BOLLINODATA – 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.

Contesto

Panoramica del trattamento

Quali sono le responsabilità connesse al trattamento?

BollinoData, inteso come strumento software, non contiene, nativamente, dati di natura sensibile; è sempre il cliente ad alimentarlo con i dati dei propri pazienti, in funzione degli specifici setting diagnostici erogati. Di conseguenza la struttura sanitaria cliente è il Titolare del Trattamento dei dati personali e delle particolari categorie di dati personali che sono gestite da BollinoData; Bollino IT Spa si configura, invece, quale Responsabile del Trattamento per gli accessi che opera sul software in assistenza e manutenzione (ivi inclusi gli aggiornamenti) e la relativa possibilità di accedere ai data base oltre che al codice sorgente (quando applicabile).

La Responsabilità di Bollino IT è limitata all'integrità ed al funzionamento del software oltre che al comportamento assunto dagli incaricati di Bollino IT S.p.A. in fase di accesso ai

database e quindi ai dati personali e alle particolari categorie di dati personali dei pazienti gestiti dal cliente.

Bollino IT Spa non è responsabile, con riferimento alla fornitura di BollinoData, delle attività di backup dei database che restano in capo alla gestione del cliente delle proprie risorse informatiche.

Ci sono standard applicabili al trattamento?

UNI EN ISO 9001:2015
UNI EN ISO 13485:2016
UNI EN ISO 27001:2017
Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017,
Relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio
UNI CEN ISO/TR 14969 Dispositivi medici. Sistemi di gestione della qualità Guida all'applicazione della ISO 13485
UNI CEI EN ISO 14971 dispositivi medici. Applicazione della gestione dei rischi ai dispositivi medici
Regolamento (UE) 2017/745 relativo ai dispositivi medici – Allegato VIII
MedDev 2.4/1 rev. 9 – Classificazione

Quali sono le finalità di trattamento?

Il software ha una finalità definita contrattualmente con il cliente; è lo stesso cliente in qualità di titolare del trattamento che ha la responsabilità di garantire legittimità, specificità e rendere espliciti gli scopi del trattamento nei confronti dei propri pazienti. Il trattamento dei dati ha lo scopo di gestire il processo sanitario dal punto di vista IT, nel rispetto dei requisiti connessi alla normativa sui Dispositivi Medici in vigore.

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?

Il software tratta dati personali e particolari categorie di dati personali (ovvero dati idonei a rilevare lo stato di salute) dei pazienti del titolare del trattamento. Sono trattati anche dati connessi alle condizioni di esenzione del paziente (anch'essi genericamente rientranti i particolari categorie di dati personali) e dati di natura amministrativa per il relativo processo di fatturazione, avvenga esso in regime privato o in regime di accreditamento con il Sistema Sanitario Nazionale.

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. Per quanto attiene l'accesso da parte di Bollino IT al software ed ai DB contenenti dati di natura personale, questo è specifico per le finalità contrattuali, esplicito poiché previsto dai requisiti di assistenza ed aggiornamento del software e legittimo poiché necessario. Tutto il personale di Bollino, in tal senso, è opportunamente e formalmente incaricato al trattamento (ovvero individuato ai sensi dell'art. 29 del GDPR) ed i relativi accessi sono memorizzati sui file di log che consentono idonea tracciabilità.

Basi legali per il trattamento

La fornitura del software avviene su base contrattuale, la liceità del trattamento lato cliente è una sua responsabilità in qualità di Titolare del Trattamento ed è suo onere garantire chiara ed idonea informazione sulle modalità di trattamento dei dati dei pazienti; acquisire ove previsto idoneo consenso al trattamento ed adempiere ad ogni vincolo normativo in merito.

BollinoData offre gli strumenti che consentono al cliente di gestire tali processi, che permangono comunque responsabilità del titolare del trattamento.

Gli obblighi di Bollino IT in qualità di Responsabile del Trattamento sono in vigore per la durata del rapporto contrattuale tra le parti; nei casi in cui il rapporto contrattuale non fosse attivo, ovvero fosse sospeso per inadempienze amministrative, il processo di assistenza e manutenzione è da considerarsi sospeso, al pari del Ruolo di Responsabile del Trattamento di Bollino IT.

Misure di sicurezza connesse al trattamento implementate dal Responsabile del Trattamento

Crittografia

L'accesso al programma avviene mediante login effettuato tramite username e password crittografate nella base dati secondo i requisiti normativi. I dati sensibili sono cifrati ed accessibili in ragione delle singole autorizzazioni dei profili e delle utenze del cliente. Questo permette l'impossibilità di interpretazione di un dato cifrato in caso di sniffing, furto o, più in generale, di ricezione accidentale dell'informazione sensibile.
Viene applicata la crittografia per i dati accesso al database (connection string), le credenziali degli utenti per l'autenticazione, altre credenziali per eventuali integrazioni ed i referti. Per le password di autenticazione viene adoperato un algoritmo SHA1 non reversibile per calcolare l'hash della parola chiave. Per altre credenziali viene utilizzato un algoritmo triple DES. I referti invece sono archiviati in formato proprietario come tipo di dati binario non interpretabile esternamente al software.

