ACCORDO SULLA PROTEZIONE DEI DATI PERSONALI

1. OGGETTO

Il presente Accordo sulla protezione dei dati definisce le condizioni alle quali Doctolib si impegna a effettuare le operazioni di Trattamento dei Dati personali forniti dall'Abbonato /Utente per la prestazione dei Servizi.

Nell'ambito del rapporto contrattuale esistente, le Parti si impegnano a rispettare le disposizioni di cui alla legislazione vigente in materia di protezione dei dati personali ("Normativa sulla Protezione dei Dati Personali") tra cui il D.Lgs. 196/2003 e ss. mod., i provvedimenti vincolanti emessi dal Garante per la Protezione dei Dati e il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, applicabile dal 25 maggio 2018 (di seguito il «GDPR»).

2. DEFINIZIONI

Le definizioni allegate al presente Accordo sulla protezione dei dati sono disponibili qui.

3. ENTRATA IN VIGORE E DURATA

Il presente Accordo entra in vigore dalla firma del Contratto cui è allegato e rimarrà efficace per tutta la durata del rapporto contrattuale tra Doctolib e l'Abbonato/Utente.

4. QUALITÀ DELLE PARTI

Le Parti convengono che l'Utente/Abbonato è il Titolare del trattamento e Doctolib, ai sensi dell'art. 28 GDPR, è il Responsabile dei Trattamenti dei Dati Personali e dei Dati Sanitari riportati nell'Allegato 1, indipendentemente dal fatto che essi siano forniti direttamente o indirettamente a Doctolib dall'Utente/Abbonato o da un Amministratore al quale l'Utente/Abbonato ha concesso l'accesso ai Servizi.

Doctolib è autorizzata dall'Utente/Abbonato a trattare, per conto del Titolare del trattamento, i Dati Personali e i Dati Sanitari necessari alla prestazione dei Servizi per le finalità, e nel rigoroso rispetto delle condizioni, di seguito menzionate.

Si precisa che l'incarico di Doctolib è limitato all'installazione, alla prestazione dei Servizi e all'hosting della Piattaforma Doctolib, delle Schede Pazienti e del Portale Pazienti. Su espressa richiesta dell'Utente/Abbonato e sotto il suo controllo e responsabilità, Doctolib potrà tuttavia assisterlo nell'importare il Database Paziente sulla Piattaforma Doctolib.

Quando il Titolare del trattamento inserisce Dati Personali o Dati Sanitari di terzi nella Piattaforma Doctolib o nel Portale Pazienti, come i dati dei colleghi, deve osservare i requisiti normativi in relazione al rilascio dell'informativa e/o all'ottenimento del consenso da parte di detti terzi.

4.1. Obblighi dell'Utente/Abbonato

L'Utente e/o l'Abbonato, in qualità di Titolare del trattamento, è l'unico responsabile della tenuta del registro dei trattamenti e, se del caso, dell'esecuzione delle formalità preliminari al trattamento dei Dati Personali e dei Dati Sanitari. Il Titolare del trattamento ha anche il compito di informare i Pazienti in merito all'inserimento dei loro Dati Personali e dei Dati Sanitari sulla Piattaforma Doctolib e delle modalità di esercizio dei loro diritti, fornendo loro l'informativa privacy.

In qualità di Titolare del trattamento, l'Utente e/o l'Abbonato è l'unico responsabile dell'esattezza, affidabilità e pertinenza dei Dati Personali e dei Dati Sanitari. In particolare, è responsabile dell'uso della Piattaforma Doctolib e dei Documenti che carica, conserva, consulta e rimuove dallo spazio di archiviazione. È tenuto a effettuare tutti gli adempimenti necessari a garantire la conformità e liceità dei trattamenti. L'Utente e/o l'Abbonato si obbliga a risarcire e tenere indenne Doctolib, i suoi rappresentanti, dipendenti e responsabili del trattamento rispetto a qualsiasi reclamo, responsabilità, danno e costo (tra cui le spese e gli onorari legali) posti a carico o subiti da Doctolib, i suoi rappresentanti, dipendenti e responsabili del trattamento derivanti dalla mancata osservanza da parte dell'Utente e/o Abbonato del presente obbligo.

L'Utente e/o l'Abbonato si obbliga a:

- Rispettare e far rispettare la riservatezza del rapporto medico-paziente;

- Attuare una politica di responsabilizzazione, gestione dei diritti di accesso e dei ruoli, garantendo la riservatezza dei Dati Personali e dei Dati Sanitari, in linea con la volontà espressa dai Pazienti e dai loro Conoscenti;

- Fornire a Doctolib i dati necessari per svolgere la propria attività quale Responsabile del trattamento, tra cui l'elenco dei Dati Personali e dei Dati Sanitari oggetto del trattamento, la base giuridica dello stesso, le finalità dei trattamenti, nonché il periodo di conservazione dei Dati Personali e dei Dati Sanitari;

- Documentare per iscritto eventuali istruzioni riguardanti il Trattamento di Dati Personali e Dati Sanitari effettuato da Doctolib;

- Assicurarsi, prima e durante il periodo del Trattamento, che Doctolib rispetti gli obblighi stabiliti dal GDPR;

- Sovrintendere ai trattamenti posti in essere da Doctolib in qualità di Responsabile del trattamento;

- Nominare un interlocutore per rappresentare il Titolare del trattamento e, se necessario, un responsabile della protezione dei Dati personali secondo quanto previsto dal GDPR;

- Assicurarsi, prima e durante il periodo del Trattamento, il rispetto degli obblighi stabiliti nel GDPR.

4.2. Obblighi di Doctolib

4.2.1. Doctolib si obbliga a:

- Trattare i Dati Personali e i Dati Sanitari secondo le finalità e il quadro definito nel presente Accordo, e a rispettare le norme tecniche e le *good practice* applicabili ai Dati Personali e ai Dati Sanitari;

- Agire solo su preventiva istruzione del Titolare del trattamento. In caso di impossibilità o difficoltà nel dare esecuzione a determinate istruzioni, Doctolib informerà tempestivamente il Titolare del trattamento. Doctolib può presentare una richiesta scritta per derogare alle istruzioni e, per poter procedere sulla base di tale deroga, deve ottenere la previa e specifica autorizzazione scritta del Titolare del trattamento.

- Non estrarre copie dei Dati Personali e dei Dati Sanitari in mancanza di autorizzazione o istruzioni del Titolare del trattamento in tal senso, non comunicarli a terzi e non utilizzarli per scopi diversi da quelli specificati nel Contratto;

- Non sfruttare o trattare i Dati Personali e i Dati Sanitari, affidatigli dal Titolare dei trattamenti, per conto proprio e/o per conto di terzi, per qualsiasi finalità e con qualsiasi modalità. In particolare, è proibito qualsiasi uso di questi Dati Sanitari per scopi di marketing, pubblicitari, commerciali o statistici;

- Avvalersi di tutti i mezzi in suo possesso, nel rispetto delle previsioni contrattuali e secondo lo stato dell'arte, per garantire la sicurezza e la riservatezza dei Dati Personali e dei Dati Sanitari che gli sono affidati e, in particolare, per evitare che siano modificati, danneggiati o comunicati a terzi non autorizzati; più in generale, attuare le misure tecniche e organizzative appropriate per proteggere i Dati Personali e i Dati Sanitari dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dalla diffusione o dall'accesso non autorizzato, in particolare laddove il Trattamento comporti la trasmissione di dati in rete, nonché da qualsiasi forma di trattamento illecito;

- Comunicare tempestivamente al Titolare del trattamento ogni violazione della sicurezza che riguardi direttamente o indirettamente i Dati Personali, i Dati Sanitari o i Trattamenti che lo riguardano;

- Effettuare backup regolari dei Dati Personali e dei Dati Sanitari;

- Condurre regolarmente test di penetrazione (o Pentest);

- Manutenere quanto necessario per il corretto funzionamento dei Servizi;

- Garantire la riservatezza dei Dati Personali e dei Dati Sanitari oggetto di Trattamento;

- Dare seguito a qualsiasi aggiornamento, rettifica, cancellazione o altre modifiche comunicate dal Titolare del trattamento relativamente ai Dati Personali e ai Dati Sanitari;

- Osservare il periodo di conservazione dei Dati Personali e dei Dati Sanitari applicabile alle finalità per le quali sono stati raccolti o forniti, come da indicazioni del Titolare del trattamento e cancellarli/renderli anonimi non appena tali scopi vengono meno, fermi restando gli obblighi di legge;

- Nominare un Responsabile della Protezione dei Dati Personali.

4.2.2. Doctolib si impegna inoltre a garantire che le persone autorizzate a trattare Dati Personali e Dati Sanitari ai sensi del presente Accordo:

- Si impegnino a rispettare la riservatezza o siano vincolati da un adeguato impegno di riservatezza;

- Ricevano la formazione necessaria in materia di protezione dei Dati Personali e dei Dati Sanitari.

Doctolib adotta le misure necessarie per assistere il Titolare del trattamento nella realizzazione delle valutazioni d'impatto relative alla protezione dei Dati Personali e dei Dati Sanitari e nella consultazione preventiva dell'autorità di controllo.

Doctolib mette a disposizione del Titolare del trattamento tutte le informazioni necessarie in relazione al Trattamento dei Dati Personali e dei Dati Sanitari al fine di assisterlo nell'adempimento dei suoi obblighi legali e regolamentari come Titolare del trattamento in conformità alle disposizioni del GDPR (Allegato 3.1).

