Valutazione d'impatto della protezione dei dati

(Data Protection Impact Analysis)

"GAIA"

Poliambulatorio Dalla Rosa Prati S.r.l.

Introduzione

Il presente documento consiste nella valutazione d'impatto "GAIA".

L' attività è stata disciplinata da un Gruppo di lavoro aziendale, composto da:

- Referenti aziendali: Dott.ssa Laura Parizzi, Dott.ssa Samanta Giovannelli, Dott. Maurizio Falzoi e Dott.ssa Valentina Bianchi
- Team società EsoSphera S.r.l.
- Ing. Francesco Pizzetti (consulente IT)
- Dott. Sergio Lizio (consulente privacy)
- Avv. Pierpaolo Maio (DPO)

Lo scopo di questa analisi è quello di valutare l'impatto sulla protezione dei dati dell'attività di trattamento in oggetto; l'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati ed ha come obiettivo la verifica delle misure in essere e loro efficacia in materia di privacy.

Informazioni essenziali:

- Data inizio analisi: 13 / 06 / 2023
- Data fine analisi: 3 / 08 / 2023
- Titolare del trattamento dati:
- Responsabile Protezione Dati:

Informazioni sul trattamento:

Trattamento / Attività Oggetto di Valutazione
Gestione chiamate in arrivo attraverso GAIA

Descrizione del Trattamento
Finalità del trattamento
▪ Migliorare il servizio di risposta ai clienti e in particolare le chiamate in arrivo cui gli operatori non possono rispondere, prevedento un ricontatto o un'immediata risposta a informazioni essenziali
Base giuridica
▪ Consenso
Origine dei dati
▪ Utenti

Responsabili esterni coinvolti	
▪ EsoSphera S.r.l. ▪ Sub-Responsabili coinvolti da EsoSphera S.r.l.: → Amazon Web Service (fornitura infrastruttura) → Datacenter Google Area Europa (TTS e ASR) → TWT S.p.A.(Provider Telefonico) → Mailgun Technologies, In. (invio e-mail) → ASCOTLC S.p.A. (Infrastruttura e connettività) → Link Mobility Italia S.r.l. (Invio SMS e WhatsApp)	
Soggetti autorizzati	
▪ Personale CUP	
Categorie di dati e di soggetti interessati dal trattamento	
▪ Utenti	▪ Dati anagrafici ▪ Dati di contatto ▪ Dati sanitari (solo tipologia prestazione richiesta)
▪ Medici	▪ Dati anagrafici (nome e cognome)
Comunicazione dati	
▪ Non prevista	
Diffusione dati	
▪ Non prevista	
Profilazione	
▪ Non prevista	
Descrizione processo	
Il trattamento in oggetto prevede la possibilità per il Poliambulatorio di gestire tutte le chiamate in arrivo, non solamente quelle cui materialmente gli operatori sono in grado di rispondere. Il centralino del Poliambulatorio alla ricezione della telefonata prevede che parta in automatico un breve messaggio che rimanda all'informativa presente sul sito web aziendale per i chiarimenti in merito alla gestione dei dati personali. Le chiamate cui non è possibile dare risposta vengono inoltrate verso GAIA attraverso un processo di integrazione VOIP tra il centralino del Poliambulatorio e i sistemi di EsoSphera. L'utente, una volta accolto dall'ASSISTENTE VOCALE GAIA, se gli uffici sono aperti, viene invitato a digitare 1 – 2 – 3 – 4 a seconda che voglia rispettivamente: prenotare un appuntamento, modificarlo o	

cancellarlo, richiedere informazioni o per contattare l'amministrazione. Nel caso in cui non digiti alcun pulsante viene informato che il sistema proverà a trasferire la sua chiamata a un operatore e, nel caso in cui non potesse rispondere, viene richiesto all'utente di lasciare i dati anagrafici e di contatto per poter essere richiamato o altrimenti riagganciare. Nel caso si proceda con una delle quattro opzioni precedentemente indicate, nel percorso di gestione della richiesta (meglio illustrato nel seguente DATA FLOW) verranno acquisite dall'utente le seguenti informazioni:

- dati anagrafici (nome e cognome);
- dati di contatto (viene richiesta la conferma del numero di telefono); e, eventualmente,
- dati sanitari (nello specifico il tipo di prestazione sanitaria per cui vuole chiedere la prenotazione).

