I N D I C E

REV.	REDATTO	VERIFICATO	APPROVATO	DATA DI EMISSIONE
02	DS	RQ	RL	04/01/2021

1. SCOPO

Scopo della presente procedura è quello di definire le responsabilità, le attività e le registrazioni da effettuare per garantire nel tempo l'idoneità dei Sistemi Informativi utilizzati per l'erogazione dei servizi, al fine di mantenere nel tempo la conformità alle normative di legge stabiliti per l'accreditamento istituzionale.

2. RIFERIMENTI

- Regione Siciliana - Legge n. 39/1988
- Assessorato Regionale alla Salute - Decreto n. 890/2002
- DECRETO 3 settembre 2021. Definizione dei requisiti organizzativi, strutturali e tecnologici per l'autorizzazione all'esercizio e per l'accreditamento del soggetto deputato al governo dell'accesso alle cure domiciliari
- D. Lgs. 196/03 e ss.mm.ii. – Codice privacy
- D. Lgs. 101/18 (modifiche al Codice privacy)
- Regolamento UE 679/2016 – Regolamento europeo per la protezione dei dati personali
- Norma ISO 9001:2015 punto 7.1.3

3. CAMPO DI APPLICAZIONE

Le norme della presente procedura si applicano alle attività finalizzate a garantire nel tempo la conformità alle normative e la piena efficienza del sistema informativo ed apparecchiature biomedicali per l'erogazione delle prestazioni sanitarie.

4. LISTA DI DISTRIBUZIONE

La presente procedura viene inviata per la sua approvazione ed applicazione a:

- Rappresentante Legale
- Direttore Sanitario
- Direttore Amministrativo
- Responsabile Qualità
- RSPP

5. ATTIVITA' E RESPONSABILITA'

Il costante controllo e la corretta manutenzione delle infrastrutture sono fondamentali ai fini della realizzazione ed erogazione di un servizio in grado di soddisfare pienamente le attese del cittadino utente in un contesto di sicurezza per i pazienti e per gli Operatori.

Particolare rilievo assume la necessità di garantire al cittadino utente la facilità di accesso ai servizi ed il comfort indispensabile per tutto il periodo della sua fruizione, nonché di assicurare a tutto il Personale che opera all'interno della SISIFO in condizioni ambientali di sicurezza e di razionalità sotto il profilo logistico che consentano di svolgere al meglio le attività cui è preposto.

La progettazione e realizzazione delle infrastrutture ha seguito le prescrizioni di legge in ordine ai requisiti minimi richiesti alle cure domiciliari per l'accreditamento da parte del SSR; la politica della qualità della SISIFO tende, tuttavia, a superare tali requisiti minimi per offrire agli operatori elevati standard di qualità in grado di soddisfare al meglio le loro esigenze.

La dotazione di

La tabella seguente riporta sinteticamente le responsabilità per la corretta attuazione del presente piano, le cui attività sono dettagliate nei paragrafi successivi.

Funzioni	*Responsabilità*

Funzioni	*Responsabilità*
Comitato Qualità	▪ Riesame della adeguatezza delle infrastrutture
Rappresentante Legale	▪ Acquisto nuovi strumenti informatici ▪ Stipula dei contratti di manutenzione
Direzione	▪ Approvazione di procedure ed istruzioni operative
Referente Manutenzione di PC e di dispositivi Informatici	▪ Definizione del piano di manutenzione e controllo delle infrastrutture ▪ Redazione bozze di procedure ed istruzioni operative ▪ Gestione dei rapporti con le ditte di manutenzione ▪ Coordinamento attività manutentori interni ▪ Supervisione lavori effettuati da ditte esterne ▪ Partecipazione ai facility tour ▪ Reporting alla Direzione sullo stato degli impianti
Responsabile Servizio Prevenzione e Protezione	▪ Conduzione dei facility tour ▪ Formazione al personale sulle misure di sicurezza
Responsabile Qualità	▪ Verifica delle procedure ed istruzioni operative ▪ Partecipazione ai facility tour
Responsabile protezione dei dati personali	▪ Sorvegliare l'osservanza del regolamento ▪ Collaborare con il titolare/responsabile, laddove necessario, nel condurre una DPIA ▪ Informare e sensibilizzare la direzione ed il personale su obblighi derivanti dal regolamento ▪ Collaborare e fungere da punto di contatto con il Garante ▪ Supportare il titolare /responsabile

6. SISTEMA INFORMATIVO

In merito al sistema informativo , si rimanda alla consultazione del sistema di gestione dei dati e delle informazioni (GDPR 2016/679) che il consorzio SISIFO ha implementato per adempiere ai dettati normativi in materia di gestione e trattamento dei dati personali e delle informazioni che per la peculiarità del servizio vengono acquisite dai diversi operatori.
La responsabilità della redazione delle procedure di raccolta e verifica della qualità e diffusione dei dati, è stato affidato ad una società di consulenza (Siapa SRL) che ricopre anche il ruolo di DPO (Data Protection Officer)
Il Consorzio ha, con specifiche lettere autorizzative, identificato le figure abilitate al trattamento dei dati e alla corretta gestione e conservazione delle informazioni.

