AMBULATORI.CLOUD

Documento di trasparenza sul trattamento e la sicurezza dei dati

Informazioni destinate a professionisti sanitari, personale autorizzato e pazienti

Come vengono trattati i dati, dove risiede il nucleo del servizio, quali misure sono applicate e quali soggetti possono essere coinvolti quando si attivano canali opzionali.

IDENTIFICAZIONE	INFORMAZIONE
Servizio	Ambulatori.Cloud
Versione	1.3
Data di emissione	7 settembre 2026
Classificazione	Documento pubblico
Contatto	assistenza@ambulatori.cloud

Ambito del documento Questo testo descrive il servizio dal punto di vista della trasparenza e della sicurezza. Integra, ma non sostituisce, l’informativa privacy del singolo professionista o ambulatorio, né l’accordo sul trattamento dei dati previsto dall’art. 28 GDPR.

1. Sintesi per chi utilizza il servizio

Principio guida. Il servizio è progettato per trattare soltanto i dati necessari alle funzioni abilitate e per rendere espliciti ruoli, luoghi, misure e soggetti coinvolti.

Tema	Informazione essenziale
Dove risiedono i dati principali	Il nucleo applicativo, il database e gli archivi operativi sono attestati su infrastruttura Aruba in Italia. La specifica sede fisica assegnata al singolo servizio non è esposta pubblicamente dal piano hosting.
Trasmissione	L'applicazione è configurata per imporre HTTPS. La cifratura TLS protegge il collegamento tra browser e servizio; non equivale a cifratura end-to-end dei contenuti.
Protezione negli archivi	Campi personali selezionati e allegati sono protetti con cifratura applicativa AES-256-CBC. Non viene dichiarata una cifratura indistinta di ogni dato o di ogni copia di backup.
Accessi	Gli account sono personali, con ruoli e permessi applicativi. Un secondo passaggio con codice temporaneo è previsto nei flussi configurati; non viene presentato come obbligatorio per ogni ruolo.
Servizi opzionali	Email, SMS e notifiche push comportano flussi verso i fornitori necessari. Push, CDN e strumenti ausiliari possono comportare trattamento fuori dallo SEE.
Uso commerciale dei dati	Il servizio gestionale non è progettato per vendere dati sanitari, mostrare pubblicità comportamentale o assumere decisioni cliniche automatizzate.
Conservazione	Non esiste un termine unico valido per ogni dato. I tempi dipendono da finalità, obblighi professionali e fiscali, istruzioni del titolare, contratto e configurazione tecnica.

Nessuna promessa assoluta. Nessun sistema informatico può garantire rischio zero. La formulazione “sicurezza garantita al 100%” non è adottata in questo documento: la sicurezza è un processo continuo, proporzionato al rischio e verificabile.

2. Chi fa cosa nel trattamento

Per i dati dei pazienti inseriti nell'ambito dell'attività sanitaria, il professionista o la struttura che decide finalità e modalità del trattamento opera normalmente come titolare del trattamento. Ambulatori.Cloud, quando tratta tali dati per erogare il servizio secondo istruzioni documentate, opera normalmente come responsabile del trattamento ai sensi dell'art. 28 GDPR.

Ambulatori.Cloud può invece agire come titolare autonomo per i dati necessari alla gestione dei propri contratti, fatturazione, richieste commerciali, assistenza, tutela del servizio e sicurezza dei propri sistemi. La qualifica effettiva va verificata per ciascun flusso e formalizzata nei documenti contrattuali.

Soggetto	Ruolo tipico	Responsabilità principale
Professionista / ambulatorio	Titolare	Stabilisce finalità, basi giuridiche, tempi di conservazione, autorizzazioni, informativa e riscontro ai diritti dei pazienti.
Ambulatori.Cloud	Responsabile per il servizio; titolare per proprie finalità	Eroga e mantiene la piattaforma, applica le misure concordate, assiste il titolare e disciplina gli eventuali sub-responsabili.
Personale di studio	Autorizzato dal titolare	Accede soltanto ai dati necessari alle mansioni, usando credenziali individuali e rispettando le istruzioni ricevute.
Paziente	Interessato	Riceve informazioni chiare, può esercitare i diritti applicabili e tutela le proprie credenziali quando dispone di un accesso.
Fornitori tecnici	Responsabili o destinatari, secondo il servizio	Trattano dati limitati alla funzione attivata e secondo contratto, legge e proprie condizioni applicabili.