In mancanza di diverse e ulteriori istruzioni specifiche del Titolare del trattamento in relazione alla natura dei Dati Personali e dei Dati Sanitari da trattare, alle finalità, alla base giuridica e al periodo di conservazione, il Titolare del trattamento riconosce dichiara ed accetta che i Dati Personali e i Dati Sanitari saranno trattati secondo le modalità di cui agli Allegati 1 e 2. In qualità di Titolare del trattamento, l'Utente/Abbonato può chiedere a Doctolib di modificare tali modalità nell'adempiere il Contratto.

5. VIOLAZIONE DEI DATI PERSONALI

Qualora Doctolib venga a conoscenza di una Violazione dei Dati Personali e/o dei Dati Sanitari, Doctolib comunica tempestivamente al Titolare del trattamento detta violazione, tramite e-mail o qualsiasi altro mezzo di comunicazione messo a sua disposizione dal Titolare del trattamento.

Su richiesta del Titolare del trattamento, tale notifica è accompagnata da ogni documento utile finalizzato a consentirgli, ove necessario, di comunicare tale violazione alla competente autorità di controllo e, se del caso, agli interessati.

La persona di contatto per la gestione degli incidenti che hanno un impatto sui Dati Sanitari ospitati è privacy.italy@doctolib.com

6. TENUTA DEL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Doctolib dichiara di tenere un registro scritto di tutti i trattamenti effettuati per conto del Titolare del trattamento in conformità con le disposizioni del GDPR.

7. INFORMAZIONE E DIRITTI DEGLI INTERESSATI

Il Titolare del trattamento è tenuto a informare l'Interessato o gli Interessati circa (i) i Trattamenti effettuati nell'ambito dei Servizi e ottenere il loro consenso o i loro consensi ogni volta che ciò sia necessario in conformità alla normativa applicabile (ii) le basi giuridiche dei Trattamenti effettuati, le finalità dei Trattamenti e l'elenco dei responsabili che possono trattare i loro dati personali.

Al fine di assistere il Titolare del trattamento rispetto a tali informazioni, Doctolib pubblica sul Portale Paziente una Informativa sulla Privacy disponibile all'indirizzo https://www.doctolib.it.

8. GESTIONE DEI DIRITTI

Il Titolare del trattamento è tenuto a dare seguito alle richieste degli Interessati in merito ai loro Dati Personali.

Per quanto possibile, Doctolib, in qualità di Responsabile del trattamento, e su richiesta del Titolare del trattamento potrà assisterlo nell'adempimento dell'obbligo di soddisfare le richieste di esercizio dei diritti degli Interessati: diritto di accesso, rettifica, cancellazione e opposizione, diritto alla limitazione del trattamento, diritto alla portabilità dei dati, diritto a non essere sottoposto a una decisione individuale automatizzata (compresa la profilazione), diritto di decidere dei propri Dati Personali, in particolare dopo il suo decesso, ecc.

Se un Interessato si rivolge direttamente a Doctolib per esercitare uno dei diritti che vanta sui suoi Dati personali trattati da Doctolib in qualità di Responsabile del trattamento, Doctolib si impegna a indirizzare l'Interessato verso il Titolare del trattamento, affinché questi possa dare seguito alla sua richiesta.
Su richiesta del Titolare del trattamento, Doctolib potrà assisterlo nel dare seguito alle richieste di esercizio di un diritto, ma non rispondere direttamente alle richieste di tali Interessati.

9. SICUREZZA E RISERVATEZZA

9.1 Per quanto riguarda i Servizi, Doctolib attua le misure tecniche e organizzative adeguate con riferimento alla sicurezza, in conformità alle disposizioni previste dalla Normativa sulla Protezione dei Dati Personali e dal GDPR, e dirette a garantire un livello di sicurezza adeguato rispetto ai rischi presentati dal Trattamento dei Dati personali dell'Utente/Abbonato, secondo quanto indicato *sub* Allegato 2 (Misure tecniche e organizzative). Per valutare il livello adeguato di sicurezza, Doctolib terrà conto dei rischi che possono derivare dalla distruzione accidentale o illecita, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso ai Dati Personali e Dati Sanitari che possono essere trasmessi, conservati o altrimenti trattati, conformemente alle disposizioni dell'articolo 32 del GDPR.

Gli obblighi di cui sopra non liberano in alcun modo l'Utente/Abbonato dall'obbligo di mettere in atto tutti i mezzi di sicurezza necessari a garantire la riservatezza dei Documenti e dei Dati Abbonati, del Database Paziente, dei Dati Utenti, dei Dati Personali e dei Dati Sanitari presenti sulla Piattaforma Doctolib.

Le parti convengono che, in caso di controllo, il Contratto di cui è parte il presente Accordo sulla protezione dei dati può essere messo a disposizione di qualsiasi autorità competente.

9.2 Segreto Professionale: Doctolib riconosce e accetta che i Dati Personali e i Dati Sanitari trattati dal Titolare del trattamento nel godimento dei Servizi sono rigorosamente coperti dal segreto professionale (articolo 622 del codice penale).

9.3 Tenuta dei dati: Salvo diverso espresso accordo sulla protezione dei dati, il Titolare del trattamento resta l'unico titolare dei Dati Abbonato/Utente pubblicati sul Portale Pazienti, così come sulla Scheda Profilo Utente e sulla Piattaforma Doctolib. Doctolib non potrà rivendicare alcun diritto sui dati pubblicati dal Titolare del trattamento. Le statistiche di utilizzo del Portale Pazienti, rese anonime, sono di proprietà di Doctolib.

10. PERSONALE DOCTOLIB

Doctolib individua team qualificati con le necessarie competenze tecniche e/o funzionali per la prestazione dei Servizi. Le persone autorizzate a trattare i Dati Personali e/o i Dati Sanitari per conto del Titolare del trattamento hanno ricevuto formazione in relazione alla normativa relativa alla protezione dei dati personali.

11. ULTERIORI RESPONSABILI DEL TRATTAMENTO

L'Utente/Abbonato concede in questa sede a Doctolib l'autorizzazione generale ad avvalersi di Responsabili ulteriori del trattamento qui elencati, laddove ciò sia ragionevolmente necessario per fornire i Servizi. Conformemente a tale autorizzazione generale, Doctolib si impegna a informare ciascun Utente/Abbonato, con un preavviso scritto di trenta (30) giorni, di ogni cambiamento previsto che comporti l'aggiunta o la sostituzione di Responsabili ulteriori del trattamento, offrendo così all'Utente/Abbonato la possibilità di sollevare eventuali obiezioni che lo stesso dovesse avere in merito a tali cambiamenti. Se l'Utente/Abbonato dovesse avere motivi legittimi e ragionevoli per opporsi alla nomina di un nuovo Responsabile ulteriore del trattamento, l'Utente dovrà tempestivamente motivare ciò a Doctolib inviandogli notifica scritta al seguente indirizzo: privacy.italia@doctolib.com, entro trenta (30) giorni lavorativi successivi alla comunicazione di Doctolib, in difetto della quale si presumerà che l'Utente/Abbonato abbia approvato e accettato tale nomina.

Dopo eventuali discussioni, in mancanza di accordo tra Doctolib e l'Utente/Abbonato, quest'ultimo potrà, nei trenta (30) giorni successivi alla notifica, recedere dalla parte del Contratto interessata dall'aggiornamento in questione.

Con riguardo agli eventuali Responsabili ulteriori del trattamento, Doctolib: (i) eserciterà la dovuta diligenza commerciale nel valutare, nominare e monitorare le attività di Trattamento dei Responsabili ulteriori del trattamento; (ii) inserirà nel contratto tra Doctolib e ciascun Responsabile ulteriore del trattamento clausole che offrano, con riguardo ai Dati Personali e Dati Sanitari degli Abbonati/Utenti, un livello di protezione equivalente a quanto previsto nel presente Accordo.

Nel caso in cui i Responsabili ulteriori del trattamento non adempiano ai loro obblighi in materia di protezione dei Dati Personali, Doctolib rimane responsabile nei confronti del Titolare per l'adempimento da parte degli ulteriori Responsabili dei loro obblighi in conformità con i termini del Contratto.

12. CERTIFICAZIONE HDS

12.1. Doctolib si avvale, quale fornitore dei servizi di hosting dei Dati sanitari di Amazon Web Services SARL (AWS), la cui sede legale è sita al 38 avenue John F. Kennedy, L - 1885 Lussemburgo, che è altresì certificato come HDS (Health Data Host - Host di Dati Sanitari) ai sensi della normativa francese in materia di sanità pubblica (articolo L1111-8 del Codice della Salute Pubblica

francese e del decreto n°2018-137 del 26 febbraio 2018 relativo all'hosting dei Dati Sanitari).

Nel gennaio 2019, AWS ha ottenuto un certificato di "host di infrastruttura fisica" e un certificato di "hosting provider". La prossima data di rinnovo di tali certificati è il 13 gennaio 2025.

I Dati sanitari e personali sono ospitati da AWS a Francoforte (Germania) e a Parigi (Francia). In qualità di Host di Dati sanitari, Doctolib affida ad AWS il subappalto dei seguenti servizi relativi all'hosting della Piattaforma Doctolib: "fornitura e mantenimento dell'operatività dei siti fisici destinati ad ospitare l'infrastruttura fisica del sistema informativo utilizzato per il trattamento dei Dati sanitari; fornitura e mantenimento in condizioni operative dell'infrastruttura fisica del sistema informativo utilizzato per il trattamento dei Dati sanitari; fornitura e mantenimento dell'infrastruttura virtuale del sistema informativo utilizzato per il trattamento dei Dati sanitari; fornitura e mantenimento della piattaforma di hosting delle applicazioni del sistema informativo; backup dei Dati sanitari".

