POLICY DI SICUREZZA DEL DATO

1. Introduzione

Le misure di sicurezza atte a garantire la riservatezza, integrità e disponibilità dei dati e la resilienza dei sistemi informativi (analogici e digitali) sono costituite da prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati. A seguito di analisi dei trattamenti e di valutazione del rischio ad essi connessi, previste dagli art. 32 del GDPR, tali misure tecnico-organizzative sono volte a ridurre al minimo i rischi di:

- Distruzione o perdita, anche accidentale, dei dati;
- Accesso non autorizzato;
- Trattamento non consentito o non conforme alle finalità della raccolta;
- Modifica dei dati in conseguenza di interventi non autorizzati o non conformi alle regole previste.

La sicurezza del dato è divisa in tre ambiti principali: sicurezza fisica, sicurezza della rete e sicurezza di sistema.
Per sicurezza fisica si intende l'accesso e la protezione fisica di strutture rilevanti per la conservazione dei dati e il sicuro mantenimento di hardware e software.
La sicurezza della rete tratta la protezione dei sistemi, in particolare quelli che sono esposti in internet e quindi al rischio di attacchi hacker (implementazione di firewall di rete e DMZ).
La sicurezza dei sistemi assicura l'adeguata gestione dei computer a livello di utente:

- Gestione delle password (quanto devono essere lunghe e quanto spesso devono essere cambiate);
- Implementazione di procedure di controllo adeguate degli accessi;
- Implementazione di procedure di crittazione adeguate;
- Monitoraggio e filtraggio di dati trasmetti (dati personali filtrati o solo trasferimento di dati crittati);
- Distruzione dei dati in maniera sicura e controllata;
- Trattamento sicuro dei dati, compreso il tracciamento delle modifiche apportate.

2. Ambito di interesse/applicazione

Tale policy si applica alla conservazione e alla sicurezza dei dati raccolti in tutte le Unità Operative/articolazioni organizzative dell'Istituto Neurologico "Carlo Besta".

3. Standard id sicurezza del dato

Nel rispetto dei principi dell'art. 5 del GDPR, l'Istituto Neurologico "Carlo Besta" utilizza per la raccolta e la conservazione del dato due piattaforme, REDCap e XNAT, le quali garantiscono:

- Inserimento dei dati e metadati clinici e dati di neuroimaging quali risonanza magnetica e tomografia computerizzata;
- Creazione di survey o database online con accesso sicuro e autenticato;
- Accesso alle due piattaforme concesso a diversi ricercatori da istituzioni differenti previa autorizzazione, e/o convenzione con terzi, e/o Reti di Ricerca;
- Funzionalità di controllo per tracciare la manipolazione dei dati e l'attività degli utenti;
- Gestione e customizzazione avanzata degli utenti;
- Autenticazione degli utenti tramite password personali e complesse (sarà obbligatorio cambiarla dopo tre mesi);
- Scadenza della sessione dopo 15 minuti di inattività.

Inoltre, verranno adottate ulteriori misure di sicurezza:

- I dati personali o confidenziali saranno crittati;
- I server saranno protetti da firewall per prevenire accessi non autorizzati;
- Backup giornalieri;
- Il database sarà accessibile solo attraverso VPN LAN-to-LAN, per le attività amministrative degli utenti abilitati a questa attività;
- L'accesso applicativo sarà garantito tramite connettività sicura, mediante l'utilizzo di certificati ssl, rilasciati dall'Ente certificatore SECTIGO, come servizio offerto dalla comunità GARR del quale l'Istituto fa parte;
- L'accesso applicativo avverrà mediante esposizione della URL attraverso DMZ e Firewall;
- L'accesso all'applicativo avverrà mediante registrazione e profilazione utente la cui responsabilità è demandata al Responsabile di progetto (Principal Investigator);
- La raccolta dei dati avverrà in maniera anonimizzata o pseudo-anonimizzata;
- Solo il personale autorizzato potrà accedere ai dati;
- Il paziente può richiedere la cancellazione dei propri dati al Responsabile di progetto (Principal investigator);
- Il paziente può richiedere una copia dei suoi dati al Responsabile di progetto (Principal investigator).

Il trattamento dei dati personali sarà effettuato sia in formato automatizzato che manuale, nel rispetto delle misure adeguate di sicurezza sopra descritte e dei principi di liceità, limitazione delle finalità e minimizzazione. Tali criteri ridurranno al necessario l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possano essere realizzate mediante l'utilizzo di dati anonimi, mediante modalità che consentano di identificare l'interessato solo in caso di necessità (pseudo-anonimizzazione).
In ottemperanza a quanto previsto dagli art. 28 e 29 del GDPR, soltanto i soggetti appositamente autorizzati al trattamento sono tenuti a trattare i dati essenziali per svolgere l'attività istituzionale. Si rinvia a quanto specificatamente descritto nella policy della condivisione dati prevista dall' Istituto Neurologico "Carlo Besta".

4. Principali rischi associati alla sicurezza del dato

In linea con le norme del GDPR, ogni progetto di ricerca considera i principi di minimizzazione del trattamento e di limitazione dell'uso dei dati personali.
Dato che tutte le misure di sicurezza descritte nella sezione precedente sono rispettate, riteniamo che i rischi associati all'uso del sistema da parte di persone designate siano ridotti al minimo. In particolare, il sistema di raccolta dati è verificabile nella sua completezza, garantendone la tracciabilità in ogni fase del progetto.
L'attuazione del progetto di ricerca richiede che ogni partner operi secondo i principi della privacy in forza all' art. 25 comma 1 del GDPR, in particolare considerando: lo stato dell'arte e i costi di implementazione; la natura, lo scopo, il contesto e gli obiettivi del trattamento; le probabilità e le diverse severità associate ai rischi; i diritti e le libertà dei soggetti posti dal trattamento stesso. In questo senso, il principio di privacy stabilisce l'obbligo di adottare adeguate misure di sicurezza per la protezione dei dati personali dei soggetti.
Le misure adottate per garantire un livello di sicurezza per il singolo rischio possono essere identificate come organizzative e tecniche. Tali misure assicurano che solo il dato personale necessario per il perseguimento di ogni specifico obiettivo venga utilizzato, con particolare attenzione all'ammontare di dati personali raccolti, l'estensione del loro trattamento, il periodo di conservazione e la loro accessibilità. Inoltre, viene garantito che i dati personali saranno resi accessibili solo a persone autorizzate e che tutti i partecipanti si impegnano collettivamente a perseguire tali misure per garantire un'adeguata protezione dei dati nel progetto di ricerca.
Al fine di rispettare la protezione dei dati e di tutelare i diritti e le libertà fondamentali degli interessati, è necessario verificare che il titolare del trattamento dei dati stessi abbia il consenso informato da parte del paziente. Il consenso informato, in base all'art. 4 del GDPR, è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano. I documenti del consenso e i fogli informativi saranno adattati secondo le leggi e le linee guida nazionali. In particolare, questi sono stati preparati in modo da descrivere con un linguaggio semplice e comprensibile: la natura dello studio, i suoi obiettivi, le procedure coinvolte, la durata prevista, i rischi e i benefici potenziali a ogni possibile disagio che possano implicare. Ogni partecipante verrà informato che l'adesione allo

studio è volontaria, che lui/lei potrà recedere dallo studio in ogni momento e che questo non influenzerà in alcun modo la sua condizione.