3. Quali dati possono essere trattati

Le categorie effettive dipendono dai moduli scelti dal professionista e dall'uso concreto. I dati relativi alla salute sono categorie particolari ai sensi dell'art. 9 GDPR e richiedono tutele rafforzate.

Categoria	Esempi	Finalità tipiche
Identificativi e contatti	Nome, cognome, codice fiscale, indirizzo, email, telefono	Anagrafica, comunicazioni di servizio, identificazione, gestione amministrativa
Agenda e prestazioni	Appuntamenti, professionista, sede, stato, promemoria	Organizzazione dell'attività e continuità operativa
Dati relativi alla salute	Informazioni inserite nelle schede, annotazioni, documenti e allegati pertinenti	Attività sanitaria e gestione collegata, secondo le scelte del titolare
Messaggi e documenti	Oggetto, testo, allegati, destinatari, stato di lettura	Comunicazioni tra struttura, professionisti, personale e pazienti
Amministrazione e adempimenti	Prestazioni, documenti fiscali e dati amministrativi	Contabilità, fatturazione e obblighi normativi
Account e sicurezza	Username, elementi di autenticazione, ruolo, token, IP, user agent, esiti di accesso	Autenticazione, prevenzione abusi, diagnosi tecnica e gestione incidenti
Assistenza	Richieste, contenuto del ticket, recapiti e informazioni tecniche	Supporto, correzione di anomalie e tutela contrattuale

I dati possono essere forniti dal paziente, dal professionista o dal personale autorizzato; alcuni dati tecnici sono generati automaticamente durante l'uso. Il servizio non deve essere usato per raccogliere informazioni eccedenti rispetto alla finalità dichiarata.

4. Perché i dati vengono trattati

Le basi giuridiche non sono identiche per ogni soggetto o funzione. Il titolare deve descriverle nella propria informativa. A seconda del caso possono rilevare l'esecuzione di un contratto o di misure precontrattuali, obblighi di legge, interesse legittimo adeguatamente bilanciato e, per i dati sanitari, le condizioni dell'art. 9 GDPR connesse alla diagnosi, assistenza o terapia sanitaria da parte di professionisti soggetti al segreto professionale.

Il consenso non è una formula universale: può essere necessario per funzioni ulteriori rispetto alla cura, per specifici canali o per finalità facoltative, ma non deve essere richiesto quando il trattamento sanitario è già fondato su un'altra idonea condizione di liceità. Marketing e comunicazioni promozionali richiedono una valutazione separata.

5. Architettura e localizzazione

Nucleo del servizio. Browser dell'utente → connessione HTTPS → applicazione Ambulatori.Cloud su infrastruttura Aruba in Italia → database e archivi operativi sul server.

Il dominio applicativo pubblico risponde attraverso infrastruttura Aruba. Aruba dichiara che i servizi principali di hosting, email e PEC sono gestiti in data center italiani e descrive una rete nazionale con sedi ad Arezzo, Ponte San Pietro (Bergamo) e Roma. Dal solo piano hosting non è possibile identificare con affidabilità la sala o il data center assegnato a questa singola istanza; per questa ragione il documento non indica una città come certezza non provata.

La collocazione italiana del nucleo non significa che ogni funzione accessoria resti sempre in Italia: quando un utente attiva notifiche, librerie distribuite da CDN o servizi esterni di utilità, il browser o il server possono comunicare con altri fornitori. La sezione seguente rende questi flussi espliciti.

6. Fornitori, destinatari e possibili trasferimenti

Servizio / soggetto	Dati potenzialmente coinvolti	Quando avviene	Localizzazione e cautela
Aruba S.p.A.	Dati applicativi, database, file, log tecnici; email o SMS se usati	Funzionamento ordinario del nucleo e dei canali Aruba	Infrastruttura principale dichiarata in Italia. Contratto, piano di backup e servizi attivi devono essere conservati dal fornitore e dal titolare.
Servizio push remoto e reti push del dispositivo	Token del dispositivo e payload della notifica	Solo per notifiche abilitate	Possono intervenire Vercel e fornitori come Google, Apple o Mozilla su infrastrutture globali. I messaggi devono essere generici e non contenere dettagli sanitari.
CDN per componenti dell'interfaccia	IP, user agent, URL richiesto e metadati tecnici	Quando una pagina carica una libreria da una rete esterna	Il fornitore CDN può operare globalmente. L'auto-ospitalità delle risorse è preferibile per ridurre terze parti.
Generatore QR esterno	Indirizzo temporaneo usato per il collegamento del dispositivo e metadati tecnici	Solo nella funzione di associazione tramite QR	L'integrazione va ridotta o sostituita con generazione locale; non deve contenere dati clinici.
Provider email del destinatario	Indirizzo e contenuto dell'email	Quando si inviano comunicazioni o codici via email	La consegna esce dal perimetro applicativo e segue anche le condizioni del provider scelto dal destinatario.

