Mappatura dei rischi

Piano d'azione

Principi fondamentali

Finalità

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl

Adeguatezza dei dati

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl

Esattezza dei dati

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl

Periodo di conservazione

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl

Raccolta del consenso

Piano d'azione / misure correttive:

È previsto un monitoraggio dopo tre mesi dall'inizio delle attività dell'App.

Misure esistenti o pianificate

Archiviazione

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Sicurezza dei siti web

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Backup

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Manutenzione

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Sicurezza dei canali informatici

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Rischi - Accesso illegittimo ai dati

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? **Trascurabile**

Rischi - Modifiche indesiderate dei dati

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? **Trascurabile**

Rischi - Perdita di dati

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Data prevista di implementazione: 24/05/21
Responsabile dell'implementazione: Meeter Congressi Srl
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? **Limitata**
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)? **Trascurabile**

DPO e richiesta del parere degli interessati

Nome del DPO/RPD

n/a

Parere del DPO/RPD

n/a

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il trattamento non è ancora iniziato. Pertanto, il monitoraggio previsto dopo tre mesi dal lancio dell'App sarà utile anche per raccogliere il parere degli interessati.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Scopo di un follow-up in generale, è diagnosticare in maniera preventiva la ripresa di una malattia, ovvero una nuova patologia collegata alla precedente o un effetto dannoso, legato ad esempio, ad un trattamento farmacologico.
Nell'ipotesi di visite periodiche, di solito a lungo termine, il paziente potrebbe dimenticare di effettuare i controlli di follow-up o di richiedere un appuntamento, con il rischio che la patologia iniziale degeneri senza poter intervenire.
L'esigenza è quella di arginare questo fenomeno.
Come con una agenda, FollowUpp supporta il medico, attraverso le sue funzioni, nella gestione degli appuntamenti dei pazienti in follow-up, ricordando a questi ultimi le fasi del monitoraggio.
L'innovazione consiste nell'invio di semplici SMS di remind su attivazione da parte del medico.
Nell'app ci sono due gruppi di dati trattati:
- i dati relativi ai medici;
- i dati relativi ai pazienti/beneficiari.

Denominazione dei trattamenti:
- trattamento dei dati dei medici;
- trattamento dei dati dei pazienti dei medici;

Finalità del trattamento è il supporto del medico nella gestione degli appuntamenti dei pazienti in follow-up.
I risultati attesi consistono nell'invio degli sms di remind ai pazienti/beneficiari, al fine di ricordare le fasi di monitoraggio;
Il contesto di utilizzo è limitato a FollowUpp, che viene scaricata dai medici e utilizzata come in dettaglio più oltre.

Quali sono le responsabilità connesse al trattamento?

FollowUpp è di proprietà di Meeter Congressi Srl, di seguito Meeter.
Pertanto, Meeter è:
- titolare del trattamento per quanto riguarda i dati personali dei medici, che vengono inseriti da questi ultimi quando scaricano FollowUpp;
- responsabile del trattamento per quanto riguarda i dati personali dei pazienti inseriti nell'App dai medici.

In quest'ultimo caso titolari del trattamento sono i medici che scaricano l'app, e, tramite l'apposizione di un flag, dichiarano di considerare le misure tecniche ed organizzative di FollowUpp, così come descritte nella presente valutazione di impatto, conformi ed adeguate ai propri criteri di sicurezza, così come predisposte da Meeter Congressi. In tal modo, le misure tecniche ed organizzative vengono riconosciute come adeguate, anche ai sensi dell'art. 28.
La descrizione completa di tale rapporto è presente nel documento denominato nomina a responsabile del trattamento.
Meeter informa con il presente documento dei fornitori a cui si rivolge, in veste di sub-responsabili.
Pertanto, la catena di responsabilità è impostata diversamente nel caso nel caso dei dati dei medici e nel caso dei dati dei pazienti.
Dati dei medici:
Titolare del trattamento --> Meeter, proprietario di FollowUpp
Responsabile --> Percettiva Scarl (di seguito Percettiva), che impegna il personale e stipula i contratti con gli sviluppatori dell'App e con i fornitori del servizio SMS.
Sub-Responsabile --> StepApp Srl (di seguito StepApp), sviluppatori dell'App, che hanno un contratto con Percettiva.
Sub-Responsabile --> Skebby - Commify Italia Srl società che fornisce la piattaforma di sms, che ha un contratto con Percettiva.
Fornitore del Servizio Cloud --> Aruba S.p.A.
Una lista completa dei fornitori e dei responsabili è rinvenibile presso Meeter Congressi Srl.

Dati dei pazienti:
Titolare --> MEDICO
Responsabile--> Meeter, proprietario di FollowUpp
Sub-Responsabile --> Percettiva Scarl (di seguito Percettiva), che impegna il personale e stipula i contratti con gli sviluppatori dell'App e con i fornitori del servizio SMS.
Sub-Responsabile --> StepApp Srl (di seguito StepApp), sviluppatori dell'App, che hanno un contratto con Percettiva.
Sub-Responsabile --> Skebby - Commify Italia Srl società che fornisce la piattaforma di sms, che ha un contratto con Percettiva.
Fornitore del Servizio Cloud --> Aruba S.p.A.
Una lista completa dei fornitori e dei responsabili è rinvenibile presso Meeter Congressi Srl.

Ci sono standard applicabili al trattamento?

I trattamenti sono effettuati esclusivamente per il tramite dell'App. Per tale motivo si prendono in considerazione, per quanto riguarda gli standard applicabili al trattamento, i TOP 10 proactive controls, ovvero un protocollo redatto da OWASP (Oper Web Application Security Project), contenente i dieci punti più importanti da tenere in considerazione per la sicurezza informatica di un software di qualsiasi tipo. Si è dunque andato a verificare se il software FollowUpp nella sua interezza (APP e BACKEND) allo stato attuale si possa considerare conforme ai 10 punti illustrati nel documento di OWASP. Ebbene, FollowUpp applica le best practices dello sviluppo, mantenendo un codice pulito, manutenibile e il più possibile sicuro. Le librerie provengono da fonti sicure. Le versioni delle librerie sono le più recenti a disposizione. Le librerie utilizzate non hanno vulnerabilità note e l'aggiornamento delle versioni delle librerie è gestibile facilmente. L'encode dell'output viene effettuato generalmente per evitare a monte le vulnerabilità XSS. La complessità della password viene verificata sia su client che su server. L'app implementa una password complessa composta da minimo 10 caratteri. La password è hashata. La comunicazione tra il server e l'app è criptata utilizzando il protocollo HTTPS. I log sono consistenti a livello di Timestamp e loggano informazioni utili (IP e user-id). Non vengono loggati dati personali. Per dettagli ulteriori contattare privacy@meeter.it

