GESTIONE APPARECCHIATURE BIOMEDICHE

Procedura GDPR

Autore/i: DPO/Supporto Specialistico
Rivisto da U.O.C. Privacy – Trasparenza e Integrità
Accettato da: U.O.C. Ingegneria Clinica -HTA

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1		Prima versione	DPO
L'ultima revisione sostituisce qualsiasi revisione precedente.			

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi – Cotugno – CTO

A.O.R.N.
"AZIENDA OSPEDALIERA DEI COLLI"
Monaldi – Cotugno - CTO
Via L. Bianchi s.n.c. - 80131- Napoli
C.F/P.I 06798201213

PROCEDURA PER LA GESTIONE DELLE APPARECCHIATURE BIOMEDICHE

Sommario

PREMESSA

Il Regolamento UE 2016/679 del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, di seguito GDPR, in vigore dal 24 maggio 2016 e applicabile dal 25 maggio 2018, impone in capo al Titolare la responsabilità di mettere in atto misure tecniche, organizzative e legali adeguate a garantire ed essere in grado di dimostrare la conformità al GDPR (art. 32 Regolamento UE 679/2016). Pertanto, in ottica di accountability, il Titolare del trattamento deve monitorare ed aggiornare i sistemi di gestione e gli strumenti informatici in uso rendendoli conformi al Regolamento UE 2016/679. In particolar modo è necessario condurre un'attenta gestione e valutazione del rischio correlato al trattamento di dati personali, come richiesto anche dalla "Valutazione di impatto sulla protezione dei dati" (art. 35 Regolamento UE 679/2016), al fine di raggiungere un livello di rischio residuo "Limitato" per il trattamento dei dati degli interessati. La valutazione dei rischi deve identificare i diversi "scenari di rischio (perdita di riservatezza, perdita di integrità e perdita di disponibilità)" e, per ognuno di essi, stimare il "livello di rischio effettivo" per i diritti e le libertà dell'interessato connesso al trattamento in esame con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

In tali scenari i servizi legati all'utilizzo delle apparecchiature biomediche, per ambito di applicazione e per contesto di erogazione, rappresentano implicitamente sensibili criticità in merito alla tutela e sicurezza dei dati personali specialmente per quanto concerne l'aspetto della riservatezza, con diretto impatto anche sulla sicurezza ed integrità del dato clinico e sanitario.

Per apparecchiature biomediche si intendono:

- apparecchi elettromedicali ai sensi della norma tecnica CEI EN 60601-1
- apparecchi elettrici di misura e da laboratorio ai sensi della norma tecnica CEI EN 61010-1
- apparecchi elettrici per pulizia, lavaggio, disinfezione e sterilizzazione di Dispositivi Medici
- Dispositivi Medici attivi (ad esclusione di DM monouso o poliuso con un numero limitato di utilizzi)
- apparecchi elettrici che non rientrino nelle definizioni precedenti ma connessi alle attività sanitarie (es. frigoriferi biologici, maceratori, ecc.)

Lo scenario relativo alle apparecchiature biomediche presenta infatti alcune criticità che ne impongono una gestione diversa da quella dei sistemi informatici di uso comune: sebbene molte apparecchiature possano essere ricondotte ad elementi comuni quali il sistema operativo e l'ambiente applicativo, bisogna ricordare che la certificazione ai sensi della Direttiva Europea 93/42/CEE prima e del Regolamento Europeo 2017/745/UE oggi, obbliga il fabbricante a congelare di fatto il software alla situazione presente al momento della certificazione non permettendo in alcuni casi sia l'aggiornamento del sistema operativo, sia l'installazione di software di protezione, che se non testati preventivamente dal fabbricante, potrebbero causare una modifica del dispositivo e quindi la perdita della responsabilità del fabbricante sul funzionamento del dispositivo (modifica del Dispositivo Medico, che necessiterebbe di una nuova certificazione).