Specificatamente e solo in merito alla qualità delle informazioni e dei dati provenienti da fonti esterne e dai fonti interne legate allo svolgimento del servizio, il consorzio si è dotato di una serie di criteri per poter valutare affidabilità, accuratezza e validità.
Le principali fonti di dati e informazioni esterne sono i pazienti e i familiari dei pazienti e l'ASP di appartenenza. Le informazioni provenienti dall'ASP sono garantite alla fonte, trattandosi del servizio pubblico inviante.
Relativamente alle informazioni ottenute dai familiari, nella prima fase di accoglienza e valutazione, disponiamo di colloquio anamnestico approfondito, somministrazione di prove testologiche, somministrazione di questionari molto accurati e standardizzati, che ci permettono di individuare l'eventuale presenza di incongruenze e di evitare le informazioni sommarie e superficiali. La somministrazione diretta di test di sviluppo ci permette di verificare la congruenza fra le informazioni ricevute, le esigenze del paziente osservate

direttamente e le prescrizioni riportate nel PAI da parte dell'ASP territorialmente competente.
Relativamente ai dati e alle informazioni interne disponiamo di una serie di strumenti (diario clinico, griglie ecc) per il rilevamento quotidiano dell'andamento delle attività.
In merito a procedure/protocolli che definiscono le modalità con cui è garantita l'integrità e la sicurezza dei dati nonché le modalità di raccolta, conservazione e di tracciamento dei dati si rimanda alla consultazione del sistema privacy redatto ai sensi del Regolamento UE 2106/679.

Il piano di gestione del sistema informatico si distingue in quattro moduli orientati alla verifica di specifiche necessità.

- Inventario
- Sicurezza informatica
- Network management
- Mantenimento del sistema informativo

6.1. INVENTARIO

Al fine di costruire una mappa dettagliata delle varie unità composte da Hardware e Software, va redatto ed aggiornato a cura dell'addetto al Sistema Informativo, con il supporto della consulenza esterna, un inventario delle singole workstation e dei server. Tale attività prevede:

a) Inventario con etichettatura del parco Hardware installato con assegnazione di un numero ai singoli elementi componenti la stazione di lavoro. Le etichette identificheranno in maniera univoca i dispositivi per singola sede secondo un layout predefinito.

b) Compilazione per ogni singola sede della scheda tecnica apparecchiature in dotazione sulla quale vengono riportati tutti i dispositivi Hw presenti; con tali dispositivi si intendono: workstations, servers, printers, hubs, routers e switches e le informazioni relative all'installato Sw (Hw, pacchetti Sw e relativo numero di licenza per PdL).

c) aggiornamento delle schede di inventario Hw e del Sw installato in azienda a seguito di ogni spostamento o implementazione.

6.2. SICUREZZA INFORMATICA

6.2.1. Premessa

Le caratteristiche strutturali del Sistema Informativo Aziendale sono le seguenti:

- **Back-Up**

Il Back-Up del sistema viene effettuato giornalmente alle ore 21:30 su un NAS tenuto sempre acceso, nelle seguenti modalità:

- Pianificazione di una attività batch (.bat) che viene lanciata dal server HP e coinvolge le applicazioni in uso. Archivi Compresi.
- Windows Server Back-Up che copia l'immagine delle applicazioni e degli archivi del punto 1.

Il responsabile del sistema informativo si accerta periodicamente (almeno una volta alla settimana) che tale procedura avvenga regolarmente.

- **Gestione Antivirus**

L'amministratore di Sistema ha provveduto ad installare Kaspersky EndPoint Security 10 per Windows sul Windows Server 2008 che provvede alla gestione dei relativi Client installati sulle

postazioni di lavoro. Utilizziamo ovviamente i programmi di gestione dell'AV. Alcune stazioni sono coperte dall'antivirus WINDOWS SECURITY ESSENTIAL.

- **WI.FI.**

In ambito di collegamento WIFI sono stati ATTIVATI 8 Access Point che sono protetti da chiave cifrata. L'accesso è gestito da un Proxy che rilascia l'autorizzazione all'accesso tramite user ID e password.

- **Server**

Il server delle applicazioni viene gestito localmente o da remoto tramite un LAN Manager. L'accesso ad Internet e quindi l'intera infrastruttura infotelematica aziendale è protetta da attacchi esterni tramite un Firewall "Endian" che permette anche la creazione di tunnel VPN (Virtual Private Network) per l'accesso e la gestione da remoto ad utenti regolarmente registrati e protetti riconoscibili con l'immissione di user e password.
Il Firewall è ovviamente aggiornato in rete sulle più recenti "firme" utilizzate dagli hacker per l'accesso fraudolento alla struttura.
Tramite il Firewall è possibile abilitare o disabilitare accessi esterni a servizi e/o indirizzi interni alla struttura.