Le risposte fornite dall'utente vengono prese in carico da GAIA che si occupa della trasformazione del parlato in testo. Il flusso audio del canale telefonico non viene registrato, ma inviato in streaming ad un fornitore terzo di EsoSphera, che restituisce il testo compreso mediante l'utilizzo della tecnologia ASR (Automatic Speech Recognition). Il fornitore terzo non conserva copia del testo ottenuto. Il dialogo trascritto viene conservato all'interno dei Server di EsoSphera.

GAIA interpreta le richieste dal punto di vista semantico utilizzando un servizio terzo (ma senza comunicare dati personali dell'utente) ed algoritmi interni di propria ideazione e produzione. I dati tecnici della conversazione sono mantenuti all'interno dei server EsoSphera per alcuni giorni a scopo di log managment e poi vengono eliminati.

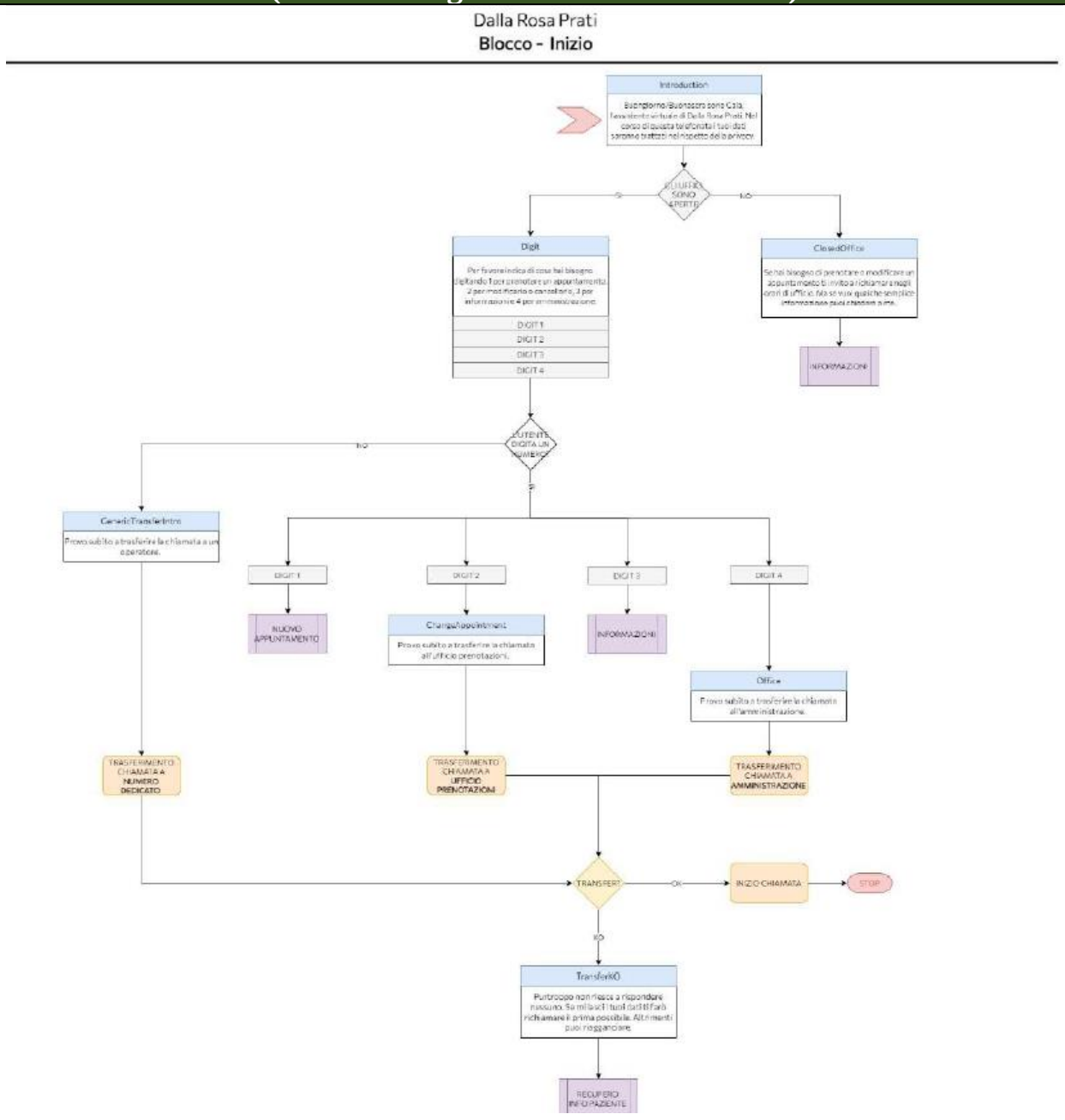
Al termine delle domande, GAIA comunica all'utente di aver preso nota di tutte le informazioni ed inoltra al Poliambulatorio le informazioni raccolte.