12.2 In qualità di Host dei Dati sanitari certificato, AWS:

(i) Tratta i Dati sanitari e personali solo su istruzioni documentate di Doctolib e implementa misure di sicurezza per controllare l'accesso a tali Dati sanitari e personali;

(ii) Mette a disposizione di Doctolib funzionalità che le consentano di (a) garantire il diritto alla portabilità degli Utenti e (b) coprire eventuali inadempimenti da parte di AWS e (c) ottenere al termine del contratto la restituzione e/o la cancellazione dei Dati sanitari personali ospitati da AWS:

(ii) Notifica Doctolib nel più breve tempo possibile in caso di incidente di sicurezza e mette in atto tutte le misure ragionevoli per mitigare i danni derivanti da tale incidente e consente a Doctolib di informare un referente contrattuale da contattare per gestire eventuali incidenti che abbiano un impatto sui Dati personali ospitati.

(iv) Si impegna a garantire che eventuali responsabili del trattamento forniscano un livello di protezione equivalente a quello garantito da AWS a Doctolib;

(v) autorizza Doctolib a condurre audit per garantire il rispetto degli obblighi previsti dal contratto con Doctolib; le misure di sicurezza tecniche e organizzative possono essere oggetto di audit documentali su richiesta di Doctolib, mentre la conformità allo standard ISO 27001 (ivi compresa la sicurezza dei datacenter) può essere verificata da Doctolib su presentazione del rapporto di audit annuale effettuato da un esperto di sicurezza terzo indipendente;

(vi) Mette a disposizione di Doctolib attraverso questo link gli indicatori di qualità e di prestazione che consentono di verificare il livello di servizio annunciato, il livello garantito, la periodicità della loro misurazione, nonché l'esistenza o l'assenza di sanzioni applicabili in caso di mancato rispetto degli stessi;

(vii) È conforme a tutte le leggi, le norme, i regolamenti e le ordinanze applicabili alla sua attività di Host di Dati sanitari.

12.3. Dal 14 ottobre 2021 Doctolib è inoltre in possesso di un certificato di "hosting provider" per il campo di applicazione "fornitura di servizi informatici in outsourcing comprendenti dati di identificazione personale, dati sanitari (compresi i dati medici), che coprono le attività ANS n. 5 e n. 6 dello Standard HDS versione 1.1 (2018)", in conformità alla dichiarazione di applicabilità (DdA) versione 1.2 del 14 settembre 2021. La data di rinnovo del suddetto certificato è il 14 ottobre 2024.

12.4 I Dati sanitari e personali sono ospitati da Doctolib a Francoforte (Germania) e Parigi (Francia). Doctolib si impegna a non utilizzare i Dati sanitari personali per finalità diverse dallo svolgimento dell'attività di hosting dei dati sanitari, salvo diversamente richiesto e documentato dal Titolare del trattamento.

12.5 Doctolib comunicherà al Titolare del trattamento qualsiasi violazione dei Dati sanitari personali ai sensi dell'articolo 5 del presente Accordo.

12.6 Doctolib mette in atto misure tecniche e organizzative appropriate relative alla sicurezza e volte a garantire un livello di sicurezza adeguato a fronte dei rischi presentati dall'hosting dei Dati sanitari personali dell'Utente/Abbonato, come indicato nell'Allegato 2 (Misure tecniche e organizzative). A tal proposito, i Dati sanitari personali saranno trasmessi solo attraverso reti di comunicazione sicure.

In caso di sviluppi tecnici introdotti da Doctolib in queste misure tecniche e organizzative, Doctolib si impegna a mantenere un livello di sicurezza equivalente a quello previsto dal presente Contratto, a meno che lo sviluppo tecnico in questione non sia imposto da un obbligo legale o normativo.

12.7 Al termine del Contratto o su richiesta dell'Utente/Abbonato in caso di ritiro della certificazione HDS di Doctolib, l'Utente/Abbonato potrà recuperare i Dati sanitari personali ospitati da Doctolib alle condizioni di cui all'articolo 14 del presente Accordo.

12.8 Il Titolare del trattamento si impegna a rispettare la Politica generale sulla sicurezza dei sistemi informativi sanitari (PGSSI-S).

13. AUDIT

13.1 Al fine di valutare la sicurezza dei Servizi, il Titolare del trattamento potrà far effettuare audit di sicurezza a proprie spese, nel rispetto delle condizioni previste dal presente articolo e nel limite di un (1) audit all'anno e per un massimo di cinque (5) giorni lavorativi; il tempo impiegato dal personale Doctolib sarà fatturato al Titolare del trattamento.

13.2 L'audit sarà limitato alla verifica dei processi, dell'organizzazione e degli strumenti direttamente ed esclusivamente legati all'attuazione delle disposizioni del GDPR per i Servizi interessati.

L'audit non avrà in nessun caso lo scopo di controllare o richiedere l'accesso a (i) qualsiasi Dato Personale o Dato Sanitario che non sia specifico, sia esso riservato o meno, o qualsiasi informazione la cui comunicazione potrebbe, a giudizio di Doctolib, danneggiare la

sicurezza dei Servizi o di suo Utente; (ii) i dati finanziari di Doctolib; o (iii) i Dati Personali relativi ai dipendenti di Doctolib o dei suoi Responsabili.

Le Parti convengono che tutte le attività intraprese come parte di un audit non devono, né congiuntamente né in altro modo: (i) ostacolare, modificare o interessare in qualsiasi modo il funzionamento di Servizi, sistemi, reti, software e/o hardware diversi da quelli destinati all'uso esclusivo dell'Utente/Abbonato; (ii) danneggiare l'infrastruttura che ospita i Servizi (iii) danneggiare, cancellare, modificare qualsiasi tipo di dato; (iv) consentire l'accesso non autorizzato o il mantenimento dei dati summenzionati.

Non è consentito alcun test di intrusione o penetrazione all'applicazione e/o alla piattaforma Doctolib per nessuna ragione, ed è esclusa tale attività nel corso degli audit senza che sia prestato il previo consenso di Doctolib a tal fine.

Doctolib metterà a disposizione dei revisori tutti i documenti e le informazioni necessarie per lo svolgimento dell'audit esclusivamente nei suoi locali, senza alcuna possibilità di rimozione o copia per qualsiasi finalità. Tale divieto si applica anche ai documenti e alle informazioni messe a disposizione dai Responsabili di Doctolib.

13.3 Almeno trenta (30) giorni prima dell'audit, il Titolare del trattamento è tenuto a inviare a Doctolib un accordo di audit che specifichi l'esatta portata dei test, le date e gli orari dei test previsti e le loro condizioni. Il revisore deve anche specificare eventuali account e profili utilizzati per i test (indirizzo IP di origine, user agent, ecc.), la metodologia utilizzata e i soggetti da controllare.

Doctolib deve preventivamente accettare il contenuto dell'accordo di audit prima che possa iniziare la relativa attività.

13.4 Le informazioni ottenute durante l'audit sono Informazioni Riservate e saranno trattate come tali dal Titolare del trattamento. Queste informazioni potranno essere comunicate solo a persone soggette a rigorosi obblighi di riservatezza e che hanno un interesse diretto e rilevante nel conoscerle e non devono essere divulgate in alcun modo al pubblico o internamente.

Se il Titolare del trattamento desidera avvalersi di un revisore esterno, questi deve ottenere il previo consenso scritto di Doctolib, fermo restando che Doctolib può rifiutare il suddetto revisore solo adducendo argomenti oggettivi e fondati.

Il revisore esterno non può in alcun modo essere un concorrente di Doctolib e deve impegnarsi per iscritto a rispettare le condizioni stabilite nel presente articolo.

Il Titolare del trattamento si impegna a comunicare il rapporto di audit gratuitamente a Doctolib, che potrà presentare le proprie osservazioni.

Doctolib avrà un periodo di tempo ragionevole dal ricevimento del rapporto per rimediare i vizi e/o le non conformità riscontrate.

14. RECUPERO DEI DATI

L'Abbonato e l'Utente potranno recuperare il Database paziente, nonché lo storico dei loro appuntamento al termine del Contratto, salvo il caso in cui tali Dati siano stati raccolti illecitamente dall'Abbonato/Utente. Questi dati saranno messi a disposizione dell'Utente/Abbonato in un formato che garantisce la loro interoperabilità. La richiesta di portabilità deve essere fatta via e-mail al seguente indirizzo: privacy.italia@doctolib.com.

Doctolib si impegna, per tutta la durata del Contratto e per tutto il processo di recupero dei dati, a tenerne una copia a disposizione dell'Utente/Abbonato. Nel caso in cui l'accesso dell'Utente/Abbonato ai Servizi Doctolib venga sospeso per qualsiasi motivo, Doctolib consentirà all'Utente/Abbonato di recuperare, con qualsiasi mezzo e su qualsiasi supporto, l'ultima copia del proprio Database Paziente, nonché la sua cronologia degli appuntamenti (fatta eccezione per il caso in cui tali dati siano stati raccolti illecitamente dall'Utente).