Trasferimenti fuori dallo SEE. Non possono essere esclusi in modo assoluto per i servizi opzionali o globali. Quando applicabile, il titolare e il fornitore devono verificare decisioni di adeguatezza, clausole contrattuali standard, DPA, sub-responsabili, localizzazione configurabile e misure supplementari.

7. Misure tecniche e organizzative

7.1 Collegamenti e protezione dei dati

- HTTPS è imposto dalla configurazione applicativa per proteggere i dati durante il transito tra utente e servizio.
- Campi personali selezionati nel database utilizzano cifratura applicativa AES-256-CBC con vettore associato al record.
- Gli allegati dei messaggi sono cifrati prima della memorizzazione sul server; i nomi fisici sono casuali e non descrittivi.
- Le chiavi e i segreti operativi devono risiedere nella configurazione protetta dell'ambiente di produzione, con accessi limitati, copia di sicurezza separata e procedura di sostituzione documentata.
- Non viene dichiarata una cifratura end-to-end: il servizio deve poter decifrare i dati necessari a erogare le funzioni autorizzate.

7.2 Identità, ruoli e sessioni

- Account individuali e ruoli distinti per amministrazione, professionisti, personale e pazienti.
- Controlli applicativi limitano la visualizzazione o l'azione in base al ruolo, al modulo e al contesto professionista/paziente.
- Codice temporaneo a uso singolo nei flussi per i quali è configurato; non è descritto come MFA universale per ogni account.
- La configurazione base prevede scadenza della sessione e rigenerazione periodica dell'identificativo; i valori di produzione devono essere sottoposti a verifica.
- Token anti-CSRF sono utilizzati nelle operazioni protette dei moduli; i controlli devono essere mantenuti durante ogni evoluzione dell'interfaccia.

7.3 Allegati e messaggistica

- Formati ammessi limitati a PDF, immagini comuni, documenti Office e testo; dimensione massima applicativa pari a 15 MB.
- Compressione applicata quando produce un risparmio utile, seguita dalla cifratura prima del salvataggio.
- Pulizia prevista per gli allegati di bozze di risposta abbandonate oltre 48 ore, se l'attività pianificata è effettivamente attiva.
- Non viene dichiarata la presenza di scansione antivirus automatica degli upload: il titolare deve applicare prudenza ai file ricevuti e il fornitore deve valutare un controllo antimalware dedicato.

7.4 Registrazione degli eventi

Il sistema registra eventi tecnici e di sicurezza quali accessi, esiti di autenticazione, invio o verifica di codici temporanei, recupero credenziali e anomalie. I log possono includere IP e user agent. Non viene dichiarata una traccia completa e immutabile di ogni singola consultazione o modifica: eventuali requisiti di audit clinico o normativo devono essere definiti separatamente.

7.5 Continuità e copie di sicurezza

L'applicazione dispone di procedure per copia e dump del database e l'infrastruttura Aruba offre opzioni di ridondanza e backup. Frequenza, conservazione, cifratura, prove di ripristino, RPO e RTO dipendono però dal piano realmente acquistato e dalle procedure operative: questo documento non attribuisce valori non verificati. Tali elementi devono essere allegati al contratto o alla scheda di esercizio della specifica installazione.

8. Stato delle garanzie dichiarate

Per evitare formule ambigue, le affermazioni sono classificate in base al tipo di riscontro disponibile.

