PARTE SPECIALE N. 2

“REATI INFORMATICI”

1. Finalità

La presente Parte Speciale contiene, per ciascuna attività sensibile, i protocolli richiesti dall'art. 6 comma 2 lett. b) del D.Lgs. 231/2001.
Tutti i destinatari della Parte Speciale sono tenuti ad adottare comportamenti conformi a quanto di seguito formulato, al fine di prevenire la commissione dei reati in essa considerati.
Nello specifico, la presente Parte Speciale ha lo scopo di:

- indicare le regole di condotta che i destinatari sono chiamati ad osservare nelle attività sensibili individuate;
- indicare all'OdV e ai responsabili delle altre funzioni dell'Ente che cooperano con esso le aree sulle quali esercitare le attività di controllo, monitoraggio e verifica.

In particolare, sono qui previsti e disciplinati standard di controllo generali, applicabili a tutti i processi, e specifici, cioè applicabili alle singole attività sensibili.
Per le violazioni dei protocolli si applica il sistema disciplinare e sanzionatorio previsto nel Cap. 7 della Parte Generale.
La Fondazione ottempera alle previsioni della NIS2 (D.Lgs. 138/2024), con le relative disposizioni dell'Agenzia Cybersicurezza Nazionale (ACN).

2. I reati presupposto

Per il dettaglio dei reati presupposto previsti dall'art. 24 bis D.Lgs 231/2001 si richiama l'***Allegato 2*** del Modello Organizzativo di Gestione e Controllo (Catalogo dei reati presupposto ai sensi del D.Lgs. 231/2001).

3. Attività sensibili

L'analisi dei processi dell'Ente svolta nel corso dei lavori di predisposizione del presente Modello ha consentito di individuare le seguenti attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato sopra richiamate:

RI.1 *Gestione di software e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a Pubbliche Amministrazioni, Enti Pubblici o Autorità – tutela del dato ai fini Privacy*

Si tratta dell'attività inerente la gestione degli accessi alle risorse informatiche da parte degli utenti della Fondazione tale da garantire la protezione e il monitoraggio delle postazioni di lavoro ed il corretto utilizzo delle risorse, della posta elettronica e della sicurezza informatica, con particolare riguardo alla gestione di documenti elettronici sanitari o amministrativi.

Il processo riguarda, più in particolare, la trasmissione dei flussi informativi alla competente ATS per territorio: detti flussi riguardante le SDO (parte riabilitativa) i RIA (parte ambulatoriale e i SOSIA) nonché la piattaforma per la gestione della lista d'attesa.

RI.2 *Utilizzo delle dotazioni informatiche aziendali*

In tale ambito rientrano tutte le attività operative compiute con l'ausilio di apparecchiature informatiche e/o sistemi informatici dai dipendenti della Fondazione Vismara-De Petri ONLUS.

4. Il sistema dei controlli

Il sistema dei controlli perfezionato dalla Fondazione Vismara-De Petri ONLUS prevede:

i) con riferimento alle attività sensibili individuate:
   - principi di controllo "generali" presenti in tutte le attività sensibili;
   - principi di controllo "specifici" applicati alle singole attività sensibili;

ii) con riferimento ai soggetti coinvolti:
   - norme di comportamento e principi di controllo strumentali all'osservanza di tali norme.

4.1. Principi di controllo generali

Di seguito sono indicati i principi di controllo di carattere generale che è opportuno considerare ed applicare con riferimento alle attività sensibili individuate:

- **Segregazione delle attività**: separazione delle attività in modo tale che nessuno possa gestire in autonomia l'intero svolgimento di un processo.
- **Norme/Circolari**: disposizioni interne e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante.
- **Poteri autorizzativi e di firma**: poteri coerenti con le responsabilità organizzative e gestionali assegnate (con indicazione, ove richiesto, delle soglie di approvazione delle spese) e chiaramente definiti e conosciuti all'interno della Fondazione Vismara-De Petri ONLUS.
- **Tracciabilità**: verificabilità *ex post* del processo di decisione, autorizzazione e svolgimento dell'attività sensibile, anche tramite

appositi supporti documentali e, in ogni caso, dettagliata disciplina della possibilità di cancellare o distruggere le registrazioni effettuate.