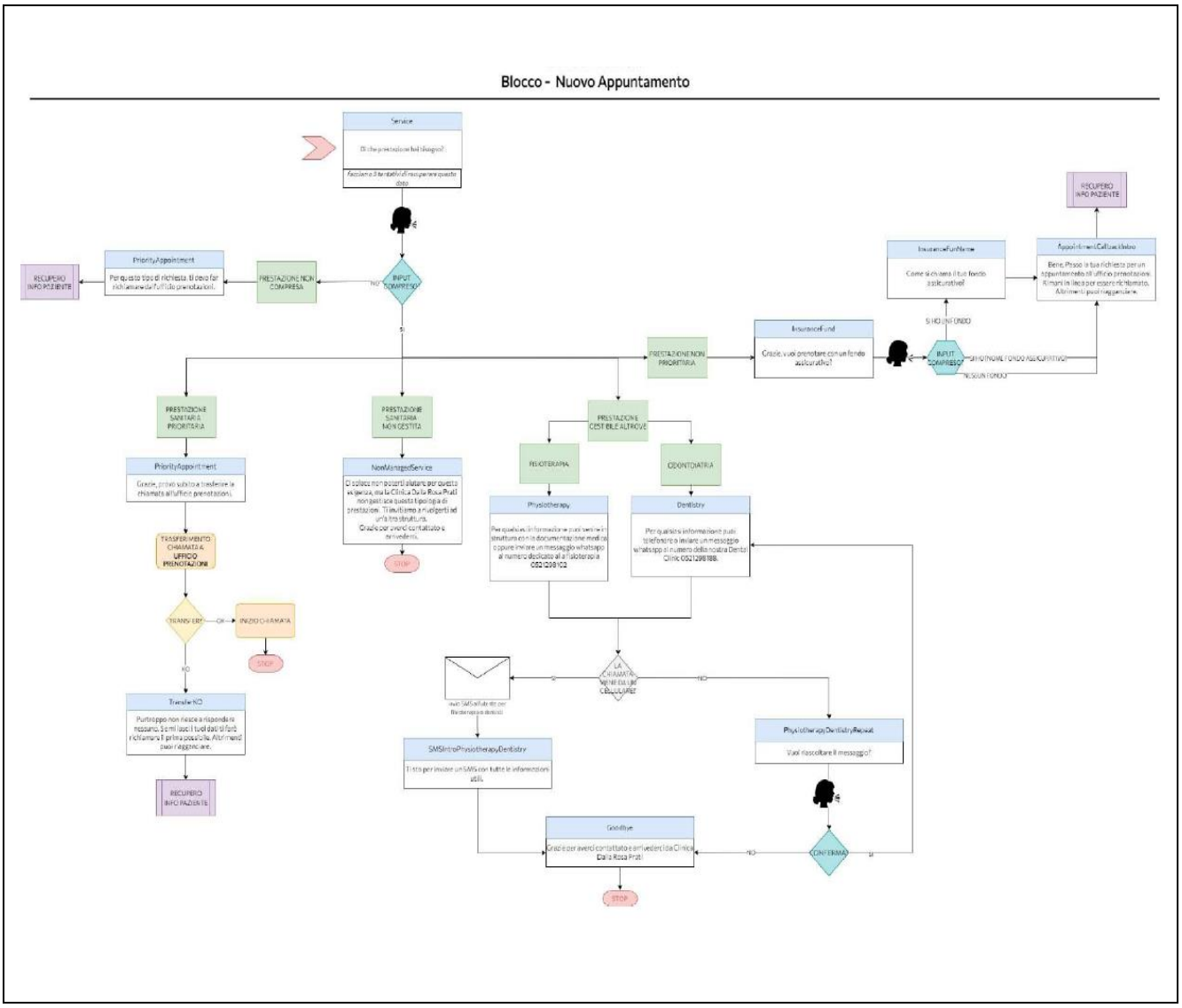
Gli operatori del CUP, nell'ipotesi in cui non abbiano risposto direttamente, provvederanno a ricontattare gli utenti qualora la richiesta avesse ad oggetto la prenotazione di una prestazione sanitaria offerta dal Poliambulatorio o un quesito non previsto tra quelli per cui è impostata una risposta automatica da parte di GAIA.