15. TRASFERIMENTO DI DATI PERSONALI

I Dati personali potranno essere oggetto di trasferimento, per le finalità elencate nell'Accordo sulla protezione dei dati personali, a società del Gruppo Doctolib, a loro subappaltatori o fornitori di servizi stabiliti in Paesi con un adeguato livello di protezione o che offrono adeguate garanzie in materia di protezione della privacy e dei diritti e delle libertà fondamentali delle persone, in conformità con la legislazione applicabile.

Doctolib informa l'Utente/Abbonato del fatto che i Dati Personali, possono altresì essere trasferiti da Doctolib verso paesi terzi a Responsabili ulteriori del trattamento, esclusivamente nel caso in cui un tale trasferimento sia necessario per prestare i Servizi richiesti. L'elenco dei Responsabili ulteriori del trattamento è qui disponibile qui.

Se il trasferimento avviene verso un Paese terzo la cui legislazione non è stata riconosciuta come in grado di offrire un adeguato livello di protezione dei Dati Personali, Doctolib garantisce che siano messe in atto misure adeguate in conformità con la Normativa sulla Protezione dei Dati Personali e il GDPR, e in particolare, se necessario, che le clausole contrattuali tipo o clausole equivalenti *ad hoc* siano incluse nel contratto concluso tra Doctolib e il Responsabile ulteriore del trattamento.

In qualità di Responsabile del trattamento, Doctolib si impegna ad conservare e far conservare i Dati Personali sul territorio dell'Unione Europea e, se del caso, a trasferire tutti gli obblighi previsti dal presente Accordo al fornitore di servizi che conserva i Dati Personali.

Inoltre, su richiesta delle autorità amministrative e giudiziarie autorizzate, Doctolib potrà comunicare i Dati Personali che tratta in nome e per conto del Titolare per adempiere ai propri obblighi di legge. In tal caso, e salvo quanto diversamente previsto dalla legge, Doctolib si impegna a informare il Titolare del trattamento di tale comunicazione.

16. CONTATTI

In caso di domande relative al Trattamento dei Dati Personali e dei Dati Sanitari effettuato da Doctolib circa le clausole contrattuali,

l'Utente/l'Abbonato può contattare il DPO di Doctolib all'indirizzo di seguito indicato.

Doctolib SAS è da considerarsi lo stabilimento principale del gruppo Doctolib, ai sensi dell'art. 4 n.16 del GDPR. L'autorità di controllo capofila per i trattamenti transfrontalieri ai sensi dell'art. 56 GDPR del gruppo Doctolib è il CNIL (https://www.cnil.fr). Per i trattamenti che non rientrano nella competenza dell'autorità di controllo capofila, l'autorità competente è il Garante per la protezione dei dati personali (https://www.garanteprivacy.it/). Il Responsabile della protezione dei dati può essere contattato al seguente indirizzo: DOCTOLIB – DPO, sede legale in Milano, Corso Giacomo Matteotti n 1, C.F./P.IVA 11537360965, oppure all'indirizzo privacy.italia@doctolib.com.

17. LEGGE APPLICABILE

L'Accordo è disciplinato e interpretato in conformità con la legge nazionale applicabile al Titolare del trattamento.

18. INTERO ACCORDO

Il presente Accordo costituisce l'intero accordo tra le Parti relativamente al suo oggetto e sostituisce tutti gli accordi precedenti o contemporanei conclusi tra le Parti aventi lo stesso oggetto, tra cui ogni versione precedente di un accordo sulla protezione dei dati personali che sia stato firmato tra Utente/Abbonato e Doctolib.

ALLEGATO 1: DETTAGLI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI

Il presente Allegato 1 contiene alcuni dettagli relativi al Trattamento dei Dati Personali e dei Dati Sanitari, in conformità all'articolo 28(3) del GDPR.

TITOLARE DEL TRATTAMENTO: l'Abbonato sottoscrittore di un Abbonamento Doctolib e/o l'Utente avente un account Utente Doctolib.

Le attività del Titolare del trattamento comprendono Trattamenti che consentono l'esercizio di attività funzionale alla prenotazione ed erogazione delle prestazioni finalizzate alla prevenzione, diagnosi e cura così come alla gestione amministrativa del proprio istituto di cura, struttura sanitaria o studio privato.

I Trattamenti consentono in particolare, ai fini della cura dei pazienti (i) la gestione degli appuntamenti; (ii) la gestione delle cartelle cliniche necessarie al follow-up del paziente; (iii) le comunicazioni tra i professionisti identificati e le strutture di cura coinvolte nella cura dell'interessato e nel coordinamento della stessa, nonché (iv) la gestione delle richieste avanzate dai pazienti tramite il Servizio Richieste.

I Trattamenti effettuati devono rispondere a un obiettivo preciso ed essere giustificati alla luce delle missioni e delle attività degli Attori Sanitari.

RESPONSABILE(I) DEL TRATTAMENTO: Doctolib S.r.l.

Le attività effettuate dal Responsabile del trattamento per conto dei Titolari del trattamento sono di seguito descritte.

TRATTAMENTO N°1: CONFIGURAZIONE DEGLI ACCOUNT ABBONATI E UTENTI

TRATTAMENTI:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ DEL TRATTAMENTO:

- Gestione degli account: configurare l'Account Utente e le credenziali degli Utenti;
- Supporto tecnico e assistenza: fornire supporto tecnico, manutenzione ed elaborazione delle richieste degli Utenti, consulenza, archiviazione, hosting e altri servizi forniti agli Utenti;
- Supporto Dati Personali: assistenza nella gestione delle Violazioni di Dati Personali e Dati Sanitari, assistenza nella conduzione della DPIA, supporto nella risposta alle richieste di esercizio dei diritti degli Interessati;
- Indirizzamento di Pazienti verso Attori Sanitari;
- Reporting, debug e statistiche.

BASE GIURIDICA DEL TRATTAMENTO:

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi trattamento
Per aiutare il titolare dei dati, la CNIL ad esempio ha messo a disposizione un quadro di riferimento che propone, a titolo indicativo, l'interesse legittimo come base giuridica. Il titolare dei dati è libero di citare un'altra base giuridica a Doctolib.

INTERESSATI:

Abbonato e Utente, secondo la definizione contenuta nel Contratto.

TIPOLOGIE DI DATI PERSONALI:

Nell'intento di ridurre al minimo il numero di Dati Personali trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i dati pertinenti e necessari avuto riguardo alle proprie esigenze in termini di gestione amministrativa dei suoi pazienti, anche tenuto conto di eventuali Dati Sanitari correlati alla prenotazione degli appuntamenti.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate:

a) **L'identità e i dati di contatto dell'Attore Sanitario**: sesso, nome, cognome, numero di telefono e indirizzo e-mail, indirizzo postale, fotografia, firma, documento d'identità, il titolo di laurea, il titolo di specializzazione e l'abilitazione professionale, il certificato di iscrizione all'Ordine di appartenenza (inclusa la data di iscrizione e il numero di iscrizione al relativo Albo).
b) **Dati professionali:** fotografia, specializzazione, dettagli della presa in carico, percorso professionale dell'Attore Sanitario, tipi di prestazione/consulto disponibili, orari di apertura e chiusura, particolarità legate al luogo in cui avviene il consulto.
c) **log di utilizzo e di connessione** che riportano le «azioni commerciali» degli Utenti all'interno della Piattaforma Doctolib e i log **tecnici** che riportano l'«attività» dei componenti software e hardware utilizzati dall'Utente/Abbonato, affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

Fatte salve istruzioni specifiche del Titolare del trattamento, Doctolib tratta tutti i suddetti Dati Personali al fine di fornire il Servizio, oggetto del Contratto.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

Si prega di fare riferimento all'elenco di cui all'articolo 11 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
In mancanza di istruzioni in tal senso da parte del Titolare del trattamento, Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali.

TRATTAMENTO N°2: LA GESTIONE DEGLI APPUNTAMENTI E DELL'AGENDA

TRATTAMENTI:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ DEL TRATTAMENTO:

- Supporto nella gestione del caricamento e dell'estrazione del contenuto delle agende, degli appuntamenti e, quando necessario del Database Paziente degli Attori Sanitari sulla Piattaforma Doctolib;
- Consentire al Titolare del trattamento di gestire la sua agenda;
- Consentire al Titolare del trattamento di gestire il percorso di cura per i Pazienti e loro Conoscenti;
- Consentire al Titolare del trattamento la gestione della sua agenda, e assicurare che la gestione dell'organizzazione del suo istituto di cura o studio sia adeguata in caso di eventuali esigenze correlate alla gestione di emergenze sanitarie;
- Consentire la prenotazione di appuntamenti online dei Pazienti, fatta per sé stessi e per i loro Conoscenti;
- Permettere la gestione degli appuntamenti;
- Consentire all'Attore Sanitario di comunicare al Paziente, e ai loro Conoscenti se applicabile, le informazioni relative e/o funzionali, al loro percorso di cura;
- Permettere al Titolare del trattamento di inviare e ricevere Documenti ai Pazienti e ai loro Conoscenti;
- Inviare SMS, e-mail e notifiche push (i) di conferma, annullamento o promemoria dell'appuntamento; (ii) informative sull'invio di Documenti; (iii) informative di promemoria (iv) informative legate alla cura del Paziente o all'organizzazione della sua attività;
- Consentire la gestione dei trasferimenti di contenuti delle agende e appuntamenti degli Attori Sanitari della Piattaforma Doctolib;
- Rapporti, debug e statistiche.

