creazione della sessione, Durata sessione, Logout manuale o scadenza automatica)

   Protezione account (Timestamp, Reset password richiesto/completato, Modifica email/telefono 2FA, Notifica se un dispositivo viene rimosso, Log di sicurezza con IP e device name, Controllo per Brute-force (Es. login da Paesi non abituali), Motivo Blocco IP (es. credenziali errate, OTP scaduta, utente disabilitato)

   Finalità: garantire la sicurezza della piattaforma e dei dati trattati, prevenire e rilevare accessi non autorizzati o utilizzi illeciti, assicurare l'integrità dei sistemi informativi, (security monitoring &

incident response) ai sensi dell'art. 32 GDPR e del Considerando 49. **Base giuridica:** legittimo interesse del titolare/responsabile alla sicurezza delle reti e dei sistemi; adempimento degli obblighi di sicurezza previsti dal GDPR. **Tempo di conservazione:** 12 mesi dalla registrazione, fatti salvi ulteriori periodi di conservazione in caso di incidenti di sicurezza o contenzioso, per il tempo strettamente necessario alla relativa gestione.

B) Log di Creazione dei Dati (Caricamento)

Caricamento file (Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Nome file caricato, Dispositivo utilizzato (browser/app)

C) Log di Creazione / Cancellazione dei Referti

Creazione referto (Timestamp, ID utente (medico, infermiere, centro, admin), IP di origine, Medico responsabile, Paziente, Dispositivo utilizzato (browser/app)

D) Firma / Firma Digitale (Timestamp, Firma digitale, ID utente (medico, infermiere, centro, admin), IP di origine, Esito (successo/fallito), Motivo fallimento (es. credenziali errate, OTP scaduta, utente disabilitato)

E) Cancellazione (Timestamp, Utente che ha Eliminato il File, ID utente (medico, infermiere, studio, centro), IP di origine, motivazione)

Finalità: documentare la tracciabilità completa del processo di refertazione, garantire l'integrità e l'autenticità dei referti e delle firme apposte, consentire a IPSG di accertare le responsabilità in caso di errori (ad es. caricamento di un referto non corrispondente al tracciato originario) e di difendersi in sede giudiziaria.

Base giuridica: esecuzione del rapporto contrattuale tra IPSG e i professionisti coinvolti nella refertazione, legittimo interesse del titolare/responsabile (art. 6, par. 1, lett. f GDPR) alla tutela dei propri diritti in caso di contestazioni, art. 9, par. 2, lett. f GDPR (accertamento, esercizio o difesa di un diritto in sede giudiziaria).

Tempo di conservazione: 10 anni dalla data dell'operazione, fatti salvi ulteriori periodi di conservazione in caso di incidenti di sicurezza o contenzioso.

Misure a tutela dei diritti degli interessati

16. Come sono informati del trattamento gli interessati?

Gli interessati sono informati del trattamento dei propri dati personali attraverso:

- Informativa privacy dedicata, fornita dal medico titolare del trattamento in fase di acquisizione del consenso informato o in occasione della visita/refertazione.
- Sezione informativa accessibile dalla piattaforma PQRST, contenente anche riferimenti ai ruoli privacy e alle responsabilità dei diversi soggetti.

L'informativa è redatta in linguaggio chiaro, comprensibile, e conforme all'art. 13 GDPR.

17. Come si ottiene il consenso degli interessati?

Il trattamento dei dati sanitari per finalità di cura (refertazione) non richiede consenso, in quanto fondato sull'art. 9.2.h GDPR (finalità di medicina, diagnosi e trattamento da parte di professionisti soggetti a segreto professionale).

Il consenso è invece richiesto per:

- Trattamenti ulteriori (es. promozione, profilazione, invio newsletter)

In tali casi, il consenso è:
- Esplicito e documentato
- Raccolto con flag separati ("punta e clicca") per ciascuna finalità
- Registrato e tracciato a sistema

18. Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati possono esercitare i propri diritti in diversi modi:
- Contattando direttamente il medico titolare del trattamento (caricatore o refertatore), che ha l'obbligo di rispondere alle richieste ai sensi degli artt. 15–20 GDPR.
- Utilizzando gli strumenti messi a disposizione dalla piattaforma, quali indirizzo e-mail privacy@ippocrateshop.com
- Su richiesta, il paziente può ricevere copia elettronica dei propri dati in formato interoperabile.