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

gruppo dati relativi ai medici:
NOME, COGNOME, EMAIL, PASSWORD, CELLULARE, FLAG CON CUI DICHIARA DI ESSERE MEDICO, SPECIALIZZAZIONI, N° ORDINE DEI MEDICI

gruppo dati relativi ai pazienti:
predefinito - NOME, COGNOME, CELLULARE, INDICAZIONE DI FOLLOW UP TRA 3, 6, 12 MESI
personalizzato - NOME, COGNOME, CELLULARE, INDICAZIONE DI FOLLOW UP CON DATA E ORA DELL'APPUNTAMENTO

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Fase relativa al medico:
Il medico scarica l'App tramite gli Store Ufficiali (Apple Store e Play Store), inserisce i propri dati, come descritti nei paragrafi precedenti. In fase di registrazione l'utente - medico - viene obbligato informaticamente a leggere la documentazione relativa alle condizioni d'utilizzo ed alla parte relativa alla protezione dei dati, compresa la presente valutazione di impatto. A questo punto l'utente può scegliere se considerare le misure di sicurezza individuate da Meeter per FollowUpp conformi ed adeguate apponendo un flag all'interno dell'app e pertanto proseguire nella propria registrazione. Sempre nell'app è possibile altresì individuare un modello di documento ex art. 28 GDPR che il medico, in qualità di titolare del trattamento dei dati dei pazienti, può utilizzare per nominare Meeter suo responsabile per il servizio di remind fornito da FollowUpp. Tale documento può essere compilato, sottoscritto e spedito all'indirizzo e-mail privacy@meeter.it. L'utente può apporre altresì un flag con cui dichiara che ha chiesto il consenso agli interessati dei quali inserirà il numero di telefono ed il nominativo. Il medico, in qualità di titolare del trattamento ha il compito di informare i pazienti di come verranno trattati i dati per il tramite dell'utilizzo dell'app. La registrazione si completa con l'apposizione dei flag di conferma. Senza il completamento della registrazione, nessun dato viene acquisito dal database e l'utente potrà decidere di lasciare l'app sul proprio telefono, ovvero di disinstallarla. Senza registrazione i dati non vengono raccolti e pertanto trattati. In caso di registrazione, il database acquisisce le informazioni. Quando il medico (in questo caso nella posizione di utente dell'App) clicca su "registrati", l'app in automatico invia un'e-mail per richiedere conferma della registrazione. All'interno dell'App sono disponibili diversi documenti.

Fase relativa ai pazienti/beneficiari:
Una volta che l'utente medico si è registrato, ogni volta che informa un paziente/beneficiario dell'esistenza dell'app, chiederà il suo consenso per inviargli i messaggi di remind in ordine alle prossime visite di follow up. Dal momento in cui registra all'interno dell'App i riferimenti (nome e numero di telefono) dei propri pazienti/beneficiari, il medico riveste la qualifica di titolare del trattamento dei dati dei medesimi pazienti. All'interno dell'App sono disponibili diversi documenti, tra cui una bozza di informativa che il medico può utilizzare per informare il paziente del trattamento ed acquisire il suo consenso. Anche se il paziente ha prestato il proprio consenso al medico, può sempre scegliere di disiscriversi dal servizio attraverso il link contenuto nel primo sms che gli viene inviato dall'app.
Il medico accede a tre funzioni all'interno dell'App: può scegliere se utilizzare una delle due funzioni di follow-up ("Predefinito", oppure "Personalizzato"), oppure infine la funzione "Agenda Follow-up" (che registra soltanto gli appuntamenti personalizzati).

FUNZIONI DI FOLLOW-UP “PREDEFINITO E PERSONALIZZATO”

1. Il medico, in qualità di titolare del trattamento, inserisce il nome, il cognome e il numero di cellulare del proprio paziente/beneficiario (tutti i campi sono obbligatori).

2. Seleziona la programmazione del follow-up (3-6-12 mesi nella funzione “Predefinito”, oppure selezionando data e ora nella funzione “Personalizzato”).

3. Ha facoltà di inserire, attivando un flag, un testo personalizzato (testo libero) che verrà visualizzato dal paziente in calce all’SMS. Il testo personalizzato resterà in memoria; il medico ha la possibilità di modificarlo o disattivarlo in qualunque momento. Il testo personalizzato nelle due modalità di utilizzo dell'App (“Predefinito” e “Personalizzato”) può essere diverso.

4. Solo all’interno della funzione “Personalizzato”, il medico può scegliere, attivando il flag “Inserisci nella mia Agenda dell'App”, se inserire la visita all'interno della propria agenda in app dei follow-up. Disattivando il flag (o comunque utilizzando la funzione “Predefinito”), la visita non verrà salvata e il medico non avrà la possibilità di modificare o annullare la programmazione dell’invio degli SMS.

5. Si chiede poi “Conferma" al medico di quanto digitato, al fine di registrarlo.

Dal momento della conferma, l’app gestirà automaticamente l’invio di 3 SMS al paziente/beneficiario: - 1° SMS: conferma del servizio - 2° SMS: remind un mese prima della visita - 3° SMS: remind una settimana prima della visita.

Testo tipo:
- Le ricordo la visita di controllo il gg-mm-aaaa alle hh.mm.
- Le ricordo la visita di controllo prevista tra una settimana.
- Le ricordo la visita di controllo prevista tra un mese.

Se il medico non inserisce firma, di default si rinviene:
Per conto dello Specialista – FollowUpp

Sono stati individuati termini che non riconducono immediatamente al concetto di visita medica, questo sia nell’ipotesi in cui l’sms giunga erroneamente ad altra persona, ovvero vi sia perdita, trafugamento delle liste degli interessati e conseguente data breach.

Se medico elimina un follow-up dall'agenda il paziente non riceverà più messaggi. Il medico dovrà assicurarsi che il paziente ne sia stato previamente informato.

FUNZIONE “AGENDA FOLLOW-UP”

In questa sezione si trovano tutte le visite di follow-up “Personalizzato” salvate.

In questa funzione è possibile:
1. Navigare di mese in mese tramite le frecce in alto;
2. Cambiare la visualizzazione lista/calendario cliccando sull'icona;
3. Cercare i follow-up di un paziente specifico attraverso la funzione “Cerca”;
4. Esportare per e-mail i follow-up che si stanno visualizzando in quel momento.