Questa situazione espone a rischi elevati le apparecchiature biomediche che necessitano di essere collegate alle reti informatiche, e in particolare:

- *riservatezza furto di identità*: raccolta e diffusione non autorizzata di dati personali (immagini, documenti, carta di identità, numero di previdenza, patente di guida…);
- *attacchi cyber-fisici*: attacchi che causano più o meno volontariamente malfunzionamenti delle apparecchiature e degli impianti, che nel caso delle apparecchiature biomediche possono avere conseguenze anche gravi sulla integrità e disponibilità dei dati.

Altra criticità riguarda le apparecchiature utilizzate in contesti di emergenza (Terapia Intensiva, Sala Operatoria, Pronto Soccorso, ecc.) per cui è difficile immaginare che l'accesso all'apparecchiatura possa essere protetta da credenziali di accesso, in quanto il fattore tempo potrebbe essere determinante.

L'Azienda dei Colli, pertanto, per il principio di accountability su richiamato e soprattutto nel rispetto dei diritti e dei bisogni dei cittadini, tra cui quelli della riservatezza e tutela dei propri dati che, per il principio della sussidiarietà e della responsabilizzazione sociale, devono essere costantemente al centro delle decisioni aziendali, deve effettuare un accurato e dettagliato adeguamento di tutte le misure tecniche ed organizzative associate alla gestione e utilizzo degli asset biomedici, in modo da garantire il richiesto livello di rischio residuo "Limitato" per l'esecuzione dei trattamenti interessati.

Questo documento espone, appunto, le linee guida adottate dall'azienda affinché possa essere assicurato quanto sopra indicato.

CAPITOLO 1
INVENTARIO APPARECCHIUATURE BIOMEDICHE

CAP. 1

Preso atto che esiste già attualmente un inventario completo di tutte le apparecchiature biomediche aziendali, occorre arricchire tale inventario con informazioni, attualmente non presenti, utili alla classificazione del rischio in termini di protezione dei dati personali.

Dovranno quindi necessariamente essere inserite nell'inventario le seguenti informazioni:

- se l'apparecchiatura conserva o tratta dati personali;
- se l'apparecchiatura è dotata di workstation integrata o separata;
- se l'apparecchiatura ha la possibilità e/o la necessità di essere collegata alla rete informatica aziendale;
- se l'apparecchiatura dovrà essere collegata alla rete internet a fronte di necessità di interventi di manutenzione o monitoraggio da remoto di dati.

Di conseguenza si dovrà evidenziare il livello di rischio in riferimento al trattamento dei dati personale e la necessità o meno della nomina ex art. 28 GDPR, disponendo dei dati relativi all'effettiva avvenuta nomina e al riferimento, nel caso in cui la nomina sia necessaria.

CAP. 2

CAPITOLO 2
ACCESSO ALLE APPARECCHIUATURE BIOMEDICHE

a) L'accesso alle apparecchiature biomediche che conservano e/o trattano dati personali, secondo le norme adottate dalla struttura sanitaria in adempimento agli indirizzamenti

normativi definiti dal Regolamento UE 679/2016 per la regolamentazione dell'accesso alle risorse informatiche, **dovrebbe avvenire esclusivamente attraverso adeguate e conformi credenziali di accesso**.

Nella fattispecie le credenziali di accesso sono costituite da:

- UserId (identificativo utente);
- Password (parola chiave).

b) Le credenziali di autenticazione dovrebbero essere univoche e non possono essere assegnate a soggetti diversi neppure in tempi successivi. Le credenziali assegnate a ciascun utente per l'accesso alle risorse informatiche, nel nostro caso alle apparecchiature biomediche, devono essere di uso strettamente personale e pertanto l'assegnatario è tenuto a custodirle con diligenza e in modo appropriato, al fine di contenere i rischi di accessi non autorizzati, furti, frodi, danneggiamenti derivanti dalla diffusione e/o utilizzo improprio delle stesse. In particolari contesti come quelli di emergenza, nei quali l'utilizzo di password personali potrebbe rappresentare un ostacolo all'utilizzo rapido dell'apparecchiatura causando un rischio di natura diverso, come una mancata erogazione della prestazione sanitaria, potranno essere valutate soluzioni alternative, come l'utilizzo di una credenziale di accesso comune, cercando però di introdurre ulteriori misure, come ad esempio un cambio più frequente della password, l'attivazione di funzioni di stand-by per i momenti di inattività delle stesse e la limitazione alle funzioni essenziali per l'esecuzione della prestazione per questo account comune. Inoltre dovranno essere impiegate misure fisiche ed organizzative più elevate per il controllo dell'accesso ai locali delle apparecchiature tali da consentirne l'utilizzo solo al personale autorizzato.