La piattaforma garantisce agli interessati la tracciabilità e l'accesso riservato e sicuro tramite area personale o supporto tecnico.

19. Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Il diritto di rettifica può essere esercitato rivolgendosi direttamente al medico titolare del trattamento, che valuta l'aggiornamento o la correzione del referto o dei dati anagrafici secondo le regole deontologiche e sanitarie.

Il diritto di cancellazione può essere esercitato nei limiti previsti dall'art. 17 GDPR, compatibilmente con gli obblighi di conservazione sanitaria e medico-legale.

L'interessato può inviare una richiesta al titolare o, se previsto, al DPO del titolare (medico o struttura), oppure utilizzare un apposito canale segnalato nella privacy policy

La piattaforma fornisce assistenza come responsabile del trattamento per garantire il corretto inoltro e tracciamento delle richieste.

20. Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare i diritti previsti dagli artt. 18 e 21 GDPR (limitazione e opposizione al trattamento mediante richiesta scritta al medico titolare del trattamento (caricatore o refertatore), o utilizzando i contatti forniti nell'informativa privacy.

Qualora IPSG agisca come responsabile, la piattaforma garantisce il supporto tecnico per la gestione della richiesta, che verrà inoltrata al titolare.

21. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Sì, IPSG Srl agisce come responsabile del trattamento ai sensi dell'art. 28 GDPR, su designazione dei medici titolari (caricatori o refertatori).

La designazione è formalizzata mediante contratto di designazione ex art. 28 GDPR, con specifica delle istruzioni fornite dal titolare, ambiti di trattamento, misure di sicurezza da adottare, obbligo di riservatezza, e obblighi in caso di data breach
Il contratto prevede l'obbligo per IPSG di:

- trattare i dati solo su istruzione documentata del titolare
- garantire riservatezza, sicurezza e tracciabilità
- assistere il titolare nell'adempimento dei suoi obblighi verso l'interessato
- cancellare o restituire i dati a fine rapporto.

Attualmente non si fa uso di codici di condotta o certificazioni ufficiali, ma l'adeguatezza contrattuale è garantita tramite revisione legale personalizzata.

22. In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Ad oggi, non è previsto il trasferimento sistematico di dati verso Paesi extra-UE.
Tuttavia, ove vi siano strumenti tecnici utilizzati da IPSG o dai medici titolari che comportino il trattamento in Paesi terzi (es. servizi cloud, e-mail, strumenti di backup), si garantisce che:

- Tali fornitori abbiano sede in Paesi con decisione di adeguatezza della Commissione UE

oppure

- Siano adottate Clausole Contrattuali Standard (SCC) approvate dalla Commissione
- Venga effettuata, se necessario, una valutazione di impatto sui trasferimenti (TIA)

Gli strumenti utilizzati sono selezionati sulla base della garanzia di adeguatezza, sicurezza e compliance con il GDPR, conformemente agli artt. 44–49 GDPR.

Sezione III

Rischi

Misure esistenti o pianificate

23. Contratto con il Responsabile del Trattamento

IPSG è Responsabile del Trattamento per conto dei medici titolari. I contratti art. 28 GDPR sono stipulati con i medici e definiscono:

- le istruzioni documentate del titolare,
- le finalità del trattamento,
- l'ambito dei dati trattati,
- gli obblighi di sicurezza, cancellazione, restituzione,
- la tracciabilità delle operazioni e degli accessi.

24. Controllo degli accessi logici

Accessi differenziati su base ruolo (refertatori, caricatori, amministratori), tramite credenziali personali, 2FA opzionale.

Registrazione e tracciabilità degli accessi.

L'accesso alla piattaforma è consentito esclusivamente previa autenticazione dell'utente (medico o paziente) tramite email e password robuste, definite secondo policy aziendali (lunghezza minima 8 caratteri, alfanumerica, con caratteri speciali e maiuscole/minuscole).

È inoltre prevista la scadenza automatica delle password ogni 90 giorni, con obbligo di aggiornamento da parte dell'utente.

Il sistema si basa sulle funzionalità offerte dal framework Laravel, che utilizza un sistema di autenticazione strutturato su "guardie" e "provider", per autenticare ogni richiesta e gestire il recupero degli utenti da database in modo sicuro.