6.2.2. Applicativi di gestione dell'assistenza e flussi comunicativi

DESCRIZIONE DEGLI APPLICATIVI DI GESTIONE
A seguito del Decreto Assessoriale del 6 Luglio 2010 pubblicato sulla GURS del 23 Luglio 2010 Parte I n° 33 contenente il "*Nuovo disciplinare tecnico per la predisposizione del tracciato record relativo all'assistenza domiciliare integrata*", la SISIFO ha l'obbligo di comunicare, per via telematica, all'Assessorato Regionale alla Salute secondo lo schema del tracciato contenuto nell'All. 1 al richiamato Decreto, una serie di dati tra i quali:

- Anagrafica del cliente (Paziente)
- Codici di Patologia
- Tipologia operatore
- Tipologia di interventi effettuati
- Etc.

Al fine di ottemperare a tale obbligo, ciascun OS nel consegnare periodicamente in SISIFO i diari relativi ai propri interventi, deve compilare il modello MD 8.5-001-056 Rev. 1"Rilevazione Tipo di Prestazione Domiciliare Integrata" (completo di legenda) che, caricato sul sistema gestionale SISIFO, viene trasferito all'ASP competente territorialmente e, da questa, al Ministero della Salute. Poiché la raccolta e la trasmissione di tali dati sensibili in forma analitica, è voluta da una Legge, il trattamento è possibile senza particolari autorizzazioni.

6.2.3. Gestione degli accessi

Nell'ottica della salvaguardia dell'integrità e della inviolabilità dei dati informatici, sono state definite le politiche di sicurezza più idonee garantendo l'accesso al sistema al personale autorizzato e differenziando le possibilità di accesso alle informazioni in base al profilo dell'utente.
A tal fine la procedura informatizzata contiene una tabella Utenti con l'elenco del personale autorizzato ed il rispettivo profilo d'accesso (Archivi/Operatori). Tutte le variazioni al profilo dell'utente, nonché l'esclusione dal sistema informativo e le aggiunte saranno gestite dall'Amministratore di sistema e comunicate per iscritto al Responsabile della Privacy. Ad ogni operatore autorizzato ad accedere alla rete informatica aziendale sono attribuite una *user ID*

e una *password* personale, che lo stesso si impegna a rinnovare periodicamente (ogni 6 mesi) e a non comunicare a terzi. È vietato utilizzare la user ID o la password di altro operatore.

6.2.4. Gestione database

L'Amministratore di sistema verifica, tramite idonea documentazione, l'identità dei soggetti ai quali consente l'accesso al database, ovvero la veridicità dei dati identificanti i soggetti autorizzati all'accesso. Copia della suddetta documentazione deve essere conservata presso l'ufficio del Personale per l'intera durata di validità delle credenziali di autenticazione concesse. L'autorizzazione all'accesso viene revocata contestualmente alla cessazione del rapporto contrattuale

L'addetto al sistema informativo, in collaborazione con la software house esterna, verifica all'atto dell'installazione, e successivamente tramite cicliche rivalutazioni, l'impossibilità da parte degli operatori di accedere ai dati archiviati per distruggerli, deteriorarli cancellarli, sopprimerli o alterarli sotto ogni forma, in tutto o in parte. Per nessuna ragione SISIFO consente che uno degli operatori di sistema abbia all'interno del suo abituale profilo la possibilità di effettuare le suddette modifiche.

E' fatto salvo il diritto dell'interessato di richiederne formalmente l'integrazione, la cancellazione o la rettifica che dovranno avvenire tramite un apposito profilo, utilizzabile esclusivamente dall'Amministratore di Sistema per il tempo strettamente necessario al compimento di tale operazione. Per la salvaguardia dei dati si procede a backup periodici ed alla installazione e manutenzione di opportuni programmi antivirus e fire-wall.

6.2.5. Gestione del software

La Casa di cure ha installato, in conformità alla normativa vigente, il software di terze parti che partecipano al processo formativo del dato utilizzato per la rendicontazione delle attività svolte e la loro successiva fatturazione e per l'analisi dei flussi informativi.

L'addetto al Sistema Informativo Aziendale effettua un costante monitoraggio sulla corrispondenza tra i settaggi dei suddetti programmi e le disposizioni in materia. E' fatto divieto ad ogni operatore di modificare contenuti e settaggi dei suddetti programmi, se non in ottemperanza di idonee disposizioni da parte dell'Ente Pubblico di riferimento ed esclusivamente per la parte che il programmatore del software avrà lasciato alla configurazione ad opera dell'utente finale.