Dalla visualizzazione calendario è possibile visualizzare i follow-up di un singolo giorno, selezionandolo dal calendario;
Dalla modalità lista è possibile modificare/cancellare ogni singolo follow-up.
Se medico elimina un follow-up dall'agenda il paziente non riceverà più messaggi. Il medico dovrà assicurarsi che il paziente ne sia stato previamente informato.

Quali sono le risorse di supporto ai dati?
Computer, antivirus, rete informatica aziendale
Google Play
App Store
Dispositivo cellulare del medico
Collegamento all'Applicazione
Informativa del medico e consenso del paziente
Macchina virtuale Aruba (Cloud), con sopra installato SQL Server come DB e il webserver, sulla stessa macchina.
Dal dispositivo al database vengono usate le API proprietarie di FollowUpp.
Dal database, attraverso librerie di Skebby- Commify Italia, trasmissione di numeri di telefono a società di servizi per invio sms;
Da società di sms invio di comunicazioni al paziente/beneficiario finale.
Dispositivo del paziente/beneficiario finale per il ricevimento degli sms.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Gli scopi del trattamento sono specifici: l'app è finalizzata al supporto del medico, in qualità di titolare del trattamento, a far ricordare ai propri pazienti/beneficiari di effettuare visite di follow-up.
Gli scopi del trattamento sono espliciti: viene descritto il processo e le finalità sono espressamente dichiarate.
Gli scopi del trattamento sono legittimi: il trattamento dei dati del medico in qualità di interessato viene svolto per finalità contrattuali, per l'utilizzo dell'app; il trattamento dei dati dei pazienti / beneficiari, in qualità di interessati, viene effettuato previo consenso che i pazienti prestano al medico, in qualità di titolare del trattamento; i responsabili del trattamento, creatori del progetto, Meeter ed i suoi sub-responsabili, al fine di cautelare maggiormente gli interessati / beneficiari finali adottano uno strumento ulteriore per permettere all'interessato / beneficiario finale di disiscriversi dal servizio, attraverso uno strumento di opt-out. L'interessato / beneficiario finale, infatti, non appena il medico - titolare del trattamento, richiede il consenso ed inserisce il suo nominativo all'interno di FollowUpp, riceve un sms, con il quale viene avvertito di aver dato il proprio numero al medico - titolare e che riceverà a tempi cadenzati, due altri sms di remind per ricordare i controlli di follow-up. L'interessato / beneficiario finale può decidere immediatamente di disiscriversi dal servizio, cliccando su un pulsante, a cui viene condotto dall'apertura dell'sms ricevuto.
Non vengono assunte responsabilità in ordine al mancato recapito degli sms, in quanto il servizio informatico non può sostituire un accordo espresso tra paziente e medico curante.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Quali sono le basi legali che rendono lecito il trattamento?
Esecuzione di un contratto per il medico / interessato con Meeter, in qualità di titolare del trattamento effettuato per il tramite di FollowUpp.
Consenso per il paziente / beneficiario al medico / titolare del trattamento per il trattamento dei dati effettuato per il tramite di FollowUpp.

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

La raccolta dei dati all'interno dell'App è stata realizzata in ossequio al principio di minimizzazione. Sono contenuti esclusivamente dati utili alla compilazione dei campi per la gestione del servizio. Ad esempio, per i beneficiari finali sono inseriti soltanto nome, cognome, numero di telefono.
Per quanto riguarda i medici, in qualità di interessati, i dati richiesti consentono la sola individuazione della categoria di appartenenza: essi sono limitati al nominativo, e-mail, numero di telefono, specializzazione e numero di iscrizione all'ordine. Tutti questi dati sono facilmente rinvenibili, in quanto si tratta di dati pubblicati sui rispettivi ordini di appartenenza.
FollowUpp non accede ad alcuna altra applicazione all'interno del dispositivo in cui è istallata. Non vi è pertanto accesso a rubrica, fotocamera, posizione, dati biometrici. Gli unici dati raccolti da FollowUpp sono i dati che il medico sia in qualità di interessato, che in qualità di titolare del trattamento, che inserisce manualmente all'interno della stessa.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

I dati sono esatti e aggiornati?

Tutti i dati inseriti in FollowUpp sono compilati dal medico, prima nella qualità di interessato, ovvero quando compila i campi che riguardano sé stesso e successivamente quando compila i campi in qualità di titolare del trattamento. Si presuppone che il medico abbia fornito una informativa ed acquisito il consenso da parte dei pazienti beneficiari dell'App prima di inserire i loro dati personali e recapiti. A tal fine Meeter mette a disposizione dei titolari del trattamento in una area dell'App un modello standard di informativa circa il trattamento dei dati dei pazienti/beneficiari, che il medico potrà completare nel modo che ritiene più opportuno, in ordine alle misure e agli standard tecnici ed organizzativi che ritiene conformi per i trattamenti dei dati dei propri pazienti. Laddove i medici modifichino o cancellino le informazioni relative a ciascun paziente, queste verranno immediatamente modificate o cancellate anche nel database di riferimento.
I dati saranno altresì cancellati dal database nel momento in cui il beneficiario di FollowUpp decida di cancellarsi dal servizio, su indicazione del titolare del trattamento.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