BASE GIURIDICA DEL TRATTAMENTO:

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi Trattamento.
Per aiutare il titolare dei dati, la CNIL ha messo a disposizione un quadro di riferimento che propone, a titolo indicativo, l'interesse legittimo come base giuridica per la gestione degli appuntamenti e delle agende. Il titolare dei dati è libero di citare un'altra base giuridica a Doctolib.

INTERESSATI:

I Pazienti e loro Conoscenti, colleghi degli Attori Sanitari.

TIPOLOGIE DI DATI PERSONALI:

Nell'intento di ridurre al minimo il numero di Dati Personali e Dati Sanitari trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i Dati personali e i Dati Sanitari pertinenti e necessari avuto riguardo alle proprie esigenze in termini di gestione amministrativa dei suoi pazienti, anche tenuto conto di eventuali Dati Sanitari correlati alla prenotazione degli appuntamenti.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate:
a) **L'identità e i Dati di Contatto del Paziente o del Conoscente:** sesso, nome, cognome, data di nascita, luogo di nascita, indirizzo postale, indirizzo e-mail e numero di telefono.
b) **la professione del Paziente o del Conoscente**: professione.
c) **Salute**: eventuale stato assicurativo, identità e i dati di contatto del medico curante, l'identità e i dati di contatto del medico di riferimento, la data/ora e il luogo dell'appuntamento, la specializzazione del medico e la natura del consulto, lo stato dell'appuntamento, i documenti medici del Paziente, le note compilate dall'Attore Sanitario;
d) **log di utilizzo e di connessione** che riportano le «azioni commerciali» degli Utenti all'interno della Piattaforma Doctolib e i **log tecnici** che riportano l'«attività» dei componenti software e hardware utilizzati dall'Utente, affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

Fatte salve istruzioni specifiche del Titolare del trattamento, Doctolib tratta tutti i suddetti Dati Personali e Dati Sanitari al fine di fornire il Servizio, oggetto del Contratto.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

- Gli Attori Sanitari;
- Le persone incaricate della segreteria, nel rispetto delle disposizioni sul segreto professionale;
- Le persone autorizzate all'interno di Doctolib
- I Responsabili ulteriori del trattamento: si prega di fare riferimento all'elenco di cui all'articolo 11 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
Di default e salvo diversa indicazione del Titolare, quest'ultimo sarà fissato per un periodo di 5 anni per lo storico degli appuntamenti.
Il Titolare è libero di comunicare a Doctolib un diverso periodo di conservazione compreso tra 1 anno e 20 anni.
In relazione alle finalità gestionali della struttura sanitaria e dello studio medico o paramedico, i dati registrati nella Piattaforma Doctolib potranno essere conservati per un periodo massimo di venti anni dalla data dell'ultimo trattamento del Paziente.

TRATTAMENTO N°3: CARICAMENTO DEL DATABASE PAZIENTE

FINALITÀ:

1/ Consentire l'estrazione del Database Paziente identificato dall'Abbonato/ Utente, Titolare del trattamento;

2/ Permettere di strutturare il Database Paziente e di caricarlo nel servizio del software medico dell'Abbonato/Utente sulla piattaforma Doctolib;

3/ Permettere l'hosting e il backup del Database Paziente sulla piattaforma;

4/ Supporto e assistenza tecnica: assicurare il supporto tecnico, la manutenzione e l'elaborazione delle richieste di Utenti e altri servizi forniti agli Abbonati/Utenti.

BASE GIURIDICA DEL TRATTAMENTO

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi trattamento.

INTERESSATI:
I Pazienti e loro Conoscenti, gli Abbonati/Utenti, loro colleghi.

Spetta al Titolare del trattamento determinare l'elenco esatto delle persone suscettibili di essere interessate dal Trattamento.

TIPOLOGIE DI DATI INTERESSATI:

Si ricorda che spetta ai Titolari del trattamento fornire nel Servizio Software Medico messo a disposizione da Doctolib solo i Dati Sanitari e i Dati Personali necessari al monitoraggio del Paziente e dei suoi Conoscenti.
Si deve escludere qualsiasi integrazione di informazioni che non siano legate allo scopo della consultazione del Paziente e dei suoi Conoscenti o che non siano essenziali per la diagnosi e la prestazione delle cure.
Prima di qualsiasi integrazione di Dati Sanitari o Dati Personali relativi al Paziente e/o ai suoi Conoscenti, spetta agli Abbonati/Utenti ottenere il consenso preventivo del Paziente e dei suoi Conoscenti.

In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate: i dati identificativi e di contatto: il cognome, il nome, la data di nascita, l'indirizzo, il numero di telefono.

DESTINATARI E RESPONSABILI SUCCESSIVI DEL TRATTAMENTO DEI DATI:

Nell'ambito di queste azioni e al solo scopo di aiutare l'Abbonato ad utilizzare i suoi Servizi, Doctolib può essere obbligato ad avere accesso ai Database pazienti su base temporanea.

PERIODI DI CONSERVAZIONE:

I Dati Personali raccolti saranno conservati per tutta la durata del rapporto contrattuale che vincola il Titolare del trattamento e Doctolib.

TRATTAMENTO N°4: GESTIONE DEL SERVIZIO RICHIESTE

TRATTAMENTI:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per la trasmissione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ DEL TRATTAMENTO:

- Consentire l'inserimento e invio della richiesta di prestazione inserita dai Pazienti nel contesto del Servizio Richieste indirizzata all'Utente;
- Permettere la gestione della richiesta;
- Consentire all'Attore Sanitario di comunicare al Paziente, le informazioni relative e/o funzionali, al loro percorso di cura;
- Permettere al Titolare del trattamento di inviare e ricevere Documenti ai Pazienti;
- Inviare e-mail di conferma ricezione della richiesta e di inoltro della documentazione richiesta legata alla cura del Paziente.

BASE GIURIDICA DEL TRATTAMENTO:

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi trattamento.

INTERESSATI:

Pazienti, secondo la definizione contenuta nel Contratto.

TIPOLOGIE DI DATI PERSONALI:

Nell'intento di ridurre al minimo il numero di Dati Personali trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i dati pertinenti e necessari avuto riguardo alle proprie esigenze in termini di gestione amministrativa dei suoi pazienti, anche tenuto conto dei Dati Sanitari correlati alla richiesta presentata tramite il servizio.
In linea di principio, i seguenti dati sono considerati pertinenti alle finalità sopra menzionate:
a) **L'identità e i Dati di Contatto del Paziente**: sesso, nome, cognome, data di nascita, indirizzo e-mail.
b) **Salute**: medico curante e di riferimento, prescrizioni mediche, analisi cliniche, referti, informazioni contenute nel Campo di Informazioni Aggiuntive che il Paziente ritiene necessarie, pertinenti e rilevanti da condividere con l'Attore Sanitario per la gestione del Servizio Richieste, Contenuti dei Documenti che possono includere Dati Sanitari, informazioni che l'Attore Sanitario può includere nel Campo Informazioni Aggiuntive che possono includere dati sanitari.

Si ricorda che spetta ai Titolari del trattamento richiedere al Paziente, e fornire nel Servizio Richieste reso disposizione da Doctolib solo i Dati Sanitari e i Dati Personali necessari alla prestazione sanitaria richiesta in tale contesto dal Paziente.
Si deve escludere qualsiasi integrazione di informazioni che non siano legate allo scopo della gestione della richiesta del Paziente o che non siano essenziali per la prestazione delle cure.

DESTINATARI E RESPONSABILI ULTERIORI DEL TRATTAMENTO:

Si prega di fare riferimento all'elenco di cui all'articolo 11 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
In mancanza di istruzioni in tal senso da parte del Titolare del trattamento, Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali.

TRATTAMENTO N. 5: GESTIONE DEI DOCUMENTI O MODULI

TRATTAMENTI:

I servizi di Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, il recupero, la consultazione e l'utilizzo, la comunicazione per trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali elencati di seguito.

FINALITA':

1/ Per permettere la creazione e la formattazione di documenti;
2/ Permettere (i) l'invio di Documenti da parte del Paziente o del Titolare e (ii) la ricezione di Documenti da parte del Paziente, del Titolare e/o di qualsiasi altro destinatario scelto dal Titolare;
3/ Consentire (i) al Titolare del trattamento di chiedere al Paziente o ad un Parente Autorizzato, al fine di facilitare la preparazione dell'appuntamento, di inviare uno o più Documenti, o di rispondere a determinati quesiti riguardanti il Paziente, (ii) la redazione di tali Documenti o moduli, e la loro firma elettronica da parte del Paziente o di un suo Parente autorizzato, (iii) la ricezione e conservazione di tali Documenti e moduli da parte del Titolare;
4/ Consentire l'apposizione di una firma elettronica semplice ai documenti.
5/ Rapporti, debug e statistiche.

BASE GIURIDICA

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi operazione di Trattamento.

A titolo indicativo, il legittimo interesse potrebbe costituire la base giuridica. Il Titolare del trattamento è libero di indicare a Doctolib un'altra base giuridica.

Per quanto riguarda i documenti e le informazioni richieste al Paziente o ad un Parente Autorizzato in preparazione di un appuntamento, si rammenta al Titolare che è tenuto al rispetto del principio di proporzionalità, ovvero di minimizzazione dei dati, e quindi di richiedere solo i documenti o informazioni strettamente necessarie alla cura del Paziente.