Stato	Cosa comprende	Come va gestito
Verificato nell’architettura applicativa	Controlli di ruolo, configurazione HTTPS, cifratura applicativa di campi selezionati e allegati, limiti agli upload, log di eventi e servizi esterni richiamati dal software.	Da riesaminare a ogni rilascio significativo.
Dipendente dall’ambiente di produzione	Segreti e chiavi effettive, politica account, OTP per ruolo, cookie e header restituiti dal proxy, attività pianificate, configurazione email e push.	Da verificare con checklist di esercizio e prova documentata.
Dipendente dal contratto del provider	Backup, retention delle copie, localizzazione assegnata, SLA, sub-responsabili, DPA e garanzie per trasferimenti.	Da comprovare con ordine, DPA, elenco fornitori e allegato tecnico aggiornati.
Non dichiarato	Certificazione del software, audit indipendente periodico, penetration test recente, monitoraggio SOC continuativo, antivirus sugli upload, rischio zero.	Non presentare come garanzia finché non esiste evidenza formale.

9. Conservazione, cancellazione e restituzione

Il principio applicato è conservare i dati per il tempo necessario e non oltre. La durata concreta è stabilita dal titolare considerando finalità sanitarie, obblighi legali e fiscali, prescrizione, difesa di diritti e istruzioni professionali. Una durata generica di 30 giorni non è adeguata per tutti i contenuti e non viene dichiarata.

Insieme di dati	Criterio di conservazione	Cancellazione / uscita
Anagrafiche, agenda e dati sanitari	Tempi definiti dal titolare in base a finalità, normativa e responsabilità professionale.	Cancellazione o anonimizzazione su istruzione verificata, quando non prevalgono obblighi di conservazione.
Documenti amministrativi e fiscali	Per il periodo imposto dalla disciplina applicabile e dalle esigenze di difesa.	Eliminazione al termine del periodo legale, secondo la policy del titolare.
Messaggi e allegati	Per la durata necessaria alla comunicazione e alla documentazione della relazione; bozze abbandonate soggette a pulizia tecnica prevista.	Eliminazione dall’archivio operativo; le copie di backup seguono il ciclo di rotazione concordato.
Log di sicurezza	Periodo limitato ma sufficiente a prevenire abusi, analizzare incidenti e tutelare il servizio.	Rotazione periodica secondo policy tecnica e vincoli legali.
Account e contratto	Durata del rapporto più il periodo necessario per obblighi e contestazioni.	Disattivazione tempestiva, restituzione/esportazione ove prevista e successiva cancellazione controllata.
Backup	Ciclo definito dal piano e dalla procedura di continuità.	Scadenza per sovrascrittura o cancellazione controllata; recupero solo per finalità di ripristino.

10. Diritti delle persone

Nei casi previsti dal GDPR, l’interessato può chiedere accesso, rettifica, cancellazione, limitazione, opposizione e portabilità, oltre a proporre reclamo al Garante per la protezione dei dati personali. L’applicabilità del singolo diritto dipende dalla base giuridica e dal contesto.

1. Per dati gestiti dal proprio medico o ambulatorio, rivolgersi prima di tutto al titolare indicato nell’informativa ricevuta.
2. Ambulatori.Cloud assiste il titolare nelle verifiche tecniche e risponde direttamente quando opera come titolare autonomo.
3. La richiesta deve permettere di identificare la persona senza raccogliere documenti o dati eccedenti.
4. Contatto generale del servizio: assistenza@ambulatori.cloud. Il recapito privacy specifico del professionista resta quello indicato nella sua informativa.

11. Gestione degli incidenti e delle violazioni

Un incidente può riguardare perdita di disponibilità, accesso non autorizzato, divulgazione, alterazione o perdita di dati. La procedura deve prevedere rilevazione, contenimento, conservazione delle evidenze, valutazione dell’impatto, ripristino e azioni correttive.

Quando Ambulatori.Cloud opera come responsabile, informa il titolare senza ingiustificato ritardo e fornisce le informazioni disponibili. Il titolare valuta il rischio per le persone e, quando richiesto, notifica la violazione al Garante entro 72 ore dal momento in cui ne è venuto a conoscenza; in presenza di rischio elevato valuta anche la comunicazione agli interessati.

12. Responsabilità condivisa

La protezione non dipende solo dal server. Professionisti e personale incidono direttamente sul rischio e devono applicare almeno le seguenti regole:

- usare un account personale e non condividere password o codici temporanei;
- assegnare il ruolo minimo necessario e revocare subito gli utenti che cambiano mansione o cessano il rapporto;
- proteggere PC e smartphone con aggiornamenti, blocco schermo, antivirus dove applicabile e backup locale controllato;
- evitare dettagli sanitari in SMS, email e notifiche push quando non strettamente necessari;
- verificare destinatario e allegati prima dell’invio; non trasferire dati in archivi personali o non autorizzati;
- segnalare immediatamente accessi sospetti, dispositivi smarriti, messaggi inviati al destinatario errato o anomalie;
- definire e riesaminare almeno annualmente ruoli, conservazione, fornitori attivi e istruzioni al personale.