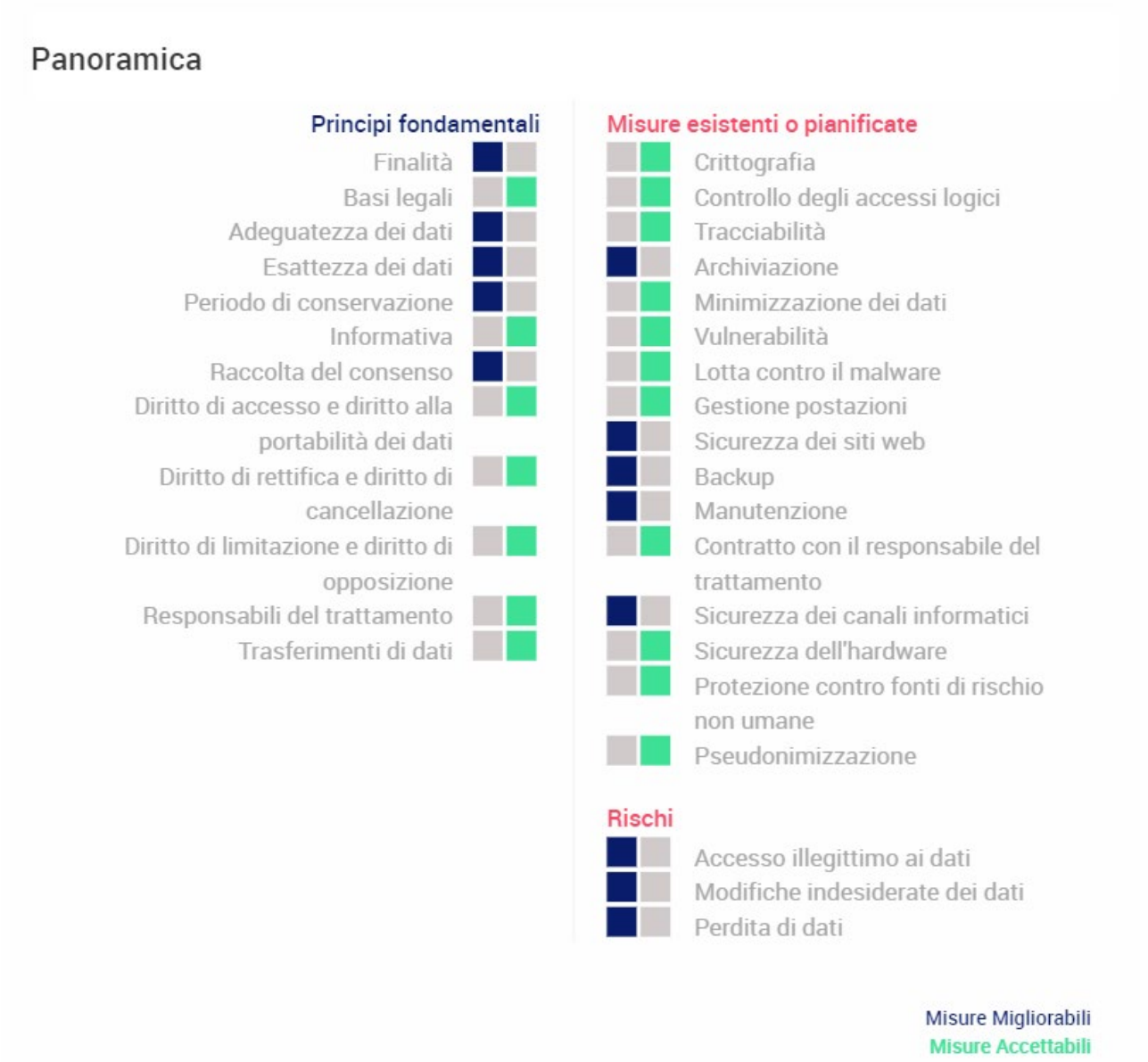
Qual è il periodo di conservazione dei dati?

Per quanto riguarda il trattamento dei dati dei medici, questi sono conservati fino alla cancellazione dell'account, pertanto il periodo di conservazione è controllato dall'utente finale.
Per quanto riguarda il trattamento dei dati dei pazienti/beneficiari, trattandosi di una agenda, i tempi di conservazione sono individuati dal titolare del trattamento, che decide se e quando cancellare eventuali appuntamenti, ovvero sono conservati fino alla cancellazione dell'account.
Per quanto riguarda i dati relativi all'invio ed al contenuto dei messaggi sms, questi sono conservati come per legge da parte del subfornitore per un periodo di 6 mesi e tale periodo viene altresì rispettato da Meeter, in qualità di responsabile del trattamento.
Per quanto riguarda le ipotesi di inattività dell'account: dopo due anni di inattività l'account sarà considerato scaduto ed i dati cancellati.
I dati vengono conservati in ogni caso per un periodo di almeno due anni, in quanto, data la natura di agenda per appuntamenti, è possibile impostare un appuntamento anche oltre il periodo preimpostato di 3 - 6 - 12 mesi.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.



Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Il medico in qualità di interessato riceve l'informativa da parte di Meeter, che è sempre rinvenibile nella sezione "note legali" all'interno di FollowUpp.
Il medico, in qualità di titolare del trattamento, chiede il consenso agli interessati all'inserimento dei propri dati di contatto all'interno di FollowUpp, la bozza di testo di informativa per i pazienti è proposta di seguito ed è sempre rinvenibile nella sezione "note legali" all'interno di FollowUpp.

Per i pazienti è stata prevista una maggiore cautela: nel momento in cui il medico, informato il paziente e ricevuto il consenso, inserisce i dati del paziente medesimo all'interno di FollowUpp, alla conferma da parte del medico segue immediatamente l'invio del primo sms di conferma al paziente: quest'ultimo potrà opporsi al trattamento ottenendo la immediata disiscrizione dal servizio cliccando sul link o pulsante predisposto per la disiscrizione.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il medico, in qualità di interessato, autorizza l'istallazione dell'app, compila i campi, inserendo i propri dati e conferma la propria volontà di utilizzare l'app, attraverso la registrazione, cliccando sull'apposito pulsante che si attiverà una volta che siano stati compilati i campi richiesti.
Il medico, in qualità di titolare del trattamento, si occupa di fornire agli interessati l'informativa e a richiedere il consenso. Per agevolare il medico nello svolgimento di questa attività, FollowUpp fornisce al medico una bozza di informativa che quest'ultimo potrà utilizzare, ovvero adattare al proprio utilizzo.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

È previsto un monitoraggio dopo tre mesi dall'inizio delle attività dell'App.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Gli interessati/ beneficiari possono rivolgersi al medico titolare del trattamento per esercitare i loro diritti. Meeter mette a disposizione l'indirizzo privacy@meeter.it che viene reso disponibile sia con l'invio del link all'interessato, sia nell'informativa che viene resa disponibile per il medico affinché raccolga il consenso da parte degli interessati/beneficiari; nel caso in cui questi ultimi scrivano direttamente a Meeter, quest'ultima contatterà il Titolare del trattamento, affinchè disporrà circa le richieste degli interessati.

Per quanto riguarda il medico, in app sono presenti due gruppi di dati: i dati di registrazione del medico, in qualità di interessato e i dati dei pazienti/beneficiari, inseriti attraverso le funzioni di follow-up.

I dati del medico, in qualità di interessato, sono resi accessibili all'interno dell'app, attraverso il pannello utente denominato "Il Mio Account".

I dati del paziente/beneficiario, immessi tramite la funzione di inserimento di follow-up "Personalizzato" e per i quali sia stata attivata la funzione "Inserisci nella mia agenda in app", sono accessibili nella sezione "Agenda Follow-up", dalla quale è possibile esportare un file che verrà ricevuto dal richiedente via e-mail.