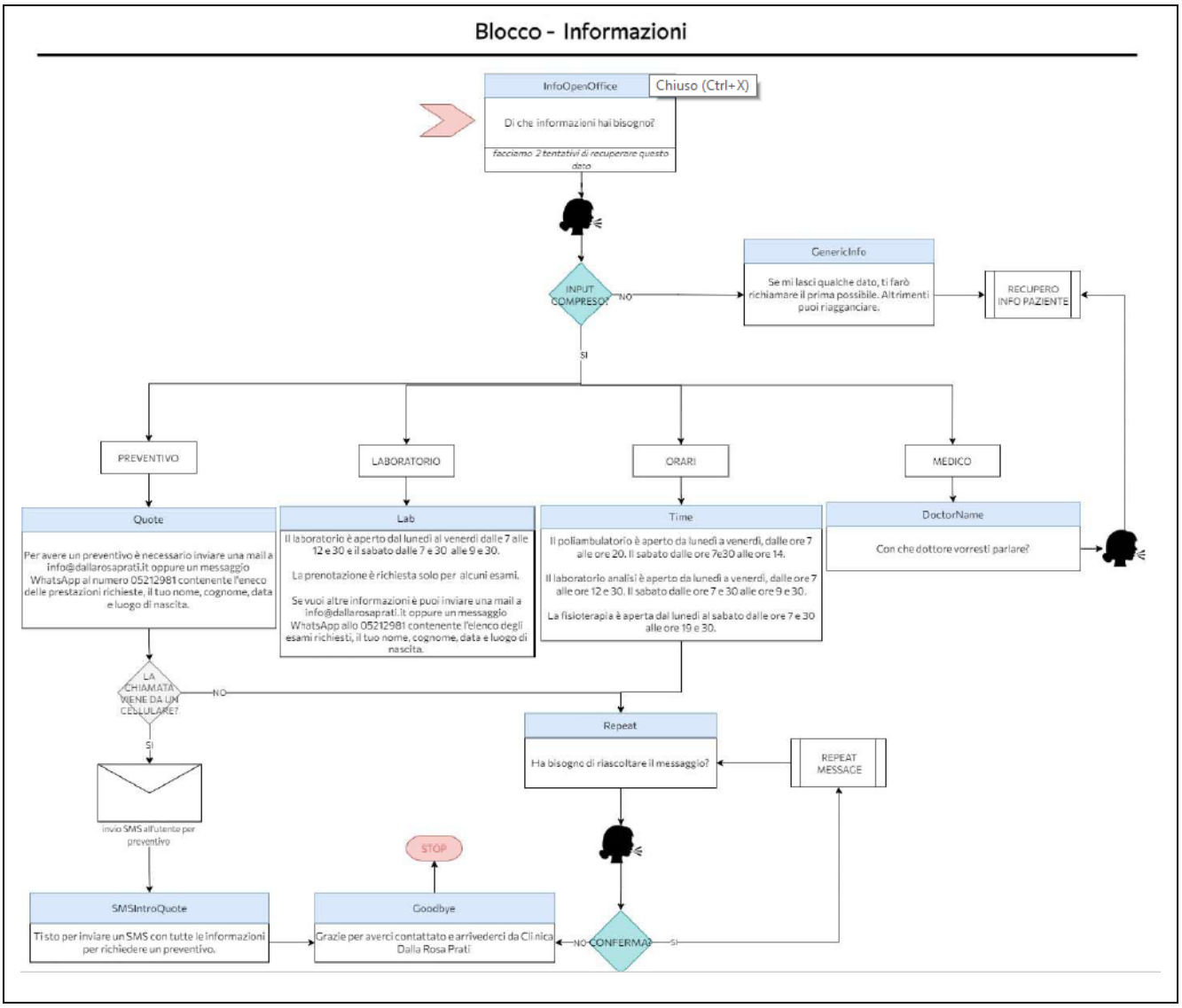
La trascrizione delle conversazioni viene conservata all'interno dei sistemi EsoSphera e le trascrizioni vengono rese disponibili al Poliambulatorio attraverso un portale di back end, il cui accesso è protetto da username e password.

