SCHEDA TECNICA

ALL. B – TERMINI E CONDIZIONI DI LICENZA

1. DESCRIZIONE DELLA PIATTAFORMA

WebApp nel campo della teleriabilitazione. Piattaforma che affianca i professionisti nella gestione del trattamento fisioterapico dei propri pazienti attraverso l'utilizzo di machine learning per l'estrapolazione di programmi di esercizio terapeutico.

2. INFORMAZIONI TECNICHE

CPU	ND
RAM	ND
Spazio su hard disk	ND (Vengono utilizzati EBS e S3)
OS	NixOS
Client supportati	ND
File System	ND
Rete	ND
Servizi	ND
Manutenzione dischi	ND
Accesso	ND
File Server	ND
Backup	Sì, quotidiano in server farm diversa.
Manutenzione	Sistemista CodeWorks 24/7. Infrastruttura gestita da AWS.
Gestione e conservazione dati	Retention di 7 giorni.

3. MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

MISURA DI SICUREZZA	DESCRIZIONE
Politiche per la Sicurezza	Il Responsabile stabilisce e adotta un insieme di policy e procedure per la sicurezza dei dati personali conformi alla Normativa applicabile.
	Il Responsabile del trattamento ha ottenuto le seguenti certificazioni: NESSUNA CERTIFICAZIONE ISO
Governance	Il Responsabile definisce i ruoli e assegna tutte le responsabilità conformemente alle policy per la sicurezza dei dati, al fine di garantire la corretta gestione del rischio derivante dal trattamento dei dati attraverso i propri sistemi applicativi. Tali responsabilità vengono stabilite riducendo al minimo la possibilità di un uso improprio, modifica non autorizzata o non intenzionale dei dati personali.
	Il Responsabile predispone uno schema organizzativo/organigramma di *governance* privacy, che individua i ruoli e le responsabilità di ciascun soggetto.
Formazione Privacy e Security	**Politiche di protezione dei dati personali** **Requisito:** *Il Responsabile del trattamento deve implementare un proprio sistema di tutela dei dati personali.* *Gli elementi includono:* *– Una struttura organizzativa vigente per la protezione dei dati con responsabilità definite (incl. la nomina di un responsabile della protezione dei dati, qualora richiesto a livello legale)* *– Conformità a tutti i requisiti legali per la protezione dei dati personali* *– Sistema di gestione dei contratti vigente per la conservazione di tutti gli accordi relativi alla protezione dei dati (es. accordi per il trattamento dei dati, accordi con sub-responsabili del trattamento ecc.)* *– Formazione sulla tutela dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* *– Accordi sulla riservatezza dei dati personali per i dipendenti del Responsabile del trattamento che trattano i dati personali del Titolare del trattamento* *– Una procedura che garantisce i diritti dei soggetti interessati (in cooperazione con il Titolare del trattamento)* *L'adozione di certificazioni sulla sicurezza dei dati e l'adesione a codici di condotta possono essere validi strumenti di controllo delle politiche di protezione*

