REFERTI WEB – VALUTAZIONE IMPATTO G.D.P.R.

RESPONSABILE DEL TRATTAMENTO			
Denominazione	Bollino IT S.p.A. a socio unico		
Partita Iva	06344961211		
Indirizzo	Via delle Industrie, 31		
Città	Napoli	Cap	80147
Legale Rappresentante	Ruggiero Bollino		
Data Protection Officer	Francesco Donato – DNTFNC83H28F839N f.donato@bollino.com		

Scopo del documento

Il presente documento ha lo scopo di consentire ai clienti di Bollino IT S.p.A. in qualità di Titolari del Trattamento di ottenere le informazioni necessarie ad effettuare la propria valutazione di impatto come prescritto dal Reg UE 2016/679.

Il documento è da considerarsi un supporto tecnico, come prescritto dalla normativa ogni valutazione è condotta dal Titolare del trattamento secondo le metodologie e le considerazioni che riterrà più idonee.

Il presente documento, nello specifico, si focalizza sul modulo per la refertazione web,

Panoramica

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento (azienda produttrice del referto) è responsabile della sicurezza dei dati personali gestiti. I dati sono affidati al Responsabile che dispone dello strumento informatico per offrire il servizio di consultazione/consegna all'interessato

Ci sono standard applicabili al trattamento?

Linee guida in tema di referti on-line - 19 novembre 2009 (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1679033)

REFERTI WEB – VALUTAZIONE IMPATTO G.D.P.R.

Quali sono le finalità del trattamento?

Semplificare le procedure di accesso degli interessati ai propri referti diagnostici svincolando dall'accesso fisico presso lo sportello della struttura diagnostica

Quali sono le categorie di interessati?

Sono interessati del trattamento i pazienti della struttura diagnostica che si configura quale Titolare del Trattamento

Quali categorie di dati personali sono trattati?

Dati Personali – ovvero dati anagrafici degli interessati
Particolari categorie di dati personali – ovvero dati relativi allo stato di salute degli interessati

Accessibilità dei dati da parte del Responsabile

Il Responsabile del Trattamento potrà accedere a tali dati esclusivamente tramite propri dipendenti e collaboratori all'uopo incaricati per finalità di natura manutentiva del sistema, previa richiesta assistenza da parte del Titolare del Trattamento. Le operazioni di aggiornamento non prevedono diretta accessibilità ai dati; ove tale esigenza di accesso fosse prevista la stessa è monitorata mediante file di log a disposizione del Titolare del Trattamento.

Basi legali per il trattamento

Il trattamento è legale in funzione del consenso richiesto ai sensi del art.9 comma 2 lettera a) del GDPR, ad opera del Titolare del Trattamento. Il Responsabile del trattamento non assume alcuna responsabilità in caso di base legale non rispettata ad opera del Titolare. È in capo al Titolare del Trattamento la consegna della utenza e della password in conformità alle disposizioni normative vigenti.

Misure di sicurezza connesse al trattamento implementate dal Responsabile del Trattamento

Crittografia

Le comunicazioni (tra browser e server) avvengono sul protocollo SSL con Algoritmo di firma SHA-256 attraverso algoritmo crittografico asimmetrico RSA con chiave a 2048 bit. I referti prodotti sono inviati al server su protocollo SSL con la stessa cifratura di cui sopra.

Storage

I dati sono conservati nel DB tranne gli allegati che sono su File System. Entrambi sono cifrati con chiavi simmetrica a 192bit. Anche le URL sono cifrate.
Il client non riporta il percorso e le directory sul filesystem dell'informazione essendo essa nascosta o cifrata

Controllo degli accessi logici

Il profilo è creato in modo automatico dal sistema Bollino che gestisce il flusso di prenotazione, accettazione, esecuzione, fatturazione. Il profilo è creato all'atto dell'accettazione in struttura con comunicazione SSL tra il sistema generante (BollinoData) e l'applicativo in oggetto. La password rispetta i requisiti previsti dal garante (lunghezza minima 8 caratteri, complessità e non ripetibilità) ed è generata in modo casuale con obbligo di modifica all'atto del primo accesso. Il sistema memorizza in file di log gli accessi e i tentativi falliti

Tracciabilità

Per motivi di sicurezza, il sistema traccia gli accessi e i tentativi di accesso oltre alla data di download del referto

Archiviazione

I referti sono conservati in modalità crittografata su filesystem e cancellati entro 45 giorni dalla loro creazione o su azione dell'interessato (attraverso il suo account). I dati accessibili sono profilati, ogni utente accede solo ai suoi dati anagrafici (nome, cognome, nascita, comune residenza) e ai dati utili a riconoscere l'esame (tipologia di esame effettuato e data dell'esame).