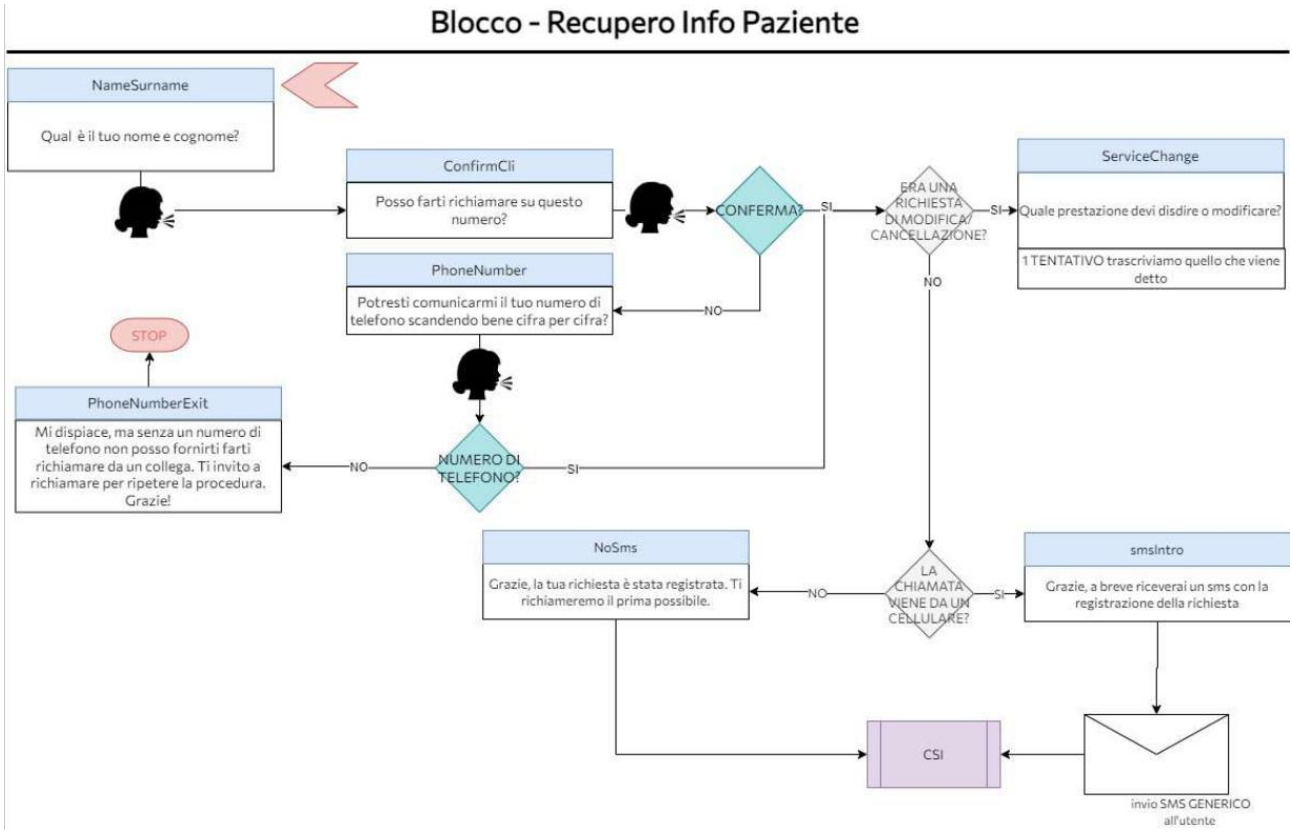
DATA FLOW

(Descrizione grafica del flusso dei dati)




Blocco - Nuovo Appuntamento
Service
INPUT COMPRESO?
PRESTAZIONE NON COMPRESA
PriorityAppointment
RECUPERO INFO PAZIENTE
PRESTAZIONE NON PRIORITARIA
InsuranceFund
INPUT COMPRESO?
PRESTAZIONE SANITARIA PRIORITARIA
PRESTAZIONE SANITARIA NON GESTITA
PRESTAZIONE GESTIBILE ALTROVE
FISIOTERAPIA
ODONTOIATRIA
Physiotherapy
Dentistry
TRASFERIMENTO CHIAMATA A UFFICIO PRENOTAZIONI
TRANSFER?
INIZIO CHIAMATA
STOP
Transfer NO
RECUPERO INFO PAZIENTE
NonManagedService
LA CHIAMATA VIENE EFFETTUATA CORRETTAMENTE?
SMSIntroPhysiotherapyDentistry
PhysiotherapyDentistryRequest
CONFERMA?
Goodbye
STOP