	*A tal fine vengono messe in atto le seguenti **misure organizzative**:* *☒Registro del trattamento in qualità di responsabile* *☒Analisi dei rischi che incombono sugli interessati in relazione ai trattamenti effettuati* *☒Nomina di un responsabile della protezione dei dati (se richiesto a livello legale)* *☒Contratti con i fornitori che svolgono parte dei trattamenti affidati (sub-responsabili) che prevedono meccanismi di tutela dei dati personali e relativi accordi di riservatezza* *☒Piano di formazione del personale in relazione alla tutela dei dati personali* *☒Adozione di un accordo di riservatezza per il personale a cui è affidato il trattamento* *☒Procedura per la risposta alle richieste di esercizio dei diritti degli interessati* *☒Registrazione delle richieste di esercizio dei diritti degli interessati*
Sub-fornitori	Se previsto l'impiego di sub-fornitori, il Responsabile garantisce che i requisiti minimi e i livelli di sicurezza del sub-fornitore siano quelli stabiliti e concordati con il Titolare.
Protezione dei Dati	**Pseudonimizzazione e cifratura** – Per i dati più critici è opportuno adottare ulteriori misure di sicurezza per evitare la comprensibilità e l'usabilità dei dati anche in caso di furto o accesso non autorizzato. **Requisito:** *Nei casi in cui il trattamento riguardi dati particolari o relativi a condanne penali o reati, nonché per i dispositivi a maggiore mobilità e quindi più soggetti a furti e smarrimenti, è opportuno applicare misure tecniche e organizzative per limitare la possibilità di utilizzo dei dati da parte di soggetti non autorizzati.*
	*A tal fine vengono messe in atto le seguenti **misure tecniche**:* *☒Cifratura dei dati sensibili in cloud* *E le seguenti **misure organizzative**:* *☒Politiche di conservazione e gestione delle chiavi di cifratura* *☒Rimozione degli elementi identificativi degli interessati ove non necessari (fasi di sviluppo, rendicontazione, uso o comunicazione di dati aggregati)*
Autenticazione ai sistemi	vedi Password Policy
Password Policy	***Controllo logico degli accessi** - L'accesso logico ai sistemi di trattamento, alle applicazioni e ai dati deve essere riservato esclusivamente ai soggetti autorizzati.* ***Requisito**: è necessario evitare l'accesso non autorizzato ai sistemi IT. Devono essere messe in atto misure tecniche e organizzative per l'identificazione e l'autenticazione degli utenti.* *L'accesso ai sistemi IT del Responsabile del trattamento deve essere limitato agli utenti autorizzati mediante un processo di autenticazione sicuro. Ogni utente deve avere un ID utente univoco. La condivisione degli account non è consentita. L'accesso ai sistemi IT e alle applicazioni del Responsabile del trattamento deve essere accessibile tramite sistemi di autenticazione che prevede come requisito minimo l'utilizzo di credenziali composte da nome utente e password. Tale protezione deve includere ma non essere limitata a una policy per la password sicura, una disconnessione automatica dopo un determinato periodo di tempo, il blocco in seguito a diversi tentativi di accesso falliti, una procedura di ripristino della password affidabile, una modifica periodica delle password. Le password devono essere sempre conservate e trasmesse in modo sicuro, ad es. mediante crittografia e funzione hash. Il Responsabile del trattamento ha definito i requisiti, le regole e gli standard delle linee guida per le password in una politica conosciuta dagli utenti è supportata a livello tecnico. Le password devono essere assegnate a una singola persona, conservate e trasmesse in modo sicuro, essere sufficientemente lunghe e complesse, modificate su base regolare, limitate in termini di validità, bloccate e successivamente eliminate se inattive per un lungo periodo di tempo e modificate immediatamente qualora compromesse. Ove possibile, in particolare per le utenze con privilegi elevati e per i sistemi e le applicazioni che ospitano dai particolari, si predilige l'utilizzazione di sistemi di autenticazione a più fattori*
	*A tal fine vengono messe in atto le seguenti **misure tecniche**:* *☒Autenticazione con username e password* *☒Autenticazione a due fattori* *☒Utilizzo di certificati digitali per l'autenticazione* *☒Sistemi di Single Sign On* *☒Sistemi di controllo scadenza password* *☒Sistemi di controllo robustezza e complessità password* *☒Sistemi di blocco account dopo numero predefinito di tentativi falliti* *☒Utilizzo password o pin per i dispositivi mobili*