13. Cosa il paziente deve sapere

Domanda	Risposta
Chi decide come usare i miei dati?	Il medico o la struttura indicati nella relativa informativa, salvo i trattamenti che Ambulatori.Cloud svolge per proprie finalità amministrative e di sicurezza.
Dove sono i dati principali?	Sul nucleo applicativo e sugli archivi Aruba in Italia. Alcune funzioni opzionali comunicano con altri fornitori, come indicato nella sezione 6.
Il gestionale è una cartella clinica elettronica?	È una piattaforma gestionale per attività ambulatoriali; l'uso concreto e i documenti caricati sono determinati dal professionista. Non va confusa automaticamente con i sistemi pubblici di Fascicolo Sanitario Elettronico.
Le notifiche contengono dati sanitari?	Devono essere formulate in modo generico. È preferibile mostrare soltanto che è disponibile una nuova comunicazione e richiedere l'accesso autenticato per leggerne il contenuto.
Posso chiedere una copia o la correzione?	Sì, nei limiti previsti dalla legge, contattando il titolare indicato nell'informativa del professionista.
I dati sono sicuri al 100%?	Nessun servizio serio può promettere rischio zero. Sono applicate misure proporzionate e il rischio viene ridotto con tecnologia, procedure e comportamenti corretti.

14. Impegni di trasparenza e aggiornamento

- Mantenere allineati il presente documento, l'informativa privacy, il contratto ex art. 28 GDPR e l'elenco dei sub-responsabili.
- Comunicare modifiche rilevanti a localizzazione, canali, finalità o fornitori prima che incidano sui trattamenti affidati.
- Documentare le verifiche della configurazione di produzione, incluse chiavi, account privilegiati, backup, ripristino e attività pianificate.
- Valutare una DPIA quando natura, scala, tecnologie o contesto rendono probabile un rischio elevato per le persone.
- Adottare privacy e sicurezza fin dalla progettazione, riducendo dipendenze esterne e contenuto dei messaggi fuori piattaforma.

15. Evidenze da conservare a supporto

Per trasformare la trasparenza in responsabilizzazione documentata, titolare e fornitore dovrebbero poter esibire, secondo il rispettivo ruolo:

- registro dei trattamenti e, ove necessario, valutazione d'impatto;
- contratto e istruzioni ex art. 28, elenco aggiornato dei sub-responsabili e relativi DPA;
- inventario dei servizi opzionali effettivamente attivi per ciascun ambulatorio;
- policy di conservazione, cancellazione, backup e prova di ripristino;
- matrice ruoli/permessi e riesame periodico degli account;
- procedura per incidenti e data breach, con registro delle decisioni;
- evidenze di aggiornamento, vulnerability management e test proporzionati al rischio;
- informazioni rese agli utenti e registrazione delle versioni pubblicate.

16. Riferimenti normativi e tecnici

R1 — Regolamento (UE) 2016/679 (GDPR), testo ufficiale EUR-Lex

R2 — Garante Privacy, misure di sicurezza e art. 32 GDPR

R3 — Garante Privacy, violazioni di dati personali (data breach)

R4 — Garante Privacy, valutazione d’impatto (DPIA)

R5 — Garante Privacy, chiarimenti sull’applicazione della disciplina per i dati sanitari

R6 — Aruba, GDPR e localizzazione dei servizi

R7 — Aruba, certificazioni e standard

R8 — Aruba, rete dei data center

R9 — Google Firebase, privacy e localizzazione dei servizi push

R10 — Vercel, Data Processing Addendum

R11 — Apple, servizio di notifiche remote APNs

17. Nota finale

Documento da mantenere vivo. La versione pubblicata deve riflettere la configurazione e i contratti realmente in uso. Una funzione disattivata non genera il relativo flusso; una nuova integrazione, un diverso provider o una modifica sostanziale richiedono riesame prima della comunicazione agli utenti.

Contatto generale: assistenza@ambulatori.cloud — Sito informativo: https://www.ambulatori.cloud