c) Gli utenti hanno diritto di accesso limitato alle risorse informatiche per le quali sono stati espressamente autorizzati, e per gli utilizzi strettamente correlati con le mansioni assegnate (profili autorizzativi).

d) Le credenziali di accesso di tipo amministrativo, tra cui quelle standard dei fornitori/produttori, devono essere acquisite dai responsabili delle UOC/UOSD dove sono installate le apparecchiature i quali, in quanto Delegati al trattamento dati, assumono l'incarico di "Custode delle credenziali di autenticazione" e pertanto sono tenuti a custodirle con estrema sicurezza e diligenza conservandole in busta chiusa sigillata e controfirmata sui lembi. Ovviamente tali credenziali di tipo amministrativo non dovranno essere utilizzate per accedere alle apparecchiature per lo svolgimento delle ordinarie attività lavorative ma semplicemente per attività straordinarie quali quelle di manutenzione o di eventuali attività di tipo sistemistico.

Nel caso in cui siano attivate apposite credenziali utente per lo svolgimento di attività di collaudo, queste dovranno essere rimosse alla fine di tali attività e prima del rilascio in esercizio delle apparecchiature.

2.1 USERID POLICY

La componente UserId delle credenziali di accesso dovrebbe essere univoca e dovrebbe essere sempre associata ad una sola persona fisica, ad eccezione dei contesti emergenziali, come già detto.

Nel momento in cui l'utente non ha più diritto/necessità di accedere ad una specifica apparecchiatura, lo userId deve essere sospeso e non cancellato, al fine di consentire indagini future e/o di non riassegnarla a persone diverse anche in momenti diversi.

2.2 PASSWORD POLICY

La componente password delle credenziali di accesso deve rispondere a specifici requisiti di robustezza e lunghezza e deve essere gestita e custodita con accurata diligenza e riservatezza. Di seguito vengono descritte le regole generali per la creazione e la gestione delle password per tutti gli utenti, a prescindere dagli eventuali ulteriori controlli e/o meccanismi specifici implementati in determinati contesti.

2.2.1 REGOLE PER LA CORRETTA GESTIONE DELLA PASSWORD

La lunghezza minima delle password è stabilita in otto caratteri, sono ovviamente esclusi da tale regola i sistemi che non gestiscano questa lunghezza, per i quali si applicherà la lunghezza massima consentita.
Le password devono essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.
Le password devono contenere almeno un carattere alfabetico maiuscolo ed un numero.
Inoltre,le password non devono:

- essere riconducibili ad un nome proprio di persona o derivante dalla userId (ad es. identico, inverso, con le lettere raddoppiate, ecc.) o comunque agevolmente riconducibile all'intestatario della userId (ad es. matricola, cognome, dati anagrafici, ufficio/funzione di appartenenza);
- essere composte di sole cifre o di una lettera o carattere ripetuto anche più volte o ancora digitata attraverso l'uso della sola barra spaziatrice;
- contenere riferimenti a dati personali (ad es. indirizzo, telefono, codice fiscale, numero della patente, ecc.) o comunque ad altre parole agevolmente riconducibili all'utente;
- poter essere lette sia nell'uno che nell'altro verso (ad es. parole o frasi palindrome: ad es. adda, ossesso, esse, ingegni, ecc.);
- sia uguale alle ultime tre utilizzate o uguale alla precedente tranne che per un carattere.

Qualora possibile, è auspicabile disporre di un sistema di controllo automatico circa la corretta composizione delle password tale da assicurare sicurezza e conformità delle stesse.