4.2 Norme di comportamento generali e principi di controllo strumentali all'osservanza delle stesse

Ai sensi del Regolamento UE 679/2016, la Fondazione ha adottato il Registro dei trattamenti ai sensi dell'art. 30 del predetto Regolamento UE 679/2016, con il quale vengono definite le modalità per il trattamento dei dati personali, anche particolari, attraverso strumenti elettronici. Il documento contiene:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di

nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare.

4.3 Principi di controllo specifici

Di seguito sono elencati gli ulteriori principi di controllo individuati per ciascuna attività sensibile rilevata.

RI.1 Gestione di software e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a Pubbliche Amministrazioni, Enti Pubblici o Autorità – tutela del dato ai fini Privacy

- ***Regolamentazione***: è adottato e mantenuto il Registro che definisce le modalità di protezione delle informazioni detenute dalla Fondazione e di diffusione delle stesse, a terzi autorizzati, mediante strumenti elettronici.
Titolare del trattamento dei dati è la Fondazione Vismara-De Petri ONLUS la quale ha disegnato il Direttore Generale, Responsabile del Trattamento, e il Responsabile CED-ITC e la Società informatica di consulenza esterna quali Amministratore di Sistema e Responsabile esterno del trattamento.

L'Amministratore di Sistema gestisce e mantiene le connessioni di rete aziendali, garantendone la funzionalità e la sicurezza, specie nei contesti nei quali queste siano interfacciate con altre reti pubbliche o private.
Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione

cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.

L'Incaricato del trattamento dei dati personali presta particolare attenzione all'esattezza dei dati trattati e, qualora inesatti o incompleti, provvede ad aggiornarli tempestivamente.

Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, sono tenuti a conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo. La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

L'Incaricato del trattamento dei dati personali modifica la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.

Gli incaricati del trattamento hanno l'obbligo di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Con specifico riferimento, invece, al trasferimento dei dati amministrativi e sanitari all'ATS Val Padana è stata individuata la seguente procedura:

- la Fondazione ha individuato nel Presidente, Vicepresidente (in assenza o per impedimento del Presidente), Direttore Generale, Vice Direttore Generale e Direttore Sanitario, i referenti per i rapporti con l'ATS Val Padana;

- ad ogni paziente è associato un codice di riferimento;

- i medici e il personale incaricato caricano sul sistema informatico la cartella clinica con il Fascicolo Sanitario e Socio-Assistenziale (FASAS) di ogni singolo paziente;

- il Direttore Sanitario e i medici dirigenti controllano la correttezza dei dati socio-sanitari;

- La Fondazione ha individuato in due dipendenti (Ufficio URP) i soggetti responsabili della trasmissione dei dati amministrativi all'ATS Val Padana (ad esempio, documentazione rilevante per la fatturazione);
- il Responsabile Ufficio Ragioneria prima dell'invio, verifica la correttezza dei dati trasmessi dai soggetti incaricati.

- ***Deleghe****:* con riferimento alle attività di gestione e trasferimento di dati sensibili, esiste un sistema di ripartizione dei poteri e delle funzioni che garantisce l'identificazione dei soggetti responsabili e dei relativi compiti.

- ***Tracciabilità***: il sistema informatico adottato garantisce la conservazione e l'archiviazione, da parte di ciascuna funzione coinvolta, di tutta la documentazione rilevante, al fine di garantire la tracciabilità dei singoli passaggi.

Ogni Incaricato del trattamento dei dati personali presta particolare attenzione a tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.

RI.2 Utilizzo delle dotazioni informatiche aziendali

Politiche di sicurezza

La Fondazione ha adottato il Codice Etico ove sono poste le regole comportamentali cui i dipendenti della Fondazione e tutti coloro che

contribuiscono allo svolgimento delle attività aziendali devono uniformarsi. Tale Codice prevede che tutti gli utenti interni e quelli esterni autorizzati all'uso delle apparecchiature e dei sistemi informatici della Fondazione debbano servirsi delle risorse informatiche aziendali nel rispetto delle disposizioni normative vigenti: sono espressi il divieto di intrusione, accesso abusivo al sistema informatico e di danneggiamento di sistemi informatici altrui.