I dati del paziente/beneficiario, immessi tramite la funzione di inserimento di follow-up "Predefinito" o tramite la funzione di inserimento di follow-up "Personalizzato" ma per i quali non sia stata attivata la funzione "Inserisci nella mia agenda in app", non verranno salvati all'interno dell'app, e pertanto il medico utente dell'app non potrà visualizzarli. In questo caso per l'esercizio dei diritti degli interessati il medico titolare del trattamento si rivolgerà a Meeter alla e-mail privacy@meeter.it affinché vengano estratte le informazioni richieste. Meeter mette a disposizione l'indirizzo privacy@meeter.it che viene reso disponibile sia con l'invio del link all'interessato/beneficiario, sia nell'informativa che viene resa disponibile per il medico affinché raccolga il consenso da parte degli interessati/beneficiari; nel caso in cui questi ultimi scrivano direttamente a Meeter, quest'ultima contatterà il Titolare del trattamento, affinchè disporrà circa le richieste degli interessati.

Valutazione: Accettabile

Commento di valutazione:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati / beneficiari possono sia rivolgersi al medico titolare del trattamento. Meeter mette a disposizione l'indirizzo privacy@meeter.it che viene reso disponibile sia con l'invio del link all'interessato, sia nell'informativa che viene resa disponibile per il medico affinché raccolga il consenso da parte degli interessati; nel caso in cui questi ultimi scrivano direttamente a Meeter, quest'ultima contatterà il Titolare del trattamento, affinchè disporrà circa le richieste degli interessati.
In caso di disiscrizione dal servizio da parte dell'interessato/beneficiario, verranno eliminati dal database tutti i relativi dati e verranno rimosse le programmazioni di invio di SMS.

Per quanto riguarda il medico, in app sono presenti due gruppi di dati: i dati di registrazione del medico, in qualità di interessato e i dati dei pazienti/beneficiari, inseriti attraverso le funzioni di follow-up.

I dati del medico, in qualità di interessato, possono essere modificati in qualunque momento, accedendo al pannello utente denominato "Il Mio Account", all'interno dell'app.

Il medico/interessato può altresì richiedere la cancellazione del proprio account, inviando una e-mail all'indirizzo privacy@meeter.it ovvero disinstallando l'App.

I dati del paziente/beneficiario, immessi tramite la funzione di inserimento di follow-up "Personalizzato" e per i quali sia stata attivata la funzione "Inserisci nella mia agenda in app", possono essere modificati e/o cancellati in qualunque momento, accedendo alla sezione "Agenda Follow-up".

I dati del paziente, immessi tramite la funzione di inserimento di follow-up “Predefinito” o tramite la funzione di inserimento di follow-up “Personalizzato” ma per i quali non sia stata attivata la funzione “Inserisci nella mia agenda in app”, non verranno salvati all’interno dell’app, e pertanto il medico utente dell’app non potrà visualizzarli. In questo caso per l’esercizio dei diritti degli interessati, quando investito da una richiesta, il titolare si rivolgerà a Meeter alla e-mail privacy@meeter.it affinché vengano estratte e modificate le informazioni relative, ovvero cancellati i dati richiesti da parte degli interessati.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Gli interessati/ beneficiari possono rivolgersi al medico titolare del trattamento. Meeter mette a disposizione l'indirizzo privacy@meeter.it che viene reso disponibile sia con l'invio del link all'interessato, sia nell'informativa che viene resa disponibile per il medico affinché raccolga il consenso da parte degli interessati; nel caso in cui questi ultimi scrivano direttamente a Meeter, quest'ultima contatterà il Titolare del trattamento, affinchè disporrà circa le richieste degli interessati.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
Meeter ha realizzato FollowUpp, che è uno strumento simile ad una agenda che viene messo a disposizione dei titolari del trattamento. La presente valutazione di impatto analizza tutte le informazioni e i rischi, individuando le mitigazioni agli stessi, in modo che gli utenti dell'app, i medici, possano valutare le sue funzioni e dichiarare, cliccando su un apposito flag all'interno della app, che ritengono le misure di sicurezza adottate conformi alle loro necessità anche ai sensi dell'art. 28 GDPR.
In ogni caso, all'interno dei documenti legali dell'app è inserito un modello di nomina ex art. 28 GDPR che ogni titolare potrà compilare, ovvero integrare e sottoscrivere, inviando una e-mail a: privacy@meeter.it.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
I dati sono ubicati su un server di Aruba, pertanto risiedono all'interno della UE. Per l'utilizzo del servizio SMS, i dati non vengono trasferiti al di fuori del SEE. Per indicazione stessa del subfornitore, ove dovesse avvenire trasferimento, questo avverrebbe esclusivamente verso Paesi interessati che siano considerati adeguati o siano in atto misure di salvaguardia appropriate e nell'ipotesi in cui l’interessato abbia diritti esigibili e mezzi di ricorso effettivi.

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia
Nella comunicazione tra il server web e l'app viene usato il protocollo HTTPS, quindi è presente una crittografia TLS delle richieste e delle risposte.
Nella comunicazione tra il server DB e il server web non si adottano protocolli di crittografia poiché si trovano sulla stessa macchina e il DB non è accessibile all'esterno.
La crittografia di database e dei file sebbene non sia stata realizzata, è attualmente in programmazione.
Verrà realizzata applicando le funzioni openssl fornite da php durante la lettura/scrittura verso il DB. Le funzioni utilizzeranno una chiave presente sulla macchina virtuale, ma non esposta dal server web.
Il database in ogni caso resterebbe sempre e comunque non accessibile all'esterno della macchina. Il desktop remoto si può disattivare da Aruba e attivare solo quando necessario, per proteggere la macchina da eventuali attacchi RDP.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Controllo degli accessi logici
L'input sul server viene validato utilizzando il validatore di Laravel, la complessità della password viene verificata sia su client che su server e sono accettate solo password molto sicure utilizzando regular expression protette da attacco ReDoS
RegEx Password:

```
/^(?=.*[0-9]+.*)(?=.*[a-zA-Z]+.*)[^ ]{8,32}$/
```

Le e-mail e i numeri di telefono vengono validati
Gli altri dati vengono filtrati automaticamente da Laravel con tecniche di Whitelisting.

Vengono loggati gli eventi di login e di login fallito.