2.2.1.1 Generazione

La generazione della prima password, se possibile, deve essere automatica e gestita in concomitanza con l'attivazione dell'identificativo utente ad essa correlato, secondo le regole di cui al punto precedente dall'apposita funzione prevista dal sistema di gestione dell'apparecchiatura.
La prima password deve avere carattere provvisorio e non deve attivare alcuna operazione diversa da quelle relative alla sua modifica, da parte dell'utente a cui è stata assegnata, con una nuova password conforme alle regole prima esposte. Solo dopo aver modificato la prima password l'utente potrà accedere alle funzioni a lui associate.

2.2.1.2 Custodia

La password di accesso, relativa ad un determinato utente è strettamente personale e non può essere comunicata ad altri, anche se limitatamente a brevi periodi di utilizzo.
Le password devono essere accettate in forma mascherata e devono essere conservate all'interno del sistema, in formato non intelligibile, utilizzando algoritmi hash standard sufficientemente robusti per garantire la non reversibilità della codifica.
Non è inoltre consentito:

- comunicare la password (anche se scaduta) per telefono o altro mezzo a soggetti non autorizzati che si presentano come colleghi, tecnici, supervisori, autorità competenti, ecc.;
- digitare la password davanti ad altri (ad es. colleghi o estranei) anche se si tratta del personale di assistenza tecnica;
- trascrivere la password su dispositivi o supporti cartacei o elettronici (ad es. foglietti apposti sul personal computer, lasciati sulla scrivania o dentro ad un cassetto, file di testo lasciati sul desktop, ecc.). Qualora si rendesse indispensabile una trascrizione di back-up, questa dovrà essere custodita in apposito mezzo forte ad accesso limitato, ed il processo dovrà essere corredato da apposita procedura operativa che ne descriva il flusso di gestione, nonché le relative competenze e le responsabilità.

Infine, qualora si avesse anche solo il dubbio che la propria password sia venuta a conoscenza di altri è fatto obbligo al legittimo titolare di provvedere immediatamente a modificarla password e, nei casi più gravi, a segnalare la sospetta o accertata violazione alla funzione competente.

2.2.1.3 Validità

a) Il controllo della validità di una password, se possibile, deve essere gestito in modo automatico dal sistema che deve bloccare l'accesso alla risorsa alla scadenza della password. Il periodo massimo di validità della password per il trattamento di dati particolari, quali nel nostro caso, deve essere non superiore a tre mesi. Tuttavia, dato il particolare contesto operativo circa l'utilizzo di apparecchiature biomediche che difficilmente consente di utilizzare password univoche e nominative, si consiglia di ridurre quanto più possibile il periodo di validità della password al fine di garantire una maggiore tutela della riservatezza dei dati trattati. Trascorso il periodo di validità, il sistema deve attivare automaticamente la procedura di cambio password ovvero in assenza di tale funzionalità, deve esserne disposto il blocco forzato da parte dell'Amministratore fino al compimento delle operazioni di cambio password.
b) Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica (es. Utenze di Servizio e Utenze Amministrative), per le quali devono essere predisposte specifiche procedure operative.
c) Ogni qualvolta si ipotizza un rischio di accessi illeciti o di compromissione della password associata ad un determinato utente, e comunque ogni volta risulti necessario per garantire la sicurezza del sistema, occorre bloccare l'accesso all'apparecchiatura con quella utenza. Ovviamente solo una utenza amministrativa, dotata di specifici privilegi di accesso, può

disporre il blocco, ed eventualmente il successivo sblocco o blocco definitivo,di quella particolare utenza.

2.2.1.4 Modifica

La modifica di una password è consentita esclusivamente al titolare della stessa. Il titolare modifica la propria password previo inserimento del proprio identificativo utente e della vecchia password.
Nella sostituzione della password, non può essere riutilizzata alcuna delle ultime 3 password di cui si è fatto precedentemente uso.