Le chiamate effettuate dal browser al server sono protette da meccanismi anti-impersonificazione, previsti nativamente da Laravel.

25. Sicurezza dei canali informatici, crittografia e protezione dei file

Utilizzo di HTTPS, firewall, monitoraggio server, aggiornamenti software regolari, protezione da accessi non autorizzati tramite VPN. Piattaforma ospitata su server con data center in UE certificati ISO 27001.

I file caricati dall'utente vengono inizialmente inviati a una cartella temporanea, dalla quale vengono poi spostati tramite cron job (script automatico) in una cartella dedicata all'utente all'interno del server.

Tale cartella non è accessibile direttamente, ma solo tramite chiamata autenticata al server, che applica i protocolli di sicurezza previsti dal framework Laravel.

I file vengono rinominati in modo cifrato utilizzando algoritmi di hashing, rendendoli non riconoscibili senza interrogare il database.

Laravel adotta meccanismi di crittografia AES-256/AES-128 con firma MAC, garantendo l'integrità e la riservatezza dei dati cifrati.

26. Archiviazione

I referti sono conservati su servizio S3 di AWS, accessibili solo ai profili autorizzati.
I referti sono consultabili dai medici titolari secondo le modalità contrattuali.

È previsto un sistema di cancellazione alla cessazione dei termini di conservazione o su istruzione del titolare.

27. Tracciabilità

Log di accesso ai documenti, modifica, download, consultazione.

Ogni referto è tracciato con data, utente, IP.

Eventuali anomalie sono rilevate tramite alert automatici e conservate in log di sicurezza.

Ogni richiesta di accesso, modifica o download dei file è registrata lato server e soggetta ai controlli Laravel, garantendo la tracciabilità delle operazioni.

Non è prevista archiviazione locale o generalizzata dei file sui dispositivi degli utenti: i file risiedono esclusivamente sul server e sono scaricabili solo previa autenticazione e autorizzazione, riducendo i rischi di dispersione dei dati.

28. Lotta contro il malware

Antivirus aggiornato lato server e postazioni, scansioni automatiche, whitelist delle applicazioni.

Sistema di monitoraggio attivo contro exploit e attacchi esterni.

29. Backup

Backup incrementali quotidiani, full settimanali, conservati in data center separati.

Procedure di *restore* testate periodicamente.

Backup cifrati.

30. Gestione dei terzi che accedono ai dati

Tutti i subfornitori cloud/hosting sono stati selezionati con DPA (Data Processing Agreement).

Controllo accessi amministratori cloud documentato

Laravel Hash consente l'hashing sicuro delle password (algoritmi Bcrypt e Argon2).
L'accesso al gestionale avviene solo tramite credenziali univoche, con sessioni gestite in conformità agli standard di sicurezza..

Nessun accesso da parte di soggetti non autorizzati.

31. Gestione del personale

Personale tecnico formato sulle policy di protezione dati e vincolato alla riservatezza.

Sessioni periodiche di aggiornamento e circolari informative.

Accesso solo ai dati necessari allo svolgimento delle mansioni.

32. Gestione delle politiche di tutela della privacy

Manuale interno aggiornato, con ruoli privacy, mappatura dei trattamenti, policy su data breach, esercizio dei diritti, tempi di conservazione, DPIA e registro trattamenti.

33. Minimizzazione dei dati

Per ciascun modulo di raccolta dati (medici, pazienti, utenti della piattaforma), è stato effettuato un audit preliminare per identificare e mantenere solo i campi strettamente necessari per la finalità dichiarata (es. per la refertazione: dati anagrafici minimi, esami caricati, output del referto).

I campi facoltativi sono evidenziati e non obbligatori; la piattaforma prevede l'uso di valori "non comunicato" laddove l'informazione non sia indispensabile.

È implementata la pseudonimizzazione (o altri meccanismi di riduzione di identificabilità) nella fase di archivio o analisi dei dati secondari non legati all'immediata cura, per ridurre l'identificabilità della persona senza pregiudicare la funzionalità clinica.

L'accesso ai dati è configurato con profili di minima autorizzazione ("least privilege"), in modo che ciascun soggetto (medico inviante, refertatore, amministratore tecnico) veda solo i dati necessari per la propria prestazione.