INTERESSATI:

Pazienti e Attori sanitari, con o senza account utente Doctolib.

TIPOLOGIE DI DATI PERSONALI:

In linea di massima, ai fini sopra indicati sono trattati i seguenti

a) Dati Personali **identificazione**;
b) Codice fiscale e/o tessera sanitaria, ai fini della fatturazione e del rimborso delle cure;
c) Dati di **contatto**;
d) Dati sullo stile di vita, come ad esempio esercizio fisico, dieta e comportamento alimentare, etc.;
e) **Anamnesi** medica e familiare e allergie;
f) Dati della **visita**;
g) Dati relativi alla **prescrizione**;
h) Dati **biometrici e biologici**;
i) Dati del **team** di assistenza sanitaria;
j) Immagini diagnostiche;
k) I **log di utilizzo** e di **connessione** che riportano le "azioni commerciali" degli Utenti all'interno della Piattaforma Doctolib e i **log tecnici** che riportano l'"attività" dei componenti software e hardware utilizzati dall'Utente/Sottoscrittore affinché Doctolib possa garantire il funzionamento e l'accesso alle funzionalità richieste.

DESTINATARI DEI DATI

I Dati Personali sono comunicati ad Attori sanitari e/o Pazienti o al Parente Autorizzato a seconda dei casi e delle specifiche esigenze correlate al perseguimento della singola finalità di trattamento sopra elencata.

Quando l'Attore Sanitario condivide un Documento o informazioni nell'ambito della preparazione o a seguito di un appuntamento fissato per il Paziente da un Parente, l'Attore Sanitario assicura, sotto la propria responsabilità, il rispetto del segreto medico nell'ambito di tale condivisione. Pertanto, l'Attore Sanitario assicura (i) che il Parente sia regolarmente autorizzato, per legge o per atto giuridico, a rappresentare il Paziente e ad accedere ai suoi Dati Sanitari, e/o (ii) ad ottenere il consenso del Paziente alla condivisione dei propri Dati Sanitari con il Parente che ha preso appuntamento per loro conto.

PERIODO DI CONSERVAZIONE:

Salvo istruzioni specifiche del Titolare del trattamento, i Documenti conservati dall'Utente nella Piattaforma Doctolib sono conservati secondo le condizioni allegate a ciascun Servizio o fino alla cancellazione da parte dell'Utente.
In deroga, e fermo restando che Doctolib ottenga l'espresso consenso del Paziente o del Parente Autorizzato, il Titolare autorizza espressamente Doctolib, in qualità di Responsabile del trattamento, a conservare nella sezione "I Miei Documenti" al fine di consentire (i) al Paziente di consultare in qualsiasi momento i Documenti e i moduli inviati o ricevuti sul proprio Account Doctolib, (ii) al Paziente di riutilizzare tali Documenti e informazioni nell'ambito del preparazione di futuri incontri su Doctolib.

TRATTAMENTO N. 6: FORNITURA DI UN SERVIZIO DI MESSAGGISTICA

OPERAZIONI DI TRATTAMENTO:

I Servizi Doctolib implicano la raccolta, la registrazione, l'organizzazione, la conservazione, l'estrazione, la consultazione e l'utilizzo, la comunicazione per la trasmissione, l'anonimizzazione e la cancellazione dei Dati personali di seguito elencati.

FINALITÀ:

1/ Facilitare la comunicazione tra gli Attori Sanitari offrendo un canale di scambio sicuro tramite la messaggistica istantanea;
2/ Consentire lo scambio di Documenti e dati che possono includere Dati personali dei pazienti;
3/ Comunicare via e-mail ai destinatari dei messaggi inviati dal Titolare del trattamento che hanno ricevuto un messaggio tramite il servizio di messaggistica Doctolib e ricordare loro via e-mail i messaggi non letti;
4/ Consentire agli Utenti del Servizio di Messaggistica di bloccare o sbloccare un altro Utente
5/ Reporting, debug e statistiche.

Nel caso in cui il Titolare del trattamento comunichi i dati anagrafici del Paziente a un Attore Sanitario che non fa parte del team di cura del Paziente in questione, il Titolare del trattamento deve prima ottenere il consenso del Paziente.

BASE GIURIDICA

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi operazione di Trattamento.

A titolo indicativo, il legittimo interesse potrebbe costituire la base giuridica. Il Titolare del trattamento è libero di indicare a Doctolib un'altra base giuridica.

Nel caso in cui il Titolare del trattamento comunichi i Dati anagrafici del paziente a un Attore Sanitario che non fa parte del team di cura del Paziente in questione, il Titolare del trattamento deve prima ottenere il consenso del Paziente.

INTERESSATI:

1/ Pazienti appartenenti al Database Pazienti degli Attori Sanitari che utilizzano il Servizio di Messaggistica Doctolib.
2/ Attori Sanitari o Assistenti con o senza un Account Utente Doctolib.

DATI INTERESSATI:

In linea di principio, sono considerati pertinenti alle finalità sopra menzionate i dati seguenti:

- Dati di identificazione;
- Dati di contatto
- Anamnesi medica, familiare e allergie;
- Dati della visita;
- Dati relativi alla prescrizione;
- Dati biometrici e biologici;
- Dati relativi al team di assistenza sanitaria;
- Immagini diagnostiche;
- I log di utilizzo e di connessione che riportano le "azioni commerciali" degli Utenti all'interno della Piattaforma Doctolib nonché i log tecnici che rendono conto dell'"attività" dei componenti software e hardware utilizzati dall'Utente, affinché Doctolib possa assicurare il funzionamento e l'accesso alle funzionalità richieste.

DESTINATARI DEI DATI:

- Attori Sanitari o Assistenti in possesso di un Account Utente;
- Attori Sanitari o Assistenti senza Account Utente invitati dagli Utenti a utilizzare il Servizio di Messaggistica.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
In mancanza di istruzioni in tal senso da parte del Titolare del trattamento, Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali.

In assenza di istruzioni contrarie da parte del Titolare del trattamento per una determinata conversazione, i messaggi e i Documenti sono conservati di default per 6 mesi dalla data di invio.

TRATTAMENTO N. 7: MIGLIORAMENTO DEI SERVIZI, PRODUZIONE DI STATISTICHE E ANONIMIZZAZIONE DEI DATI

OPERAZIONI DI TRATTAMENTO:

I Servizi Doctolib comportano la raccolta, la registrazione, l'organizzazione, la conservazione, l'estrazione, la consultazione e l'utilizzo, la comunicazione mediante trasmissione, l'anonimizzazione e la cancellazione dei Dati Personali di seguito elencati.

FINALITÀ:

1/ Miglioramento dei Servizi;
2/ Produzione di statistiche per conto dell'Utente/Iscritto;
3/ Anonimizzazione dei dati.

BASE GIURIDICA

Spetta al Titolare del trattamento determinare tale base giuridica prima di qualsiasi operazione di Trattamento.

INTERESSATI:

1/Abbonato/Utente come definiti nel Contratto.

DATI INTERESSATI:

Al fine di ridurre al minimo i Dati Personali trattati, il Titolare del trattamento deve assicurarsi di raccogliere e utilizzare solo i dati pertinenti e necessari rispetto alle proprie esigenze di trattamento per la gestione medica e amministrativa dei propri Pazienti.

I seguenti dati sono in linea di principio considerati rilevanti, per le finalità sopra menzionate:

- Informazioni relative all'Attore Sanitario: sesso, indirizzo postale (città);
- Dati professionali dell'Attore Sanitario: specialità, motivi di visita disponibili, orari di apertura e chiusura, particolarità relative al luogo di consultazione;
- I log di utilizzo e connessione che riportano le "azioni commerciali" degli Utenti all'interno della Piattaforma Doctolib nonché i log tecnici che riportano le "attività" dei componenti software e hardware utilizzati dall'Utente/Abbonato affinché Doctolib possa garantire la funzionamento e accesso alle funzionalità richieste;
- Informazioni relative al Paziente o Conoscente: Sesso, data di nascita (mese/anno), luogo di nascita, indirizzo postale (città di residenza);
- Stato dell'appuntamento;
- Dati Sanitari: data/ora e luogo dell'appuntamento, specializzazione del medico e natura della visita.

Salvo diversa indicazione del Titolare, Doctolib tratta tutti i Dati Personali sopra indicati al fine di fornire il Servizio oggetto del Contratto.

È probabile che questi dati siano utilizzati per la creazione di statistiche e vengano resi anonimi.

DESTINATARI DEI DATI

Si prega di fare riferimento all'elenco di cui all'articolo 11 del presente Accordo.

PERIODO DI CONSERVAZIONE:

Un periodo preciso di conservazione dei dati deve essere stabilito dal Titolare del trattamento e comunicato a Doctolib.
In mancanza di istruzioni in tal senso da parte del Titolare del trattamento, Doctolib applicherà i periodi di conservazione eventualmente raccomandati dal Garante per la protezione dei dati personali o previsti dalla Normativa in materia di Protezione dei Dati Personali.

ALLEGATO 2: MISURE TECNICHE E ORGANIZZATIVE
Appendice 2- A : Misure tecniche e organizzative standard

[Nota: questa appendice 2-A è applicabile per impostazione predefinita (tranne nel caso in cui sia impostato un Connettore tra la Piattaforma e sistemi informativi di terze parti - questo caso è disciplinato dall'appendice 2-B. Per maggiori dettagli sull'appendice applicabile, si prega di fare riferimento al contratto di abbonamento.]