CAPITOLO 3
PROFILI AUTORIZZATIVI

CAP. 3

Per Profilo Autorizzativo (o privilegio utente), si intende un insieme di regole, relativo ad un applicazione/servizio, che ne definiscono le modalità di utilizzo da parte degli Utenti. Queste regole possono essere espresse nell'insieme di risorse ed attributi (c.d ruoli applicativi - Amministratore, Utente, Operatore) che ne regolano l'accesso.
I profili autorizzativi devono essere:

- definiti sulla base delle specifiche applicazioni informatiche (es. sistemi, apparati di rete) che gli utenti devono utilizzare durante la normale attività lavorativa;
- in ragione del ruolo ricoperto e limitatamente alle mansioni svolte;
- configurati per limitare l'accesso ai soli dati necessari alle finalità dell'attività lavorativa (principi del "at least privilege" e "need to know");
- limitate nel tempo in ragione delle effettive necessità lavorative.

Il rilascio dei profili autorizzativi deve avvenire attraverso procedure formalizzate. Le procedure devono comprendere il rilascio delle autorizzazioni speciali per il personale tecnico-sistemistico, e di quelle eventualmente temporanee per il personale addetto alle assistenze/manutenzioni.

CAPITOLO4
TUTELA E PROTEZIONE DEI DATI

CAP. 4

Deve essere assicurata la costante disponibilità dei dati contenuti nei DB (memorie) delle apparecchiature biomediche mediante procedure di backup, trasferimento in cloud, etc. In alternativa, per le apparecchiature che non trasferiscono i dati sui DB/Cloud aziendali, prevedere adeguata custodia e protezione dei referti cartacei prodotti.
Assicurare la riservatezza dei dati per eventuale trasferimento verso altre apparecchiature o altri repository o per estrazione degli stessi (es.: preparazione convegni, preparazione articoli scientifici per riviste mediche, etc.) mediante appropriate procedure di cifratura/pseudonimizzazione.
Non potendo procedere per tutte le apparecchiature biomediche all'aggiornamento automatico del sistema operativo e all'aggiornamento automatico delle basi antivirus o di altri eventuali software interni di protezione, bisognerà verificare che le stesse siano periodicamente aggiornate almeno ogni qualvolta vengono comunicate dai fabbricanti eventuali patch di aggiornamento (attività di

hardening). Se tali attività sono demandate a fornitori esterni occorrerà assicurarsi che le manutenzioni periodiche effettuate comprendano anche questa attività.
Richiedere e raccogliere la eventuale documentazione relativa alle misure tecniche ed organizzative adottate dai produttori per le attività di manutenzione ordinaria e da remoto, nonché per attività di monitoraggio dei dati contenuti nelle apparecchiature biomediche attraverso collegamenti internet, se previsti. Nel caso di backup in cloud operati direttamente dai produttori conoscere se possibile la ubicazione dei server cloud.
Per le apparecchiature dismesse per fuori uso o per sostituzione procedere alla cancellazione dei dati in esse contenuti. (*Dettagliare modalità e tempi nella suddetta procedura anche se le operazioni sono demandate ai Fornitori/Produttori*).
Come dettagliato nel "Regolamento aziendale sull'utilizzo dei sistemi informatici", tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, dischi esterni, memorie a stato solido, ecc.), contenenti dati personali/particolari/giudiziari nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale dell'UOC SIA e seguire le istruzioni da questo impartite. È tassativamente vietato l'utilizzo di supporti rimovibili personali.
L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
L'eventuale utilizzo di supporti magnetici esterni (es. dischi rigidi USB, USB Pen Drive, SD (mini, micro e nano), unità CD/DVD-ROM USB ecc.) contenenti dati personali, particolari e giudiziari è possibile solo internamente all'Azienda e previa autorizzazione del Responsabile dell'UOC SIA e la loro custodia deve avvenire solo in armadi chiusi a chiave. Eventuali manomissioni nella custodia ed esposizione a possibili utilizzi dei supporti da parte di terzi devono considerarsi quali potenziali violazioni alla protezione e sicurezza dei dati (cd. data breach) che se riguardanti dati personali, particolari e giudiziari vanno notificati al Garante Protezione Dati Personali entro 72 ore dall'evento (art. 33 GDPR) ed eventualmente agli interessati (art. 34 GDPR).