I log di attività e archivi storici sono conservati in forma aggregata o anonimizzata ove possibile, per evitare che i processi di audit o analisi operativa comportino la visibilità di dati identificativi non necessari.

È prevista una revisione periodica (annuale o biennale) del dataset detenuto: in occasione della revisione si valuta l'effettiva necessità degli archivi ancora attivi, si anonimizzano o cancellano i dati non più indispensabili in base alla finalità o agli obblighi di legge.

Il sistema è progettato secondo il principio di "privacy by default" e "privacy by design": le impostazioni predefinite raccolgono il minimo indispensabile, e nell'implementazione di nuove funzionalità la minimizzazione è considerata fin dalla fase di progettazione.

34. Politica di tutela della privacy

IPSG ha adottato una politica di tutela della privacy ispirata ai principi del Regolamento UE 2016/679 (GDPR), basata sull'approccio del "privacy by design e by default".
L'organizzazione interna prevede:

- Una figura di referente privacy con funzioni di coordinamento delle attività di compliance, anche se attualmente non è stato designato un DPO in quanto non ritenuto obbligatorio (v. art. 37 GDPR, valutazione in corso).
- Una mappatura documentata dei trattamenti e dei relativi flussi di dati, mantenuta aggiornata.
- Procedure interne per la valutazione dell'impatto privacy di nuovi progetti (es. nuove funzionalità della piattaforma).
- Attività periodiche di audit interni e aggiornamento formativo rivolti al personale coinvolto nella gestione dei dati, inclusi medici e amministratori tecnici.
- Registri dei trattamenti aggiornati e mantenuti in formato elettronico.
- Uso di strumenti contrattuali con clausole privacy rafforzate per tutti i fornitori e soggetti terzi (ex art. 28 GDPR).

L'obiettivo è garantire un equilibrio tra le esigenze operative della piattaforma e la protezione dei diritti fondamentali degli interessati.

35. Gestione dei rischi

La gestione dei rischi privacy è integrata nei processi operativi della piattaforma e segue un modello ciclico di identificazione, valutazione e mitigazione dei rischi.
Le principali attività previste sono:
- Mappatura preventiva dei rischi connessi ai trattamenti di dati sanitari, dati di contatto, dati di pagamento, e dati tecnici di accesso alla piattaforma.
- Valutazioni di impatto (DPIA) per i trattamenti potenzialmente ad alto rischio, come la refertazione a distanza e l'accesso multiutente da parte di più professionisti sanitari.
- Controlli tecnici e organizzativi sulla sicurezza, documentati e riesaminati regolarmente (es. backup, crittografia, tracciabilità degli accessi, controllo accessi profilati).
- Monitoraggio delle violazioni dei dati (data breach) attraverso log di sistema e un sistema interno di segnalazione, con procedure definite per la notifica al Garante.

Accesso illegittimo ai dati

36. Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

- Dati sanitari: violazione della privacy medica, esposizione a discriminazioni o pregiudizi (es. lavorativi, assicurativi), danni psicologici legati alla perdita di riservatezza su condizioni di salute.
- Dati di contatto/pagamento: furto d'identità, uso fraudolento dei dati, truffe, phishing.
- Dati tecnici di accesso: accessi non autorizzati all'account, manipolazione o cancellazione dei referti.

37. Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Accesso non autorizzato da parte di personale interno (es. uso improprio degli account amministrativi).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).

38. Quali sono le fonti di rischio?

- Fonti interne: personale tecnico o medico con accessi privilegiati non sufficientemente tracciati/formati.
- Fonti esterne: attori malevoli (hacker), soggetti interessati a ottenere dati sanitari sensibili per fini economici o reputazionali.
- Fonti non umane: malfunzionamenti dei sistemi, bug nel software, configurazioni errate, mancanza di crittografia o backup.

39. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Contratto con il responsabile del trattamento, Tracciabilità, Gestione dei rischi, Backup, Controllo degli accessi logici, Gestione delle politiche di tutela della privacy

40. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante

Anche se le misure tecniche e organizzative pianificate (autenticazione a due fattori, segregazione degli accessi, logging, crittografia, contratti ex art. 28 GDPR) mitigano significativamente il rischio, resta elevata l'intensità dell'impatto potenziale in caso di evento avverso, soprattutto per i dati di natura sensibile trattati.

41. Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata

Tuttavia, restano rischi residuali legati a errore umano, configurazioni errate, attacchi esterni sofisticati.

Le vulnerabilità non sono strutturali e non vi è un'esposizione elevata al pubblico.

La probabilità non è nulla, ma moderatamente bassa.

Modifiche indesiderate dei dati

42. Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

- **Dati sanitari:** violazione della privacy medica, esposizione a discriminazioni o pregiudizi (es. lavorativi, assicurativi), danni psicologici legati alla perdita di riservatezza su condizioni di salute.
- **Dati di contatto/pagamento: furto** d'identità, uso fraudolento dei dati, truffe, phishing.
- **Dati tecnici di accesso:** accessi non autorizzati all'account, manipolazione o cancellazione dei referti.

43. Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

- Accesso non autorizzato da parte di personale interno (es. uso improprio degli account amministrativi).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).

44. Quali sono le fonti di rischio?

- Fonti esterne: attori malevoli (hacker), soggetti interessati a ottenere dati sanitari sensibili per fini economici o reputazionali.
- Fonti non umane: malfunzionamenti dei sistemi, bug nel software, configurazioni errate, mancanza di crittografia o backup.
- Fonti interne: personale tecnico o medico con accessi privilegiati non sufficientemente tracciati/formati.

45. Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Controllo degli accessi logici
- Tracciabilità
- Sicurezza dei canali informatici
- Gestione dei terzi che accedono ai dati
- Gestione del personale
- Minimizzazione dei dati
- Politica di tutela della privacy
- Gestione dei rischi
- Gestione delle politiche di tutela della privacy

46. Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante

L'alterazione dei dati sanitari può avere impatti rilevanti sulla salute dei pazienti, sulla responsabilità medico-legale e sulla reputazione della piattaforma.
Le misure di controllo previste mitigano in parte, ma non annullano, l'impatto in caso di evento.

47. Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata

Il sistema prevede già misure strutturali (profilazione, audit, backup, log) che riducono la probabilità di modifiche non tracciate o fraudolente.
Tuttavia, l'intervento umano (es. errore medico, uso improprio dell'account) e le vulnerabilità informatiche restano possibili.

Perdita di dati

48. Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

- Dati di contatto/pagamento: furto d'identità, uso fraudolento dei dati, truffe, phishing.
- Dati sanitari: violazione della privacy medica, esposizione a discriminazioni o pregiudizi (es. lavorativi, assicurativi), danni psicologici legati alla perdita di riservatezza su condizioni di salute.
- Dati tecnici di accesso: accessi non autorizzati all'account, manipolazione o cancellazione dei referti.

49. Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

- Accesso non autorizzato da parte di personale interno (es. uso improprio degli account amministrativi).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).
- Attacchi informatici esterni (es. brute force, malware, phishing, esfiltrazione).
- Errori umani nella gestione dei permessi (es. errata assegnazione di privilegi di accesso).
- Utilizzo condiviso o non sicuro di credenziali (es. tra medici o personale non autorizzato).

50. Quali sono le fonti di rischio?

- Fonti esterne: attori malevoli (hacker), soggetti interessati a ottenere dati sanitari sensibili per fini economici o reputazionali.
- Fonti non umane: malfunzionamenti dei sistemi, bug nel software, configurazioni errate, mancanza di crittografia o backup.
- Fonti interne: personale tecnico o medico con accessi privilegiati non sufficientemente tracciati/formati.

51. Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

- Contratto con il responsabile del trattamento
- Controllo degli accessi logici,
- Sicurezza dei canali informatici,
- Tracciabilità,
- Gestione dei terzi che accedono ai dati,
- Gestione delle politiche di tutela della privacy,
- Gestione del personale,
- Gestione dei rischi,
- Minimizzazione dei dati,
- Politica di tutela della privacy

52. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante

L'alterazione dei dati sanitari può avere impatti rilevanti sulla salute dei pazienti, sulla responsabilità medico-legale e sulla reputazione della piattaforma. Le misure di controllo previste mitigano in parte, ma non annullano, l'impatto in caso di evento.

53. Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata

Il sistema prevede già misure strutturali (profilazione, audit, backup, log) che riducono la probabilità di modifiche non tracciate o fraudolente. Tuttavia, l'intervento umano (es. errore medico, uso improprio dell'account) e le vulnerabilità informatiche restano possibili.