Descrizione del Servizio ReferOn

La piattaforma ReferOn offre un servizio che consente di recuperare referti e altri documenti in formato PDF attraverso un trasferimento sicuro in modalità “on demand”. L'operazione avviene mediante richiesta al backend dell’app, che a sua volta interagisce con il repository della struttura aderente selezionata, trasferendo i documenti in formato “base64”.

Il servizio è accessibile esclusivamente tramite app mobile per sistemi Android e iOS, disponibile nei rispettivi store. Il funzionamento della piattaforma ReferOn garantisce che i documenti/referti siano disponibili in modo:

- **Non persistente e disponibilità limitata nel tempo**: I documenti/referti vengono richiesti e trasferiti direttamente dai sistemi documentali delle strutture aderenti all’app richiedente tramite comunicazioni machine-to-machine; il servizio è configurabile e per ogni tipologia di documento è possibile stabilire la relativa disponibilità temporale. I documenti potrebbero essere memorizzati, per un periodo limitato di tempo, su sistemi di storage basati su Crittografia con Transparent Data Encryption (TDE)*.
- **Sicuro**: Il servizio utilizza protocolli “https” e informazioni crittografate. Solo il backend della piattaforma riceve e trasferisce i dati all’app, evitando così di esporre i punti di accesso ai dati.
- **Aggiornato**: I documenti/referti sono richiesti in tempo reale ai sistemi documentali delle strutture aderenti al servizio o al sistema di storage basati su Crittografia con Transparent Data Encryption (TDE).

Per quanto riguarda i referti, ReferOn gestisce il servizio di download per conto delle strutture sanitarie aderenti, in conformità al DPCM 8 agosto 2013 e successive modifiche, nonché alle Linee guida del Garante per la protezione dei dati personali. I referti sono disponibili tramite la piattaforma per 45 giorni dalla data di generazione del referto stesso, come previsto dalle Linee Guida del Garante Privacy del 19 novembre 2009. Dopo tale periodo, l’accesso ai referti tramite ReferOn non sarà più possibile. Per altri tipi di documenti, la durata di disponibilità digitale è stabilita dalla struttura aderente.

ReferOn è un servizio opzionale, e permette agli utenti che vi aderiscono di accedere ai propri documenti/referti tramite tablet o smartphone (Android/iOS), con la possibilità di visualizzarli, inviarli a terzi (come il proprio medico curante), o stamparli direttamente dal proprio dispositivo. L’accesso al servizio avviene tramite credenziali (codice fiscale come username e password), assegnate al momento dell’adesione. La password impostata all’atto della sottoscrizione è sempre possibile modificarla autonomamente tramite l’app.

I documenti disponibili tramite ReferOn vengono trasferiti “on demand” direttamente dai repository delle strutture aderenti o da sistemi di storage basati su Crittografia con Transparent Data Encryption (TDE), senza essere memorizzati su supporti legati alla piattaforma. Il trasferimento avviene in modalità “base64” con protocollo “https”, garantendo un processo sicuro end-to-end dal repository al dispositivo dell’utente.

L’adesione al servizio è facoltativa, e la mancata accettazione dei termini non consentirà l'accesso al servizio descritto; tuttavia, i documenti/referti continueranno ad essere disponibili secondo le procedure adottate dalle singole strutture aderenti (ad esempio, in formato cartaceo).

L'accesso al servizio avviene tramite una comunicazione di invito fornita dalla struttura aderente, che può essere inviata a mezzo e-mail o consegnata su supporto cartaceo. La comunicazione include le istruzioni per scaricare l’app ReferOn e collegarla alla struttura invitante mediante scansione del QR-Code contenuto nell’invito.

I dati archiviati dalla piattaforma ReferOn per il servizio includono:

- Codice Fiscale crittografato dell'utente.
- Numero di cellulare crittografato (necessario per l'invio di token tecnici).
- Password di accesso crittografata.
- Identificativo della struttura aderente connessa.
- Identificativo del dispositivo mobile per notifiche push.
- Altri dati tecnici non riconducibili all'utente come persona fisica.

I dettagli anagrafici degli utenti rimangono negli archivi della struttura aderente e non vengono trasferiti a ReferOn, che gestisce solo il Codice Fiscale opportunamente crittografato tramite protocolli sicuri. I documenti/referti vengono trasferiti ai dispositivi degli utenti in formato PDF con modalità "base64" e possono essere visualizzati con sistemi di produttività personale installati sul dispositivo utente a suo carico (es. Acrobat Reader).

Le strutture aderenti al servizio sono elencate di seguito, con link ai rispettivi siti/portali per consultare il responsabile del trattamento e l'informativa sulla privacy oppure scrivere una mail al DPO:

- **Clinica Montevergine:** Privacy Policy
- **Laboratorio Aeclanum:** Laboratorio Aeclanum
- **Ospedale Cosenza:** Informativa Trattamento Dati
- **Casa di Cura Santa Rita – Atripalda (Gruppo Nefrocenter) - mail**: dpo@clinicasantarita.it
- **Centro di Radiodiagnostica Medica Aprile**: Contatti Centro Aprile
- **Ospedale Evangelico Betania**: Politica sulla Privacy

Accettando i presenti termini di servizio, l'utente conferma di aver compreso le modalità di trattamento dei dati personali e le dinamiche di funzionamento del servizio ReferOn, consentendo al trattamento dei dati necessari. L'utente è informato che il servizio è opzionale e che nessun documento/referto verrà trasferito senza adesione esplicita. L'utente può eliminare i dati gestiti dal servizio in qualsiasi momento tramite l'app.

Questa informativa è soggetta a modifiche; pertanto, è responsabilità dell'utente aggiornarsi accedendo alle funzionalità disponibili nell'app.

(*) Transparent Data Encryption (TDE)

I documenti archiviati sono conservati in formato BLOB e quindi non visibili; sono inoltre protetti tramite Transparent Data Encryption (TDE), una tecnologia di crittografia avanzata nativa (byDesign), che garantisce la sicurezza delle informazioni a riposo ed assicura che tutti i dati personali, inclusi eventuali documenti sensibili, siano custoditi in forma cifrata e risultino illeggibili senza le chiavi di decodifica autorizzate. TDE è una tecnologia implementata nativamente nei database ed il suo scopo principale è impedire l'accesso non autorizzato ai file del database e ai relativi backup.
L'adozione di TDE rappresenta una misura di sicurezza fondamentale per la conformità alle normative sulla protezione dei dati, garantendo che le informazioni sensibili non possano essere compromesse in caso di furto o perdita dei file del database.
L'accesso ai dati in chiaro è quindi riservato esclusivamente agli utenti autorizzati, secondo principi di autenticazione e controllo degli accessi di tipo strong, il tutto nel pieno rispetto della vigente normativa in tema di sicurezza delle informazioni. Principi di responsabilità e sicurezza nell'intera soluzione DB:

- I dati personali non vengono mai archiviati o trasmessi in chiaro.
- Le chiavi di crittografia sono gestite in modo sicuro e accessibili solo a personale autorizzato.
- Ogni tentativo di accesso non autorizzato ai dati è monitorato e registrato per garantire la massima trasparenza e protezione.