Controllo degli accessi logici

Gli amministratori di sistema del cliente gestiscono gli accessi logici al software, i diritti e le policy. BollinoData consente diversi livelli di impostazione in ragione delle specifiche esigenze. Gli accessi effettuati da BollinoData sono sempre tracciati, sia mediante richiesta diretta, sia tramite file di Log per le attività svolte dal personale sia in presenza che, ove necessario, durante un accesso da remoto.
I profili degli utenti sono configurabili sia per gruppi che per specifico operatore. L'accesso alla configurazione viene garantito tramite opportuna profilazione dell'amministratore che ha anche il compito di creare le utenze. Al primo accesso l'utente è obbligato a modificare la password che deve rispettare i seguenti criteri:
1. La password deve essere lunga almeno 8 caratteri.
2. Deve rispettare almeno 3 dei seguenti requisiti:
- contenere almeno una lettera minuscola
- contenere almeno una lettera maiuscola
- contenere almeno un numero
- contenere almeno uno dei seguenti caratteri speciali
  (~!@#$%^&*()_+-={}|[]"\+:;'<>?,./)
3. La stessa password non può più essere riutilizzata

La password ha validità di 90 giorni ma l'utente ha facoltà di modificarla autonomamente in qualsiasi momento. Se smarrita non può essere recuperata ma l'amministratore può resettarla di modo che lo stesso utente la possa nuovamente modificare.

Vulnerabilità

Bollino IT adotta il Risk Thinking come specifica metodologia operativa. Pertanto, l'approccio orientato alle vulnerabilità aziendali e del software fa parte della logica aziendale sin dalla fase di progettazione, passando per lo sviluppo, il testing, la produzione ed installazione al cliente, l'assistenza e la manutenzione. Tale approccio è validato dalla certificazione ISO 27001 ottenuta dall'azienda a valle di verifica condotta da ente terzo qualificato e indipendente. Il Certificato è disponibile sul sito aziendale

Politica di tutela della privacy

Bollino applica alla propria organizzazione una rigida politica di Information Security come certificato dall'ottenimento della certificazione ISO 27001 da ente esterno, indipendente ed accreditato.

Gestione del personale

Tutto il personale di Bollino IT, in relazione agli specifici ruoli e mansioni, è incaricato al trattamento dei dati inteso come soggetto individuato secondo art. 29 del GDPR

Integrità dei dati

Integrità dei dati acquisiti: si riferisce alla loro correttezza e alla loro accuratezza. Gli utenti autorizzati sono responsabili dell'introduzione corretta dei dati, ma essi spesso possono commettere errori. BollinoData aiuta gli utenti a trovare un errore appena immesso e a correggere errori dopo che sono stati inseriti. Inoltre mantengono l'integrità di ogni record nel database nei seguenti modi:

- applicando dei controlli di campo: un campo potrebbe essere un valore numerico, una lettera maiuscola, o uno di un insieme specifico di caratteri. Il controllo assicura che un valore cada in specifici limiti. Questi controlli prevengono semplici errori verificabili durante l'immissione di dati;
- applicando controlli di accesso: solo chi ha l'autorizzazione almeno per visualizzare i dati può accedere al sistema. Il livello successivo, ossia la possibilità di modificare i

dati, dev'essere gestito in modo da consentire la modifica dei dati solo a chi è autorizzato e in modo da evitare conflitti
- mantenendo un log delle modifiche: ossia una lista di tutte le modifiche fatte sui dati (inserimento, cancellazione, modifica o semplice visualizzazione)

Gestione dei rischi

La gestione dei rischi è centrale nella vision di Bollino e delle proprie tecniche di sviluppo, come evidenziato dalla certificazione ISO 27001 e dall'utilizzo degli standard:
- IEC 62366-1:2015/Amd 1:2020 - Medical devices — Part 1: Application of usability engineering to medical devices — Amendment 1
- IEC 62304:2006/Amd 1:2015 - Medical device software — Software life cycle processes — Amendment 1

Sicurezza dei canali informatici

In ragione delle specifiche tecniche richiesta dal cliente (che secondo il principio di accountability, in qualità di titolare del trattamento dei dati dei propri pazienti può definire il proprio livello di protezione commisurato ai propri obiettivi di sicurezza) è possibile applicare diverse logiche di protezione nelle connessioni distribuite.
Per quanto attiene il servizio SMS, questo è svolto da Aruba in qualità di autonomo Titolare del Trattamento, come disciplinato da "Condizioni di Fornitura del Servizio SMS Aruba.it" al paragrafo 21

Manutenzione

L'attività di manutenzione del software, ovvero di aggiornamento del software è svolta dal personale di Bollino opportunamente incaricato e idoneo in ragione dell'Art. 29 del GDPR. La manutenzione avviene sempre secondo una attività gestita in ambiente separato da Bollino IT, testata e messa in produzione (quindi applicata ai sistemi clienti) solo al momento opportuno.

Bollino IT non gestisce la manutenzione dell'hardware del cliente che è quindi in carico al Titolare del Trattamento

Lotta contro il malware

La misura è in carico al Titolare del Trattamento

BOLLINODATA – VALUTAZIONE IMPATTO G.D.P.R.

Gestione postazioni

La misura è in carico al Titolare del Trattamento

Backup

Il backup è in carico al titolare del trattamento. Più generalmente per quanto attiene la business continuity, Bollino IT S.p.A. offre il servizio di assistenza e manutenzione del software secondo specifici accordi contrattuali. Tale servizio afferisce esclusivamente al software e non contempla le policy, le infrastrutture ed i processi di ripristino aziendali.

Redazione	Approvazione
	BOLLINO IT S.p.A. A SOCIO UNICO Via delle Industrie, 31 - 80147 N… Tel. 081 5592819 - Fax 081.559… Part. IVA 0634…