È inoltre affermato l'obbligo per tutti gli utenti di tutelare l'integrità delle apparecchiature e dei sistemi informatici interni, astenendosi da manipolazioni che ne possano modificare in qualsiasi modo le funzionalità. Il Codice Etico è trasmesso in copia elettronica a tutti i dipendenti.

Il documento viene aggiornato dal Consiglio di Amministrazione della Fondazione.

La Fondazione ha inoltre adottato un apposito Regolamento sui sistemi informatici, nominando il Responsabile CED-ICT e la Società di consulenza esterna informatica come Amministratore di sistema e Responsabile esterno del trattamento.

Organizzazione della sicurezza per gli utenti interni

I profili utente dei dipendenti sono *standard* e prevedono le stesse abilitazioni: il profilo utente di ogni dipendente permette l'accesso alle risorse informatiche ed alla rete attraverso connessione protetta ed autenticazione personale.

Ogni profilo utente è utilizzato previo inserimento di credenziali univoche ed individuali *(password*). Ciascun dipendente può accedere solo alla propria area di competenza per adempiere ai compiti assegnati.

Le credenziali di autenticazione non utilizzate da più di tre mesi sono disattivate, salvo il rilascio di apposite autorizzazione per le sole esigenze di gestione tecnica.

Linee guida comportamentali e regole operative sono definite anche riguardo al corretto uso delle apparecchiature informatiche ed alla protezione delle singole postazioni di lavoro (es. *screensaver* con *password*, spegnimento del *computer* in casi di allontanamento prolungato dal posto di lavoro, …).

Organizzazione della sicurezza per gli utenti esterni

La Fondazione non ha attivato profili per utenti esterni, eccezion fatta per l'Organismo di Vigilanza; l'accesso di eventuali utenti esterni ai sistemi aziendali è espressamente autorizzato dalla Fondazione.

Classificazione e controllo dei beni

Gli *assets* informatici della Fondazione risultano tracciati.

I controlli sullo stato di attivazione delle licenze *software* e sui relativi contratti e licenze d'uso sono eseguiti dalla Società di consulenza esterna informatica.

La Fondazione ha identificato i dati personali trattati, le relative operazioni di trattamento, nonché gli strumenti elettronici utilizzati per l'elaborazione degli stessi.

I dati sottoposti a trattamenti manuali presenti su supporti non informatici sono raccolti in appositi archivi ad accesso selezionato, di cui è responsabile il dipendente incaricato della gestione dei dati.

I documenti aziendali sono sottoposti a registrazione ed a classificazione e sono memorizzati in maniera tracciabile, al fine di garantirne l'autenticità e l'affidabilità.

La Fondazione ha definito la struttura organizzativa dei soggetti con attribuzioni ai sensi del Regolamento UE 679/2016. Il Vice Direttore Generale è stato individuato "Responsabile del trattamento".

Sicurezza fisica e ambientale

La protezione fisica delle attrezzature informatiche in dotazione è garantita dalle misure di sicurezza adottate nei locali degli uffici.

Gestione delle comunicazioni e dell'operatività

All'interno dei documenti aziendali relativi al settore informatico sono analizzati i rischi di distruzione e di perdita di dati, nonché i rischi di accessi non autorizzati ed i rischi di natura logica e fisica; in corrispondenza di ogni rischio la Fondazione ha identificato le misure di protezione relative.

La Fondazione si avvale delle procedure di salvataggio automatizzato e conservato sul server, effettuato tramite sistemi di gestione che periodicamente effettuano una copia dei dati presenti sul server della sede e ne effettuano una copia sul cloud.

La protezione da *software* pericoloso è attuata attraverso il *firewall*, appositi *software antivirus* e *antispam.*

La Fondazione ha formalizzato nel Regolamento sui sistemi informatici il divieto per tutto il personale di utilizzare *software* di qualsiasi tipo distribuiti gratuitamente (*freeware*) o in prova (*shareware*); inoltre nessun profilo utente dei dipendenti ha le abilitazioni necessarie per l'installazione di prodotti *software*.

L'installazione e l'attivazione delle licenze *software* sono monitorate dal Responsabile CED-ICT, che monitora le rispettive scadenze.

La Fondazione si avvale dell'installazione di appositi *software antivirus* e *antispam*, aggiornati costantemente ed attivati su tutti i *firewall*, *mail* di posta, *intranet server* e sui *desktop* dei *pc*.