L'app implementa un livello 1 di autenticazione con password complessa composta da minimo 10 caratteri, nonostante l'app tratti informazioni personali.
L'app implementa un recupero password semplice basato solo su e-mail.
La password è hashata utilizzando le funzioni standard e molto sicure fornite da PHP.
La sessione di un utente è mantenuta tramite un token lungo 32bytes memorizzato nel DB e generato casualmente utilizzando funzioni sicure fornite da PHP. La sessione scade e l'utente è obbligato a rieffettuare il login in seguito alla scadenza. Il token deve essere inviato per ogni richiesta effettuata all'API.

È consentito l'accesso sulla macchina virtuale su Aruba a un solo utente. L'accesso viene loggato attraverso il sistema di logging di Windows, automaticamente configurato.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Tracciabilità

L'applicazione effettua logging di tutte le richieste utilizzando il Sistema di logging presente in Lumen. I log sono consistenti a livello di Timestamp e loggano informazioni utili (IP e user-id). Non vengono loggati dati personali.
La macchina virtuale di Aruba logga tutti gli accessi attraverso il sistema di logging di Windows, automaticamente configurato.

Valutazione: Accettabile

Archiviazione

I dati personali e i log sono protetti dal danneggiamento fisico dei dischi rigidi, poiché la macchina è su sistema Cloud e quindi distribuito.
Verranno effettuati backup periodici dei dati sul DB su un altro server.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Minimizzazione dei dati

I dati memorizzati sono il minimo necessario per poter fornire il servizio, ovvero nome del paziente, numero di telefono e data dell'appuntamento.

Valutazione: Accettabile

Commento di valutazione:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Vulnerabilità

Il DB è chiuso all'esterno e i dischi rigidi, trattandosi di un Cloud, non possono danneggiarsi. Verranno effettuati backup periodici dei dati sul DB su un altro server. Windows server è aggiornato all'ultima versione disponibile.

Verranno verificati nuovi aggiornamenti. Il software (sia API che App) è mantenuto su un repository Git e in seguito a fase di test viene rilasciato in produzione.

Le librerie utilizzate nel software provengono da fonti sicure e vengono gestiti da Composer per quanto riguarda le API e da NPM per quanto riguarda l'app Cordova. Le versioni delle librerie sono le ultime e sono stati lanciati tool di ricerca vulnerabilità sulle librerie che hanno risposto nei seguenti modi.

API: API - Symfony Security Check Report - No packages have known vulnerabilities;

App Cordova: (Utilizzando Retire.js)

L'unica vulnerabilità nota è una vulnerabilità di jQuery che viene esposta solamente se la libreria è usata in Drupal o in altri CMS (non il caso di FollowUpp)

Le librerie utilizzate non hanno vulnerabilità note e l'aggiornamento delle versioni delle librerie è gestibile facilmente con Composer e NPM. Le uniche librerie non gestite automaticamente sono jQuery e jQuery-UI nell'app Cordova, per limitazioni della tecnologia, in ogni caso si possono aggiornare manualmente e rilasciare una nuova versione dell'app in qualsiasi momento.

Valutazione: Accettabile

Commento di valutazione:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Lotta contro il malware
L’unica postazione è una macchina virtuale su Aruba. La macchina viene usata solo da un utente per la gestione del server. Il personale è autorizzato a utilizzare solo macchine protette.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Gestione postazioni
L’unica postazione è una macchina virtuale su Aruba. La macchina viene usata solo da un utente per la gestione del server. Il personale è autorizzato a utilizzare solo macchine protette.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Sicurezza dei siti web
L’app non comunica con siti web. Le API utilizzano protocollo HTTPS. L’unica pagina web front-end è una pagina utilizzata per la disiscrizione degli interessati/ beneficiari. La pagina non usa cookie e la disiscrizione viene effettuata tramite un token anonimo generato a ogni richiesta che viene rimandato indietro al server.

Valutazione: Migliorabile
Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Backup
Verranno effettuati backup periodici dei dati sul DB su un altro server.

Valutazione: Migliorabile
Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Manutenzione
La Manutenzione è gestita da Aruba. La manutenzione fisica non avviene su una macchina dedicata, dato che viene utilizzato un sistema Cloud distribuito.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Contratto con il responsabile del trattamento
Le sopra citate misure di sicurezza e protezione dei dati sono garantite dal sub-responsabile del trattamento (StepApp Srl) e specificate nel relativo contratto di nomina. Per quanto riguarda la fornitura di servizi Cloud: si collocheranno i trattamenti dei dati dei medici ed i trattamenti dei dati dei pazienti.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Sicurezza dei canali informatici
Il firewall Windows Defender è configurato e attivo sulla macchina virtuale.
Le porte del DB non sono accessibili dall'esterno ed è visibile solo dalla macchina stessa.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Sicurezza dell'hardware
Il server è impostato su una infrastruttura virtuale di Aruba Cloud. Vengono osservati da Aruba seguenti parametri di funzionalità operativa:
A) Risorse del Data Center attraverso il quale viene erogato il Servizio: - Uptime del 100% su base annuale per alimentazione elettrica e/o climatizzazione ambientale;
- Uptime del 99,95% su base annuale, di accessibilità tramite rete internet alla Infrastruttura virtuale creata ed allocata dal Cliente;
B) Infrastruttura virtuale creata ed allocata dal Cliente: - Uptime del 99,95% su base annuale, per la disponibilità dei nodi fisici (server) che ospitano l'Infrastruttura virtuale;

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Protezione contro fonti di rischio non umane
Per quanto riguarda l'infrastruttura virtuale le misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.) sono individuate dal fornitore Aruba e ritenute idonee da Meeter e dai suoi sub-fornitori.

Valutazione: Accettabile
Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.

Pseudonimizzazione
Nella tabella degli appuntamenti presente nel cloud Aruba il riferimento al nominativo del medico viene mutato in ID e non nel nominativo esteso.

Valutazione: Accettabile

Commento di valutazione:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi

effettivamente realizzati, se è possibile implementare le azioni previste.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

RICEVIMENTO DI COMUNICAZIONI NON INERENTI AL SERVIZIO, MANCATO RICEVIMENTO DI SMS DI REMIND, RICEVIMENTO DI UN REMIND ERRATO, PERDITA DEGLI APPUNTAMENTI IN AGENDA DEL MEDICO, MODIFICA DEGLI APPUNTAMENTI IN AGENDA

Quali sono le principali minacce che potrebbero concretizzare il rischio?