Minimizzazione dei dati

I dati accessibili da parte del Responsabile del Trattamento sono solo quelli relativi all'utente che ha avuto accesso all'account e solo se non sono sopraggiunti i 45 giorni dalla loro creazione. I dati dell'utente sono solo quelli anagrafici. Il Responsabile del Trattamento non accede a particolari categorie di dati personali

Vulnerabilità

L'applicativo è installato su server Aruba e quindi il servizio è disponibile come servizio SaaS. Gli aggiornamenti di sicurezza sono effettuati dal provider dei servizi SaaS. Il provider gestisce anche la sicurezza per gli accessi al server. Gli aggiornamenti dell'applicativo, di sicurezza ed evolutivi, sono effettuati dal personale di Bollino e tracciati e documentati su sistema gestionale interno.

Lotta contro il malware

Aggiornamenti di sicurezza eseguiti dal provider del servizio (Aruba)

Gestione postazioni

Il server che fornisce il servizio è di proprietà del provider del servizio (Aruba). Bollino effettua solo attività di aggiornamento evolutivo e di sicurezza del codice dell'applicativo con personale interno, attraverso canale protetto (SSL o SFTP) con tracciamento delle attività su gestionale interno.

Sicurezza dei siti web

L'applicativo è un applicativo WEB. L'accesso al servizio è effettuato attraverso browser su protocollo SSL. Gli aggiornamenti evolutivi sono effettuati con lo stesso meccanismo o su protocollo SFTP. La sessione è mantenuta utilizzando la tecnologia dei cookies. I cookie di sessione sono cifrati, non persistenti, hanno il flag secure attivato e l'attributo HttpOnly impostato. I cookie non contengono informazioni critiche quali password e non sono composti da parti predicibili come username o valori elaborati basati su algoritmi sequenziali. L'identificatore della sessione nel cookie ha lunghezza pari a 256 bit. Il tempo di scadenza oltre il quale non è più considerato valido è settato a 30 min. La sessione ha la stessa durata

REFERTI WEB – VALUTAZIONE IMPATTO G.D.P.R.

Backup

I backup dell'applicativo sono gestiti dal provider ARUBA. I servizi di Web Hosting Aruba Business sono erogati mediante un sistema ridondato e clusterizzato su piattaforma VMware vSphere ed i dati sono ospitati su storage SAN dedicati con replica e backup di tipo geografico che sfruttano la rete di data center del gruppo Aruba.it, per la massima sicurezza di disponibilità del servizio e di integrità dei dati. Il Backup è giornaliero, le informazioni sono consultabili direttamente al link: https://hosting.aruba.it/sicurezza.aspx

Manutenzione

La manutenzione fisica dei dispositivi è demandata al provider Aruba, le informazioni connesse sono consultabili al link: https://hosting.aruba.it/sicurezza.aspx

Controllo degli accessi fisici

Il controllo degli accessi fisici è riservato al personale del provider (Aruba) secondo le policy del Data Center e consultabile al link: https://hosting.aruba.it/sicurezza.aspx

Sicurezza dell'hardware

I locali adibiti ai server sono nella ServerFarm di Aruba e sottoposti alla sua gestione e sicurezza. I criteri adottati dal provider sono consultabili al link: https://hosting.aruba.it/sicurezza.aspx

Redazione

Approvazione

BOLLINO IT S.p.A.
A SOCIO UNICO
Via delle Industrie, 31 - 80147 NAPOLI
Tel. 081 5592819 - Fax 081 5592820
Part. IVA 06344961211