SICUREZZA DEL PRODOTTO

- **Verifica identità**: successivamente alla creazione dell'account Utente, l'accesso ai servizi richiede la verifica dell'identità dell'Utente tramite il processo OnFido per verificare il possesso di un documento di identità valido..

- **Autenticazione a due fattori:** ogni volta che l'Utente si connette a nuove apparecchiature, deve fornire la sua password e un codice ottenuto via e-mail o SMS, utilizzabile una sola volta.

- **Politica delle password:** composta da un minimo di 8 caratteri tra numeri, simboli, lettere e lettere maiuscole, le password più comuni sono vietate (ad esempio, login, nome, semplici sequenze di numeri). La password deve superare un test di complessità calcolato dinamicamente analizzando la difficoltà di decifrarla.
  L'Utente deve utilizzare il proprio ID di accesso e la propria password per accedere ai Servizi.

- **Protezione della sessione Utente:**
  Le sessioni aperte possono essere sbloccate con due modalità:
  1. con password (la sessione scade automaticamente dopo 7 giorni);
  2. tramite codice PIN:
     a. I codici PIN troppo semplici non sono ammessi;
     b. la sessione si blocca automaticamente con richiesta inserimento codice PIN dopo 1 ora di inattività;
     c. la sessione scade automaticamente ogni notte.

- **Processo di recupero sicuro**: Gli account possono essere recuperati in due modi:
  - Reimpostazione della password tramite e-mail
  - Reimpostazione della password tramite SMS con supporto Doctolib sulla verifica delle informazioni sull'account prima di consentirne il recupero.

  Il successo in uno di questi modi comporta l'annullamento automatico di tutte le sessioni attive.

- **Controllo granulare degli accessi**: gli Amministratori possono conferire ad ogni Utente diritti specifici all'interno della loro organizzazione.

- **Tracciabilità delle azioni**: Le azioni dei diversi Utenti di un'organizzazione sono registrate e messe a verbale. Le azioni "sensibili" (modifica dell'accesso alle agende, creazione di account di amministratore) sono soggette a notifiche di sicurezza.

- **Protezione contro il furto dell'account**: i tentativi di connessione con password riusciti da un nuovo dispositivo sono notificati all'utente dal 2FA.

SICUREZZA DELLA PIATTAFORMA

- **Aggiornamenti di sicurezza automatici**: le patch di sicurezza sono qualificate e applicate automaticamente ai nostri componenti.

- **Sistemi operativi aggiornati e migliorati**.

- **Vigilanza e sicurezza:** monitoriamo continuamente le minacce note ed emergenti, le vulnerabilità e i vettori di attacco.
  Firewall e sistemi di filtraggio degli accessi dedicati (proxy, vpn...).
  Protezione contro gli attacchi DDoS (*distributed denial of service*).
  Protezione contro gli attacchi software (WAF).

- **Tracciabilità:** registriamo ogni azione, monitoriamo e allertiamo per qualsiasi evento di sicurezza.

- **Datacenter protetti**: HDS, ISO 27001, Tier 3, forte sicurezza fisica, personale sul posto 24/7.

DISPONIBILITÀ

- Tutti i dati sono replicati in più datacenter.
- Ogni datacenter ha diversi collegamenti di rete con l'esterno.
- Tutti i servizi e i componenti sono coperti da procedure di *disaster recovery*, per lo più automatiche.
- Qualsiasi guasto viene automaticamente rilevato e allertato da un sistema di monitoraggio completo per ogni componente tecnico e servizio aziendale.
- Attuazione di una politica di backup e recupero dei dati per combattere attacchi ransomware sul nostro database.

CIFRATURA DEI DATI

Cifratura delle comunicazioni:

- Tutti i dati scambiati con e tra i sistemi sono cifrati utilizzando i protocolli TLS.

- Gli accessi tecnici si realizzano attraverso una connessione con cifratura e autenticazioni forti, con una convalida sistematica tra pari.

Memorizzazione dei dati:

- Tutti i nostri database sono cifrati a riposo.
- Le chiavi di cifratura sono cifrate con una chiave principale creata secondo lo stato dell'arte e sono conservate presso Atos all'interno di un dispositivo informatico protetto.
- I Documenti sono protetti da divese tecniche di crittografia.
-
- Questi dati possono essere visibili solo all'Utente. Doctolib è sempre responsabile dell'archiviazione e della disponibilità dei dati, ma non può leggere le informazioni sanitarie. Nessun operatore e intermediario del sistema informatico può leggere questi dati.

CONTROLLO DELL'ACCESSO DEI DIPENDENTI

Si applica la politica del "privilegio minimo" per cui a ciascun lavoratore sono concessi solo gli accessi necessari corrispondenti alla mansione lavorativa prestata.

L'Utente stesso può concedere a un membro del team di supporto, se necessario e in caso di indagine investigativa, solo l'accesso temporaneo ai dati.

Solo alcuni membri accreditati e sensibilizzati del team dell'infrastruttura Doctolib possono accedere ai dati in caso di guasti legati alla memorizzazione dei dati.

LE MIGLIORI PRATICHE DI SICUREZZA DELLE APPLICAZIONI

Memorizzazione delle password: hashed (*tritata*) grazie alla robusta funzione di *hashing* (*bcrypt*).
Limite di velocità: i Servizi e gli Utenti sono protetti contro gli attacchi di depauperamento delle risorse (*Denial of Service*), gli attacchi di "forza bruta" e il recupero automatico dei nostri dati, attraverso un algoritmo intelligente che controlla la condivisione e l'accesso ai Servizi e blocca le richieste automatiche.

CICLO DI VITA DELLO SVILUPPO DEL SOFTWARE SICURO (S-SDLC)

Sensibilizzazione, formazione in materia di sicurezza: gli sviluppatori sono formati e resi edotti in merito alle migliori pratiche in termini di sviluppo sicuro delle applicazioni.
Sicurezza a partire dalla progettazione: Ogni nuova caratteristica del prodotto Doctolib è progettata in collaborazione con esperti di sicurezza.
Revisione del codice sorgente:
La sicurezza del codice sorgente di Doctolib viene analizzata automaticamente a ogni modifica.
Le revisioni manuali del codice sorgente vengono eseguite quando viene modificato un componente sensibile.

Verifiche di vulnerabilità:
Test di penetrazione:
Doctolib incarica regolarmente note aziende di eseguire penetration test sulle nostre applicazioni e piattaforme.

Programma di ricompense per la segnalazione di vulnerabilità (*bug bounty*):
Dipendenti e ricercatori esterni vengono premiati quando identificano una falla di sicurezza sulle nostre nel prodotto Doctolib.

ACCESSO FISICO ALLA SEDE DI DOCTOLIB

Gli uffici di Doctolib sono protetti da un allarme e dotati dei più moderni sistemi di sicurezza e di controllo degli accessi sia all'entrata, che negli ascensori o nei piani che ospitano le cosiddette aree di attività sensibili.
Tutti gli accessi autorizzati ai locali sono registrati.
Tutti i sistemi sono gestiti presso datacenter approvati. Questi sono dotati di sistemi di videosorveglianza e di sicurezza e di un servizio di sicurezza. Solo un piccolo gruppo di specialisti di Doctolib, debitamente formati, è autorizzato all'accesso. Ognuno di questi accessi è registrato.

Accesso da parte dei dipendenti dell'Istituto:

Tutti i dipendenti hanno un badge con la loro foto, che permette loro di accedere ai locali in base al loro accreditamento all'interno dell'azienda. L'accreditamento è definito secondo il ruolo del dipendente o secondo la richiesta del manager, che deve essere convalidata dal dipartimento responsabile. Indossare un badge è obbligatorio per ogni dipendente. Se un dipendente dimentica di indossare il badge, deve andare alla reception e presentare una carta d'identità o un passaporto all'addetto alla reception. L'addetto alla reception controllerà l'identità del dipendente con il database delle risorse umane e, se il controllo è positivo, rilascerà un badge temporaneo (da restituire alla reception entro la sera dello stesso giorno).

Collegamento con il Sistema Informatico dell'ente:

Il collegamento con il Sistema Informatico dell'ente può essere fatto in diversi modi: (Spuntare la casella appropriata)

- Connettore API tra l'agenda Doctolib e quella del SI
- Connettore locale, l'agenda Doctolib consente di risalire alla Scheda Paziente del SI.
- VPN IPSec tra il server e Doctolib (al fine di confermare la disponibilità).

Appendice 2- B: Misure tecniche e organizzative specifiche

[Nota: questa appendice 2-B è applicabile solo nel caso in cui sia stato istituito un Connettore per garantire l'interoperabilità tra la Piattaforma e i sistemi informativi di terze parti. Per maggiori dettagli sull'appendice applicabile, fare riferimento al Contratto di abbonamento.]

SICUREZZA DEL PRODOTTO

- **Verifica identità** successivamente alla creazione dell'account Utente, l'accesso ai servizi richiede la verifica dell'identità dell'Utente tramite il processo OnFido per verificare il possesso di un documento di identità valido.

- **Autenticazione a due fattori:** ogni volta che l'Utente si connette a nuove apparecchiature, deve fornire la sua password e un codice ottenuto via e-mail o SMS, utilizzabile una sola volta.

- **Politica delle password:** composta da un minimo di 8 caratteri tra numeri, simboli, lettere e lettere maiuscole, le password più comuni sono vietate (ad esempio, login, nome, semplici sequenze di numeri). La password deve superare un test di complessità calcolato dinamicamente analizzando la difficoltà di decifrarla.
  L'Utente deve utilizzare il proprio ID di accesso e la propria password per accedere ai Servizi.