ALTERAZIONE NON AUTORIZZATA DEL DATABASE, ELIMINAZIONE NON AUTORIZZATA TOTALE O PARZIALE DEL DB, UTILIZZO DEL DATABASE CON I RIFERIMENTI DEI MEDICI PER FINALITA' DIVERSE DA QUELLE INDIVIDUATE, UTILIZZO DEL DATABASE CON I RIFERIMENTI DEI PAZIENTI PER FINALITA' DIVERSE DA QUELLE INDIVIDUATE

Quali sono le fonti di rischio?

FONTI UMANE INTERNE, FONTI UMANE ESTERNE, FONTI NON UMANE

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Controllo degli accessi logici, Tracciabilità, Sicurezza dell'hardware, Backup, Sicurezza dei siti web, Manutenzione, Contratto con il responsabile del trattamento, Protezione contro fonti di rischio non umane, Archiviazione, Sicurezza dei canali informatici, Pseudonimizzazione

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Trascurabile, Ove, nonostante le misure di sicurezza impostate, vi fosse accesso da parte di malintenzionati, anche le comunicazioni sono state impostate in modo da non rendere immediatamente riconducibile ad una visita medica il testo del messaggio sms di remind.
Nella tabella relativa ai beneficiari presente sul server Aruba sono rinvenibili esclusivamente:
- appuntamento individuato da numero di telefono, nome e cognome, data e ora
- combinazione con ID (pseudonimizzazione) e pertanto non immediatamente riferibile a medico

Nella tabella relativa agli utenti medici presente sul server Aruba sono rinvenibili esclusivamente:
- dati di registrazione

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, La DPA sottoscritta con il responsabile Aruba garantisce contro le minacce e fonti di rischio, mentre le misure pianificate consentono di ritenere il rischio trascurabile.

Valutazione: Migliorabile

Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)? Trascurabile
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)? Trascurabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

RICEVIMENTO DI COMUNICAZIONI NON INERENTI AL SERVIZIO, RICEVIMENTO DI UN REMIND ERRATO, MODIFICA DEGLI APPUNTAMENTI IN AGENDA, PERDITA DEGLI APPUNTAMENTI IN AGENDA DEL MEDICO

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

ALTERAZIONE NON AUTORIZZATA DEL DATABASE, ELIMINAZIONE NON AUTORIZZATA TOTALE O PARZIALE DEL DB, UTILIZZO DEL DATABASE CON I RIFERIMENTI DEI MEDICI PER FINALITA' DIVERSE DA QUELLE INDIVIDUATE, UTILIZZO DEL DATABASE CON I RIFERIMENTI DEI PAZIENTI PER FINALITA' DIVERSE DA QUELLE INDIVIDUATE

Quali sono le fonti di rischio?
FONTI NON UMANE, FONTI UMANE ESTERNE, FONTI UMANE INTERNE

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Sicurezza dei siti web, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane, Pseudonimizzazione

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile, Ove, nonostante le misure di sicurezza impostate, vi fosse una modifica non autorizzata dei dati personali, le misure individuate consentono di abbattere notevolmente le conseguenze sugli interessati.
Nel testo degli sms non c'è riferimento a termini direttamente riconducibili allo stato di salute.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile, La DPA sottoscritta con il responsabile Aruba garantisce contro le minacce e fonti di rischio, mentre le misure pianificate consentono di ritenere il rischio trascurabile.

Valutazione: Migliorabile

Piano d'azione / misure correttive:
Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)? Trascurabile
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)? Trascurabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
MANCATO RICEVIMENTO DI SMS DI REMIND, PERDITA DEGLI APPUNTAMENTI IN AGENDA DEL MEDICO

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
ELIMINAZIONE NON AUTORIZZATA TOTALE O PARZIALE DEL DB

Quali sono le fonti di rischio?
FONTI NON UMANE, FONTI UMANE ESTERNE, FONTI UMANE INTERNE

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Controllo degli accessi logici, Archiviazione, Vulnerabilità, Lotta contro il malware, Backup, Sicurezza dei siti web, Manutenzione, Sicurezza dei canali informatici, Contratto con il responsabile del trattamento, Sicurezza dell'hardware, Protezione contro fonti di rischio non umane

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, L'individuazione degli impatti principali, ovvero: mancato ricevimento di sms di remind lato paziente / beneficiario e perdita degli appuntamenti lato medico / utente è considerata in ogni caso limitata, in quanto l'app non è l'unico strumento di contatto tra il paziente ed il medico, in quanto quest'ultimo ha altri canali di comunicazione diretti ed immediati con il paziente.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

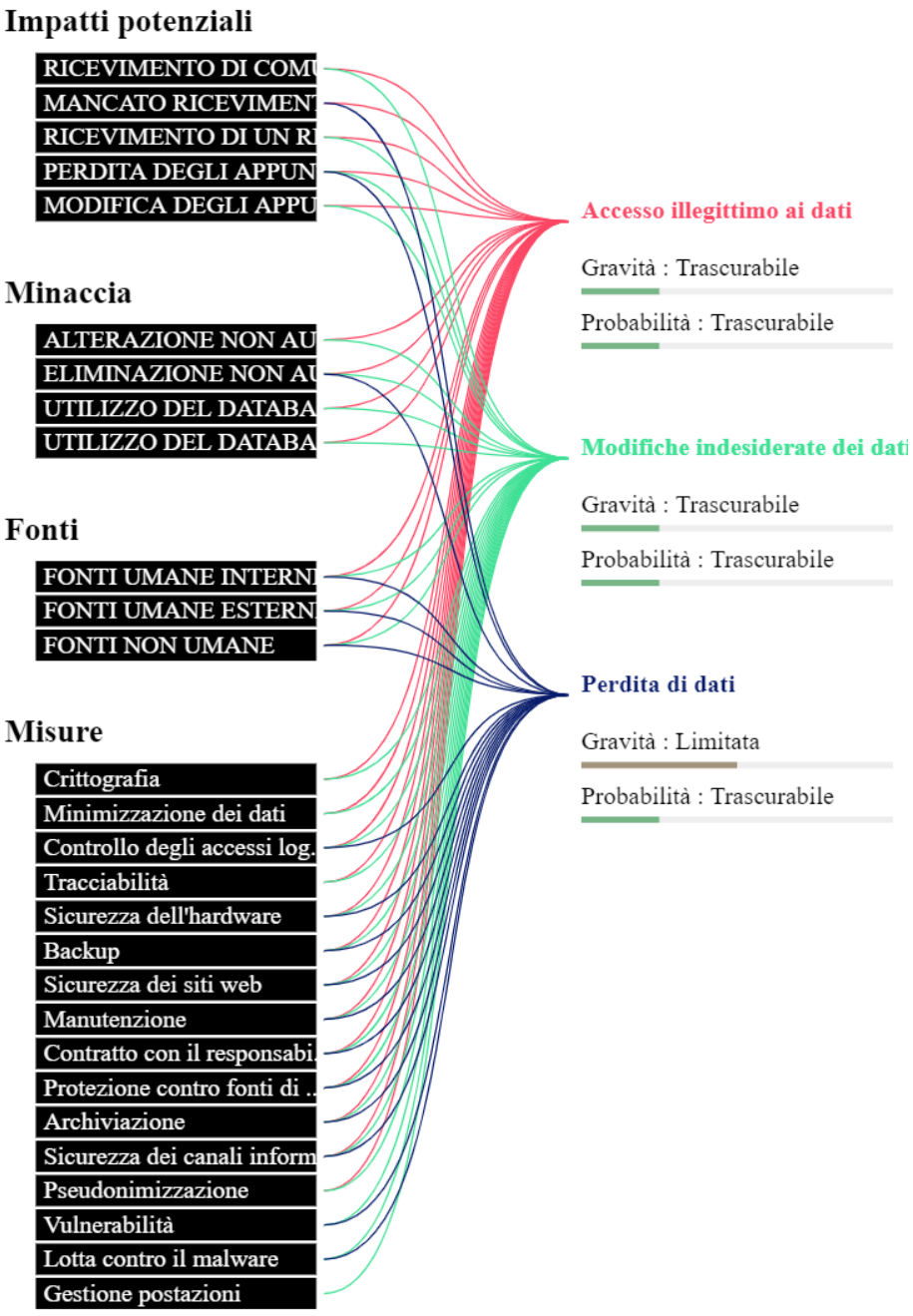
Trascurabile, La DPA sottoscritta con il responsabile Aruba garantisce contro le minacce e fonti di rischio, mentre le misure pianificate consentono di ritenere il rischio trascurabile.