E' fatto altresì espresso divieto agli operatori di procurarsi, riprodurre, diffondere, comunicare o consegnare codici, parole chiave o altri mezzi idonei al superamento delle misure di sicurezza poste a protezione dei software.

6.2.6. Disaster recovery

Per assicurare la tutela dei dati a fronte di un evento catastrofico che può interessare la struttura della Casa di cure si è attivata una procedura per custodire una copia di sicurezza dei dati delle applicazioni critiche presso il Data Center. La procedura prevede:

- ☐ Terza copia di sicurezza remota dei dati
- ☐ Spazio di 2 TB (espandibili) in area protetta su cui copiare periodicamente i dati dei programmi principali in uso:
- ☐ Sicurezza nel transito (utilizzo di VPN/SSL) e nella custodia dei dati (Cifratura).

I dati dalle applicazioni sono copiati (settimanalmente) su un area di storage localizzata presso Sisifo. la copia incrementale (solo le differenze) dei dati viene inviata al Data Center.

I software degli applicativi delle centrali sono su server in remoto telecom.

A fronte di un evento catastrofico, pertanto, i dati saranno tutelati. Per riattivare il sistema si dovrà procedere all'approvvigionamento dei server e di tutto quanto necessario

per ripristinare il corretto funzionamento delle diverse applicazioni presso la sede della Casa di cure.

6.2.7. Piano di ripristino e procedure manuali

Il "*Piano di ripristino*", contenente nel dettaglio i tempi necessari al ripristino e le procedure da applicare fino al ripristino parziale o totale, risiede sul sistema informativo.
Per la registrazione manuale dei dati durante il mancato funzionamento del Sistema Informativo si utilizzeranno documenti cartacei che riproducono il format dei moduli nei quali sono articolate le cartelle cliniche, ambulatoriali ed infermieristiche; tali documenti sono disponibili presso tutte le postazioni di lavoro.
Ogni operatore terrà in evidenza tutti i documenti cartacei utilizzati per procedere alla trascrizione dei relativi dati sul Sistema Informativo quando questo sia ripristinato.

6.2.8. Documentazione sanitaria, certificazioni e notificazioni

Le informazioni riportate sulla documentazione sanitaria ed oggetto di certificazione e di notificazione, una volta inserite a sistema, non sono modificabili. L'organizzazione dei profili operatore e le regole di sistema debbono garantire l'impossibilità di alterare il dato inserito da altri ed anche dallo stesso operatore. Non sono possibili cancellazioni o correzioni di dati già inseriti.
L'operatore incaricato di elaborare e trasmettere agli Enti Pubblici registrazioni circa le operazioni della SISIFO è responsabile della corrispondenza al vero di quanto contenuto nella notifica.

6.2.9. Network Management

L'attività di network management si prefigge di stabilizzare, mantenere ed evolvere l'infrastruttura di rete, avendo cura di effettuare le scelte di volta in volta più appropriate per la selezione degli apparati di comunicazione e dei protocolli di rete con il preciso scopo di garantire la velocità di trasmissione, la stabilità delle connessioni e la sicurezza della rete.
Tale attività viene svolta da ditta esterna con il supporto dell'addetto al sistema informativo aziendale.

6.2.10. Attività di manutenzione del Software applicativo

Tutte le informazioni relative ai malfunzionamenti del software applicativo (BUG delle applicazioni) sono comunicate all'addetto al sistema informativo aziendale che provvede a predisporre gli opportuni interventi della consulenza esterna.

6.2.11. Attività di mantenimento degli archivi

Sono condotte a cura dell'addetto al sistema informativo aziendale che provvede a:

a) Verificare giornalmente le copie di sicurezza.
b) Pianificare e manutenere i salvataggi degli archivi presenti nelle diverse postazioni di lavoro. (Backup centralizzato se la postazione è in rete o demandato all'utente con supporti per il backup in locale ove necessario);
c) Verificare giornalmente le attività automatiche di riorganizzazione ed ottimizzazione dei dati;
d) Raccogliere eventuali report prodotti in automatico dalle procedure di backup e di riorganizzazione relativi alle anomalie riscontrate;
e) Risolvere, ove possibile, eventuali anomalie o inoltrare le richieste eventuali al fornitore o al produttore;
f) Archiviare periodicamente una copia degli archivi per assicurare il ripristino, almeno parziale, dei dati in caso di disastri causati da incendi, furti o altre cause naturali, accidentali o diverse.

6.2.12. Altre attività

Verifica degli spazi sui dischi dei server e delle postazioni di lavoro.

Il Presidente del Consorzio Sisifo
Avv. Giuseppe Piccolo

SISIFO CONSORZIO DI COOPERATIVE SOCIALI ARL
P.IVA 04799350824