CAPITOLO5
COLLAUDO

CAP. 5

Il collaudo è l'attività mediante la quale l'Azienda verifica la corretta esecuzione della fornitura dell'apparecchiatura elettromedicale. È composto da un collaudo amministrativo teso a verificare la correttezza di tutta la documentazione e da un collaudo tecnico mirato a controllare le condizioni di sicurezza e di perfetto funzionamento dell'apparecchiatura che potrebbero essere presenti a causa di un problema durante il trasporto o per un difetto di fabbricazione.
È il momento in cui si compila il verbale che permette dal punto di vista amministrativo di liquidare le spettanze e dal punto di vista tecnico di dare l'avvio all'utilizzo dell'apparecchiatura.
Tale attività risulta adeguatamente illustrata nella "Procedura di collaudo per le apparecchiature elettromedicali" che è stata arricchita di un'apposita sezione per la valutazione della conformità

all'art. 32 del Regolamento UE 679/2016. Tale sezione consente di raccogliere in modo sistematico tutte le informazioni necessarie alla corretta valutazione del rischio relativo alla protezione dei dati ed eventualmente rappresenta il contesto per predisporre, se richieste, ulteriori misure tecniche ed organizzative per la limitazione del rischio.
Il verbale di collaudo, oltre alle informazioni tecniche già attualmente contenute, dovrà quindi contenere:

- tipologia dei dati paziente trattati
- modalità di accesso ai dati
- modalità di connessione alla rete
- elenco di applicativi aziendali interconnessi
- modalità di acquisizione/esportazione dati
- tempi e modalità di conservazione/aggiornamento dati
- sistema operativo interno al dispositivo
- software previsto all'interno del dispositivo
- gestione delle credenziali
- modalità di backup dei dati
- nomina di responsabile e sub-responsabili esterni, con relativi recapiti

La verifica puntuale delle misure di cui sopra, viene effettuata attraverso checklist di controllo, finalizzate a:

- ✓ mappare il rischio, ai fini del trattamento dei dati personali delle apparecchiature già presenti e collaudate in Azienda;
- ✓ integrare la procedura di collaudo in modo che una serie di informazioni vengano prelevate già al momento della messa in esercizio per la prima volta dell'apparecchiatura.

CAPITOLO6
DISMISSIONE DELL'APPARECCHIATURA

E' attualmente prevista una procedura per la messa in fuori uso, la dismissione e l'alienazione delle apparecchiature biomediche.
La procedura si preoccupa essenzialmente di valutare se il bene in questione rappresenta una antieconomicità per l'Azienda per diverse motivazioni (obsolescenza, irreparabilità, non idoneità a nuove normative, inutilizzo, ecc.) e quindi ne propone e ne sancisce la messa in fuori uso e l'alienazione. La procedura prevede poi che il bene possa essere dismesso in diverse modalità, dallo smaltimento a carico di ditte specializzate, fino alla donazione, tipicamente a paesi in via di sviluppo attraverso associazioni onlus.
Sussiste quindi la criticità relativa alla valutazione della presenza all'interno delle apparecchiature messe in fuori uso di dati personali.
La procedura in questione dovrà regolamentare la problematica relativa all'eventuale presenza di dati personali all'interno delle apparecchiature messe fuori uso in quanto sussiste una significativa criticità in merito loro riservatezza e protezione.

CAPITOLO 7
PUBBLICAZIONE ED AGGIORNAMENTO

La presente procedura è stata adottata dal Titolare del trattamento, su proposta del DPO, e condivisa con l'U.O.C. Privacy – Trasparenza ed Integrità e con l' U.O.C. Ingegneria Clinica- HTA .
La suddetta procedura entra in vigore il giorno successivo alla sua approvazione. Il suo contenuto è soggetto ad aggiornamento periodico.
La sua diffusione, a cura dell'U.O.C. Privacy – Trasparenza ed Integrità, avverrà nelle seguenti forme: attraverso la rete informatica interna e la pubblicazione sul sito aziendale.
È fatto obbligo a chiunque spetti di osservarla.