	☒ *Time-out sessione per le applicazioni* *E le seguenti **misure organizzative**:* *☒Procedure di assegnazione degli account* *☒Inventario aggiornato degli account assegnati* *☒Inventario aggiornato degli account di servizio utilizzati dalle applicazioni* *☒Cancellazione o disabilitazione degli account non utilizzati dopo un periodo di tempo definito* *☒Formazione del personale sull'uso account aziendali* *☒Regolamenti o politiche per gli account aziendali e la robustezza delle password* *☒Procedure di azzeramento o ripristino password*
Profili Utenti	**Profili di autorizzazione e controllo delle autorizzazioni** – Nessuna lettura, copia, modifica o rimozione non autorizzata all'interno del sistema informatico o per il trattamento di dati su supporti cartacei. **Requisito:** *Il Responsabile del trattamento deve definire specifici profili di autorizzazione per i soggetti che accedono ai dati e mettere in atto soluzioni per il controllo dei diritti di accesso e le necessarie autorizzazioni, che devono essere strettamente limitate a consentire l'attività delegata al soggetto autorizzato. Il controllo delle autorizzazioni prevede anche politiche e strumenti di monitoraggio e di registrazione degli accessi ai dati. Particolare attenzione deve essere posta all'assegnazione di privilegi elevati, che devono essere riservati ai tecnici che effettuano operazioni di amministrazione dei sistemi, delle banche dati e delle applicazioni (cd. Amministratori di sistema). Gli amministratori di sistema devono avere un account con privilegi elevati individuale per eseguire le loro attività di amministrazione diverso da quello utilizzato per le attività che non richiedono diritti particolari. I dischi e le memorie destinate allo smaltimento o riutilizzo devono essere distrutti o soggetti a cancellazione sicura.*
	*A tal fine vengono messe in atto le seguenti **misure tecniche**:* *☒Ruoli e autorizzazioni basati sul principio della necessità di accesso ai dati* *☒Configurazione dei file server con aree ad accesso limitato in base alle autorizzazioni assegnate* *☒Configurazione delle applicazioni per l'assegnazione di privilegi minimi per eseguire l'attività assegnata all'utente* *☒Sistema di registrazione (log) delle modifiche dei privilegi assegnati* *☒Sistema di alert delle modifiche dei privilegi assegnati* *☒Sistema di registrazione (log) dell'accesso ai sistemi da parte degli amministratori di sistema* *☒Sistema di registrazione (log) dell'accesso alle applicazioni o ai database da parte degli amministratori di sistema* *E le seguenti **misure organizzative**:* *☒Creazione di profili utente con autorizzazioni in base al ruolo e a compiti assegnati (Segregation of duty, need to know e last privilege)* *☒Riesame regolare delle autorizzazioni* *☒Account con privilegi amministrativi individuali e utilizzati solo quando necessario* *☒Account individuali anche per i tecnici esterni che necessitano di credenziali amministrative* *☒Verifica delle caratteristiche soggettive di esperienza, capacità e affidabilità degli amministratori di sistema* *☒Elenco aggiornato degli amministratori di sistema, con il dettaglio dei compiti assegnati* *☒Verifica periodica delle attività degli amministratori di sistema*
Reti di comunicazione	
Protezione della rete	**Protezione della rete e dei dispositivi –** La rete, gli host e i dispositivi collegati in rete devono disporre di misure di protezione da attacchi di malintenzionati e da software malevolo. **Requisito:** *il Responsabile del trattamento è obbligato ad adottare le misure tecniche e organizzative per garantire la disponibilità (oltre alla riservatezza e l'integrità) dei dati trattati proteggendo la rete, i dispositivi e i dati conservati, elaborati o in transito da effetti dovuti a software malevolo o attacchi di malintenzionati. I dati devono essere elaborati, trasmessi e conservati con strumenti la cui sicurezza è implementata secondo gli standard*
	*A tal fine vengono messe in atto le seguenti **misure tecniche**:* *☒Protezione tramite sistemi firewall* *☒Appliance UTM (Unified Threat Management)* *☒Sistemi IDS, IPS o IDPS* *☒Sistemi NAC (Network Access Control)* *☒Sistemi DLP* *☒Sistemi SIEM*

Antivirus	
IPS	
Mobile Device Management	Il Responsabile adotta misure di sicurezza aggiuntive per la gestione dei rischi introdotti dall'uso di dispositivi portatili (qualora ne sia previsto l'utilizzo) che consentono accesso ai dati.
Backup	**Controllo delle disponibilità e controllo della recuperabilità –** Salvataggio periodico dei dati e procedure per recuperare i dati il prima possibile. **Requisito:** *I dati devono essere conservati i più copie su reti/sistemi/sedi separate. Il Responsabile del trattamento deve mettere in atto una politica di backup e di ripristino che garantisce il recupero del sistema e dei dati.*
	*A tal fine vengono messe in atto le seguenti **misure tecniche**:* *☒Sistemi di backup in cloud* *☒Sistemi di disaster recovery con piattaforme DRaaS in cloud* *A tal fine vengono messe in atto le seguenti **misure organizzative**:* *☒Contratti con i fornitori per la fornitura di hardware sostitutivo con tempi definiti (SLA)* *☒Piani di backup e di recovery del software, delle configurazioni e dei dat* *☒Procedure di continuità operativa* *☒Procedure di ripristino dei dati*
Continuità operativa	
Gestione degli incidenti	**Gestione delle risposte agli incidenti che possono comportare violazioni dei dati personali / data breach** **Requisito:** *Il Responsabile del trattamento deve implementare un proprio sistema di gestione degli incidenti e delle violazioni dei dati personali (cd. Data breach).* *Gli elementi includono:* *– Un processo per segnalare violazioni della protezione dei dati personali (in particolare in cooperazione con il Titolare del trattamento)* *Una procedura per la gestione degli incidenti che possono comportare violazioni dei dati personali*
	*A tal fine vengono messe in atto le seguenti **misure organizzative**:* *☒Procedura per la risposta ad incidenti di sicurezza* *☒Procedura per la gestione e la notifica delle violazioni dei dati (data breach)* *☒Adozione di un registro dei data breach*