Blocco - Informazioni
InfoOpenOffice
Chiuso (Ctrl+X)
Di che informazioni hai bisogno?
facciamo 2 tentativi di recuperare questo dato
INPUT COMPRESO?
NO
GenericInfo
Se mi lasci qualche dato, ti farò richiamare il prima possibile. Altrimenti puoi riagganciare.
RECUPERO INFO PAZIENTE
SI
PREVENTIVO
LABORATORIO
ORARI
MEDICO
Quote
Per avere un preventivo è necessario inviare una mail a info@dallarosaprati.it oppure un messaggio WhatsApp al numero 05212981 contenente l'eneco delle prestazioni richieste, il tuo nome, cognome, data e luogo di nascita.
Lab
Il laboratorio è aperto dal lunedì al venerdì dalle 7 alle 12 e 30 e il sabato dalle 7 e 30 alle 9 e 30.
La prenotazione è richiesta solo per alcuni esami.
Se vuoi altre informazioni è puoi inviare una mail a info@dallarosaprati.it oppure un messaggio WhatsApp allo 05212981 contenente l'elenco degli esami richiesti, il tuo nome, cognome, data e luogo di nascita.
Time
Il poliambulatorio è aperto da lunedì a venerdì, dalle ore 7 alle ore 20. Il sabato dalle ore 7e30 alle ore 14.
Il laboratorio analisi è aperto da lunedì a venerdì, dalle ore 7 alle ore 12 e 30. Il sabato dalle ore 7 e 30 alle ore 9 e 30.
La fisioterapia è aperta dal lunedì al sabato dalle ore 7 e 30 alle ore 19 e 30.
DoctorName
Con che dottore vorresti parlare?
LA CHIAMATA VIENE DA UN CELLULARE?
NO
SI
Repeat
Ha bisogno di riascoltare il messaggio?
REPEAT MESSAGE
Invio SMS all'utente per preventivo
STOP
SMSIntroQuote
Tisto per inviare un SMS con tutte le informazioni per richiedere un preventivo.
Goodbye
Grazie per averci contattato e arrivederci da Clinica Dalla Rosa Prati
NO
CONFERMA?
SI


Blocco - Recupero Info Paziente
NameSurname
Qual è il tuo nome e cognome?
ConfirmCli
Posso farti richiamare su questo numero?
CONFERMA?
SI
ERA UNA RICHIESTA DI MODIFICA/ CANCELLAZIONE?
SI
ServiceChange
Quale prestazione devi disdire o modificare?
1 TENTATIVO trascriviamo quello che viene detto
NO
PhoneNumber
Potresti comunicarmi il tuo numero di telefono scandendo bene cifra per cifra?
NO
STOP
PhoneNumberExit
Mi dispiace, ma senza un numero di telefono non posso fornirti farti richiamare da un collega. Ti invito a richiamare per ripetere la procedura. Grazie!
NO
NUMERO DI TELEFONO?
SI
NoSms
Grazie, la tua richiesta è stata registrata. Ti richiameremo il prima possibile.
NO
LA CHIAMATA VIENE DA UN CELLULARE?
SI
smsIntro
Grazie, a breve riceverai un sms con la registrazione della richiesta
CSI
invio SMS GENERICO all'utente

Possibili danni specifici connessi al trattamento

- danno per la reputazione
- perdita del controllo dei dati personali
- perdita di riservatezza di dati personali protetti da segreto professionale
- impossibilità di accedere a servizi e opportunità

Analisi dei rischi

MATRICE DEI RISCHI		
Valore	**Rischio**	**Tipo d'intervento**
Pari a 1	Basso-Trascurabile	Controllo
Da 2 a 4	Medio-Basso	Monitoraggio
Da 6 a 9	Medio-Alto	Azione richiesta
Da 12 a 16	Alto	Azione Urgente

R: rischio

P: probabilità

G: gravità

R = P x G					
Probabilità	Alta	**4**	**8**	**12**	**16**
	Medio-alta	**3**	**6**	**9**	**12**
	Medio-bassa	**2**	**4**	**6**	**8**
	Bassa	**1**	**2**	**3**	**4**
		Bassa	Medio-bassa	Medio-alta	Alta
		Gravità			