Controllo degli accessi

In caso di risoluzione del rapporto di lavoro di un dipendente con la Fondazione, la stessa dispone la disabilitazione del profilo utente.

Gestione degli incidenti e dei problemi di sicurezza informatica

Sono analizzati dalla Società di consulenza esterna informatica i rischi di distruzione e di alterazione dei dati ed i rischi di eventi incidentali ai danni dei sistemi informatici aziendali; in corrispondenza di ogni rischio viene riportato l'elenco delle contromisure adottate e relative sia a procedure aziendali sia a strumenti informatici.

Malfunzionamenti o anomalie sul funzionamento dei sistemi e delle apparecchiature informatiche (ad es. *server,* rete, singoli *software,…*) sono gestiti dall'Amministratore di Sistema.

Audit

La verifica circa l'efficacia e l'efficienza della gestione della sicurezza informatica è affidata all'Amministratore di Sistema che annualmente deve effettuare una Relazione al CdA.

Risorse umane e sicurezza

La Fondazione ha comunicato a tutti dipendenti il contenuto del Codice Etico.

In caso di risoluzione del rapporto di lavoro di un dipendente, quest'ultimo ha l'obbligo di restituire tutte le apparecchiature ricevute.

Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi informativi

Tutti i materiali tecnologici, sia *hardware* che *software,* sono acquistati da lla Fondazione mediante Amministratore di Sistema da fornitori sottoposti a processo di selezione e qualifica e sono previamente valutati anche dal punto di vista della sicurezza delle informazioni.

Sono installati solo *software* con apposita licenza d'uso ed è vietato l'utilizzo di *software* per i quali la Fondazione non abbia provveduto ad acquistare l'apposita licenza: in particolare, la Fondazione ha formalizzato il divieto di duplicare, installare e/o detenere programmi ed ogni altro prodotto *software* senza esplicita autorizzazione e il divieto di utilizzare prodotti *software* per

eseguire attività connesse a finalità personali dalle quali derivi direttamente o indirettamente un lucro per il lavoratore o un danno per la Fondazione.

Il *download* di software può essere effettuato solo per scopi professionali.

Gli interventi di manutenzione correttiva ed evolutiva sulla rete *intranet* e sui sistemi di rete sono eseguiti dall'Amministratore di Sistema.

Le evoluzioni o personalizzazioni dei *software* installati sono gestite dal Responsabile CED-ICT.

Tutti i *software* e *file* scaricati legittimamente da *internet* o provenienti da fonti esterne alla Fondazione sono controllati mediante *software* specifico di rilevazione *virus* prima che il *file o software* abbia contatto con altri programmi.

Tutte le componenti *hardware* sono registrate.

L'uso di risorse è monitorato e regolato dall'Amministratore di Sistema, al quale spetta il compito di controllare i cambiamenti apportati ai sistemi ed alle strutture di elaborazione delle informazioni.

5. Flussi informativi verso l'Organismo di Vigilanza

Oltre agli obblighi informativi verso l'O.d.V. richiamati nella Parte Generale, saranno definiti specifici flussi di reporting di dati e/o informazioni relativi ai processi sensibili e strumentali individuati nella presente Parte Speciale, secondo le indicazioni del documento denominato "Flussi di reporting delle unità organizzative verso l'Organismo di Vigilanza per attività sensibile"

Su base annuale, l'Amministratore di Sistema formalizza all'OdV apposita relazione scritta sullo stato dei sistemi informatici e dei sistemi informativi secondo i seguenti items:

1- Stato dei sistemi informatici e informativi dell'Ente.

2- Eventuali elementi di vulnerabilità.

3- Stato del sistema di protezione da virus e attacchi informatici.

4- Previsione della business continuity plan.

5- Previsione del disaster recovery plan.

6- Sistema di log di sistema.

7- Sistema di backup dei dati aziendali.

8- Sistema di criptazione e cifratura per la tutela dei dati particolari e giudiziari.

9- Eventuali audit o penetration test effettuati.

10- Stato del server della Fondazione.

11- Manuale della conservazione digitale e Responsabile della conservazione digitale.

12- Stato del sistema rispetto standard relativi ai sistemi informatici e informativi.