Valutazione: Migliorabile

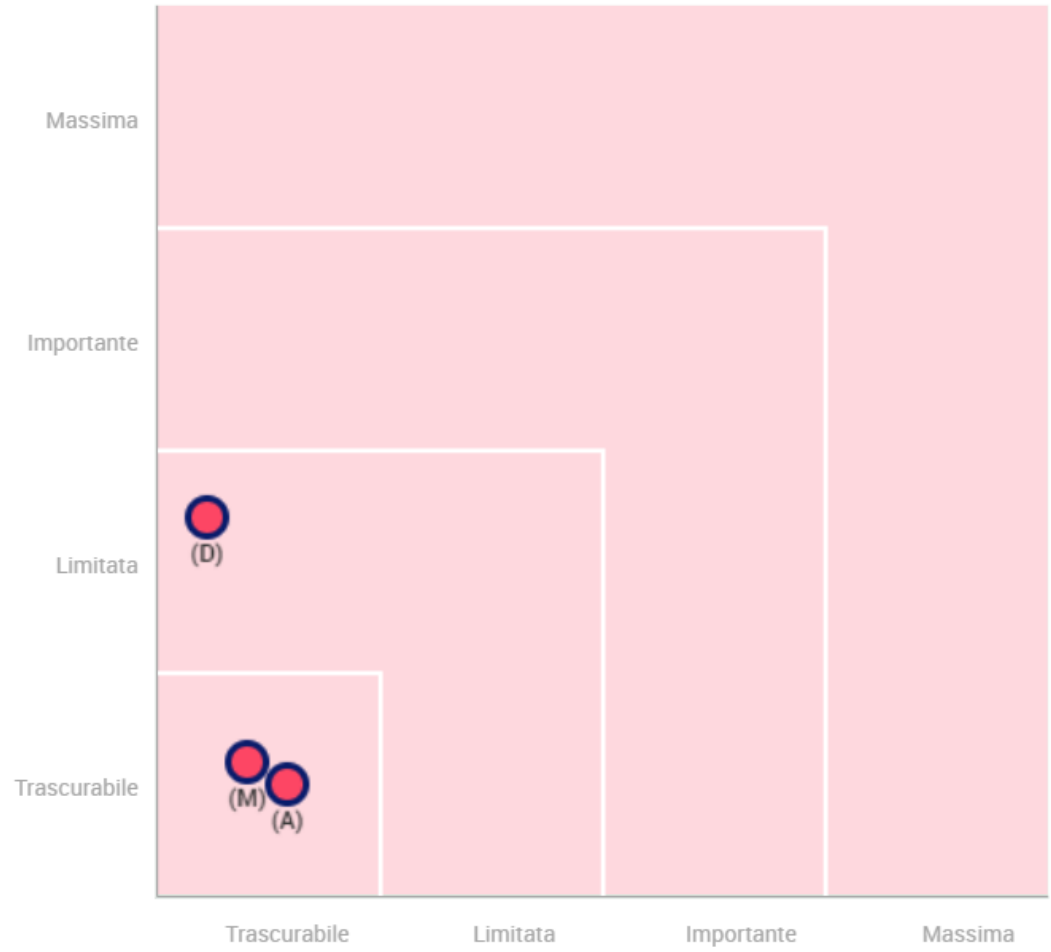
Piano d'azione / misure correttive:

Si intende monitorare il piano programmato dopo i primi tre mesi di utilizzo di FollowUpp, per verificare, con i casi effettivamente realizzati, se è possibile implementare le azioni previste.
Alla luce del piano d'azione, come valutate la gravità di questo rischio (Perdita di dati)? Limitata
Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Perdita di dati)? Trascurabile

Panoramica dei rischi


Impatti potenziali
RICEVIMENTO DI COMU
MANCATO RICEVIMENT
RICEVIMENTO DI UN R
PERDITA DEGLI APPUN
MODIFICA DEGLI APPU
Minaccia
ALTERAZIONE NON AU
ELIMINAZIONE NON AU
UTILIZZO DEL DATABA
UTILIZZO DEL DATABA
Fonti
FONTI UMANE INTERN
FONTI UMANE ESTERN
FONTI NON UMANE
Misure
Crittografia
Minimizzazione dei dati
Controllo degli accessi log.
Tracciabilità
Sicurezza dell'hardware
Backup
Sicurezza dei siti web
Manutenzione
Contratto con il responsabi
Protezione contro fonti di ..
Archiviazione
Sicurezza dei canali inform
Pseudonimizzazione
Vulnerabilità
Lotta contro il malware
Gestione postazioni
Accesso illegittimo ai dati
Gravità : Trascurabile
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile

Gravità del rischio



Probabilità del rischio

- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

18/02/21