- **Protezione della sessione Utente:**
  Le sessioni aperte possono essere sbloccate con due modalità:
  3. con password (la sessione scade automaticamente dopo 7 giorni);
  4. tramite codice PIN:
     a. I codici PIN troppo semplici non sono ammessi;
     b. la sessione si blocca automaticamente con richiesta inserimento codice PIN dopo 1 ora di inattività;
     c. la sessione scade automaticamente ogni notte.

- **Processo di recupero sicuro**: Gli account possono essere recuperati in due modi:
  - Reimpostazione della password tramite e-mail
  - Reimpostazione della password tramite SMS con supporto Doctolib sulla verifica delle informazioni sull'account prima di consentirne il recupero.

  Il successo in uno di questi modi comporta l'annullamento automatico di tutte le sessioni attive.

- **Controllo granulare degli accessi**: gli Amministratori possono conferire ad ogni Utente diritti specifici all'interno della loro organizzazione.

- **Tracciabilità delle azioni**: Le azioni dei diversi Utenti di un'organizzazione sono registrate e messe a verbale. Le azioni "sensibili" (modifica dell'accesso alle agende, creazione di account di amministratore) sono soggette a notifiche di sicurezza.

- **Protezione contro il furto dell'account**: i tentativi di connessione con password riusciti da un nuovo dispositivo sono notificati all'utente dal 2FA.

SICUREZZA DELLA PIATTAFORMA

- **Aggiornamenti di sicurezza automatici**: le patch di sicurezza sono qualificate e applicate automaticamente ai nostri componenti.

- **Sistemi operativi aggiornati e migliorati**.

- **Vigilanza e sicurezza:** monitoriamo continuamente le minacce note ed emergenti, le vulnerabilità e i vettori di attacco.
  Firewall e sistemi di filtraggio degli accessi dedicati (proxy, vpn...).
  Protezione contro gli attacchi DDoS (*distributed denial of service*).
  Protezione contro gli attacchi software (WAF).

- **Tracciabilità:** registriamo ogni azione, monitoriamo e allertiamo per qualsiasi evento di sicurezza.

- **Datacenter protetti**: HDS, ISO 27001, Tier 3, forte sicurezza fisica, personale sul posto 24/7.

DISPONIBILITÀ

- Tutti i dati sono replicati in più datacenter.
- Ogni datacenter ha diversi collegamenti di rete con l'esterno.
- Tutti i servizi e i componenti sono coperti da procedure di *disaster recovery*, per lo più automatiche.
- Qualsiasi guasto viene automaticamente rilevato e allertato da un sistema di monitoraggio completo per ogni componente tecnico e servizio aziendale.
- Attuazione di una politica di backup e recupero dei dati per combattere attacchi ransomware sul nostro database.

CIFRATURA DEI DATI

Cifratura delle comunicazioni:

- Tutti i dati scambiati con e tra i sistemi sono cifrati utilizzando i protocolli TLS.
- Gli accessi tecnici si realizzano attraverso una connessione con cifratura e autenticazioni forti, con una convalida sistematica tra pari.

Interoperabilità tra i sistemi:

- In presenza di un Connettore tra i sistemi informativi del Abbonato/Utente e i sistemi informativi di Doctolib, al fine di garantire l'interoperabilità dei sistemi, i flussi e i Documenti trasmessi tramite le API sono soggetti a decrittazione da parte dell'applicativo Doctolib prima della trasmissione.
- All'Abbonato/Utente verrà inviata una coppia di chiavi segrete (una chiave principale e una chiave di backup) da Doctolib per consentire al suo sistema informativo di

autenticarsi con il sistema Doctolib. L'Abbonato/Utente è responsabile della riservatezza di questa coppia di chiavi e di garantirne la protezione secondo le migliori pratiche, in particolare la cifratura a riposo delle chiavi e il controllo degli accessi.
- L'Abbonato/Utente deve assicurarsi che il proprio sistema informativo sia in grado di autenticarsi automaticamente con la seconda chiave segreta qualora la chiave principale venga rifiutata da Doctolib.
- In caso di sospetto di compromissione di una delle chiavi segrete, l'Abbonato/Utente deve darne immediata comunicazione a Doctolib, al fine di avviare una procedura di rinnovo della chiave.
- All'Abbonato/Utente verrà offerto da Doctolib di restringere l'uso delle chiavi segrete ad un insieme di indirizzi IP fissi del sistema informativo dell'Abbonato/Utente. Nel caso in cui l'Abbonato/Utente scelga di non limitare l'uso delle chiavi segrete ai propri indirizzi IP fissi, resta inteso che l'Abbonato/Utente è consapevole che, in caso di compromissione di una delle sue chiavi, Doctolib non potrà essere ritenuta responsabile per uso fraudolento di dette chiavi da parte di una persona o di un sistema non autorizzato.

Memorizzazione dei dati:
- Tutti i nostri database sono crittografati a riposo.
- Le chiavi di crittografia sono crittografate con una chiave master creata secondo le regole dell'arte e sono ospitate presso Atos all'interno di un dispositivo hardware sicuro.
- Questi dati possono essere visibili solo all'Utente. Doctolib è ancora responsabile dell'archiviazione e della disponibilità dei dati ma senza poter leggere le informazioni sanitarie. Nessun attore o intermediario del sistema informativo può leggere questi dati.

CONTROLLO DELL'ACCESSO DEI DIPENDENTI

Si applica la politica del "privilegio minimo" per cui a ciascun lavoratore sono concessi solo gli accessi necessari corrispondenti alla mansione lavorativa prestata.

L'Utente stesso può concedere a un membro del team di supporto, se necessario e in caso di indagine investigativa, solo l'accesso temporaneo ai dati.

Solo alcuni membri accreditati e sensibilizzati del team dell'infrastruttura Doctolib possono accedere ai dati in caso di guasti legati alla memorizzazione dei dati.

LE MIGLIORI PRATICHE DI SICUREZZA DELLE APPLICAZIONI

Memorizzazione delle password: hashed (*tritata*) grazie alla robusta funzione di *hashing* (*bcrypt*).
Limite di velocità: i Servizi e gli Utenti sono protetti contro gli attacchi di depauperamento delle risorse (*Denial of Service*), gli attacchi di "forza bruta" e il recupero automatico dei nostri dati, attraverso un algoritmo intelligente che controlla la condivisione e l'accesso ai Servizi e blocca le richieste automatiche.

CICLO DI VITA DELLO SVILUPPO DEL SOFTWARE SICURO (S-SDLC)

Sensibilizzazione, formazione in materia di sicurezza: gli sviluppatori sono formati e resi edotti in merito alle migliori pratiche in termini di sviluppo sicuro delle applicazioni.
Sicurezza a partire dalla progettazione: Ogni nuova caratteristica del prodotto Doctolib è progettata in collaborazione con esperti di sicurezza.
Revisione del codice sorgente:
La sicurezza del codice sorgente di Doctolib viene analizzata automaticamente a ogni modifica.
Le revisioni manuali del codice sorgente vengono eseguite quando viene modificato un componente sensibile.

Verifiche di vulnerabilità:
Test di penetrazione:
Doctolib incarica regolarmente note aziende di eseguire penetration test sulle nostre applicazioni e piattaforme.

Programma di ricompense per la segnalazione di vulnerabilità (*bug bounty*):
Dipendenti e ricercatori esterni vengono premiati quando identificano una falla di sicurezza sulle nostre nel prodotto Doctolib.

ACCESSO FISICO ALLA SEDE DI DOCTOLIB

Gli uffici di Doctolib sono protetti da un allarme e dotati dei più moderni sistemi di sicurezza e di controllo degli accessi sia all'entrata, che negli ascensori o nei piani che ospitano le cosiddette aree di attività sensibili.
Tutti gli accessi autorizzati ai locali sono registrati.
Tutti i sistemi sono gestiti presso datacenter approvati. Questi sono dotati di sistemi di videosorveglianza e di sicurezza e di un servizio di sicurezza. Solo un piccolo gruppo di specialisti di Doctolib, debitamente formati, è autorizzato all'accesso. Ognuno di questi accessi è registrato.

Accesso da parte dei dipendenti dell'Istituto:

Tutti i dipendenti hanno un badge con la loro foto, che permette loro di accedere ai locali in base al loro accreditamento all'interno dell'azienda. L'accreditamento è definito secondo il ruolo del dipendente o secondo la richiesta del manager, che deve essere convalidata dal dipartimento responsabile. Indossare un badge è obbligatorio per ogni dipendente. Se un dipendente dimentica di indossare il badge, deve andare alla reception e presentare una carta d'identità o un passaporto all'addetto alla reception. L'addetto alla reception controllerà l'identità del dipendente con il database delle risorse umane e, se il controllo è positivo, rilascerà un badge temporaneo (da restituire alla reception entro la sera dello stesso giorno).

Collegamento con il Sistema Informatico dell'ente:

Il collegamento con il Sistema Informatico dell'ente può essere fatto in diversi modi: (Spuntare la casella appropriata)
- Cconnettore API tra l'agenda Doctolib e quella del SI
- Cconnettore locale, l'agenda Doctolib consente di risalire alla Scheda Paziente del SI.
- VPN IPSec tra il server e Doctolib (al fine di confermare la disponibilità).