Misure di sicurezza attualmente adottate

Fisiche	▪ Sistemi antincendio locali server / archivi ▪ Sistemi di climatizzazione locale server / backup
Organizzative	▪ Accesso digitale tramite autenticazione e autorizzazione ▪ Database / banche dati conservati in luoghi fisicamente distinti ▪ Formazione ▪ Istruzioni per il trattamento ▪ Nomina per iscritto personale ▪ Nomina Amministratore di sistema

	▪ Nomina per iscritto responsabili esterni e adeguate misure di sicurezza assicurate dagli stessi ▪ Procedura Data Breach ▪ Procedure in termine gestione e protezione dati ▪ Definizione delle tempistiche di conservazione dei dati
Informatiche	▪ Antivirus/Antispam ▪ Credenziali di autenticazione ▪ Definizione profili d'autorizzazione distinti ▪ Back Up periodici ▪ Firewall/WAF (Web Application Firewall) ▪ Monitoraggio dei Log di accesso alla rete interna ▪ Log Amministratori di sistema ▪ Costante aggiornamento del Sistema operativo ▪ Cifratura dei dati

Criticità e rischi per diritti e libertà degli interessati

		P	G	R
Impatto	Riservatezza dei dati	1	3	3
	Disponibilità dei dati	1	3	3
	Integrità dei dati	1	2	2

Non trattandosi di un processo relativo a decisioni basate unicamente sul trattamento automatizzato di cui all'art. 22 del GDPR e non essendo neanche prevista una profilazione dell'utente, si può ritenere che, sulla base delle misure di sicurezza attualmente in vigore, il rischio in linea generale possa essere considerato di livello medio-basso.

Dal punto di vista della riservatezza del dato (valore 3), il rischio principale è che a tali informazioni abbiano accesso soggetti terzi non autorizzati o che le stesse vengano diffuse esternamente. Ma in tal senso queste informazioni vengono riportate solo al personale del CUP del Poliambulatorio, formalmente autorizzato ad accedere a tali dati, e nel percorso che prevede la trasformazione del parlato nel testo scritto neanche i Sub-Responsabili esterni coinvolti hanno accesso ai dati personali; infatti, come riportato nella descrizione, il flusso audio del canale telefonico non viene registrato, ma inviato in streaming ad un fornitore terzo di EsoSphera, che restituisce il testo senza conservarne copia.

Dal punto di vista della disponibilità del dato (valore 3), il rischio principale è che tali informazioni una volta acquisite possano andar perse e, quindi, non consentire all'utente di usufruire del servizio richiesto o di essere ricontattato per ottenere le informazioni o fornire dati utili al processo in oggetto. Si ritiene sussiste un

rischio medio basso, in quanto la società EsoSphera conserva il dialogo trascritto e i dati tecnici all'interno dei suoi Server per un periodo di tempo determinato. Inoltre, una volta comunicati, tali dati sono archiviati direttamente anche dal Poliambulatorio.

Infine, in termini di completezza del dato (valore 2), in considerazione di quanto detto finora si ritiene veramente bassa la possibilità che possa configurarsi una deliberata alterazione di dati personali da parte dei soggetti coinvolti o la cancellazione o distruzione parziale di dati da parte degli stessi.

Misure di sicurezza da adottare per eliminare / ridurre il rischio

Per mantenere o, se possibile ridurre il livello di rischio individuato, è consigliabile:

- monitorare il funzionamento del processo attraverso degli audit a campione;
- monitorare l'operatività delle misure di sicurezza al momento in vigore;
- verificare periodicamente l'attualità dei permessi e delle responsabilità attribuite;
- effettuare formazione al personale coinvolto da tale trattamento e sottolineare l'importanza della comprensione e conoscenza della procedura relativa al data breach al fine di intervenire tempestivamente nel caso ravvisino una violazione.

Rischio residuo

A seguito dell'adozione delle precedenti misure si può ritenere che il rischio, anche se non rimosso completamente, in quanto sempre collegato a una serie di incognite difficilmente eliminabili, può sempre considerarsi basso / medio-basso.

Indicazioni DPO

Sezione dedicata al Titolare del trattamento
Indicazioni del DPO
☐ Accettate ☐ Non accettate ☐ Richiesta ulteriori chiarimenti
Eventuali osservazioni del Titolare sulle indicazioni espresse dal DPO