Sistema Socio Sanitario

Regione Lombardia

ASST Nord Milano

Azienda Socio Sanitaria Territoriale Nord Milano

Deliberazione pubblicata all'Albo Informatico dell'Azienda
Dal 01/07/2021 al 22/07/2021

Il Responsabile U.O.C. Affari Generali
(dott.ssa Silvia Liggeri)

Deliberazione n. 574 del 28/06/2021

Tit. di Class. 1.1.02

A269
GR

OGGETTO: Regolamento sulle modalità di custodia e sulle misure di sicurezza per la tutela degli archivi informatici: Rimozione sicura dei dati dell'Azienda Socio Sanitaria Territoriale Nord Milano in ottemperanza al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – Applicazione delle misure tecniche previste dall'Art. 32.

IL DIRETTORE GENERALE

PREMESSO che le norme introdotte dal Regolamento (UE) 2016/679 in data 27.04.2019 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di protezione dei dati personali;

RICHIAMATI i precedenti atti deliberativi in ordine all'applicazione della normativa sul trattamento dei dati personali, ovvero:

- deliberazione n. 753 del 04/11/2020 approvazione del Regolamento informatico;
- deliberazione n. 659 del 24/12/2003 approvazione del Regolamento generale sul trattamento dei dati;

RICHIAMATO l'art. 32 del Regolamento Generale sulla protezione dei Dati (GDPR UE/2016/679) commi 1, 2 ,4, ai sensi del quale: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;

DATO ATTO della collaborazione in essere tra l'UOC Servizi Informatici Aziendali e l'UOS Affari Legali, Ufficio Privacy, finalizzata all'adozione delle più adeguate misure di sicurezza in ambito tecnico e organizzativo sul trattamento dei dati;

PRESO ATTO altresì, che in attuazione dell'art. 32 del Regolamento Generale sulla Protezione dei Dati (GDPR – UE/2016/679), e nell'ambito più generale delle azioni congiuntamente attuate dalle due Strutture aziendali citate, è stato predisposto il seguente Regolamento sulle modalità di custodia e sulle misure di sicurezza per la tutela degli archivi informatici: Rimozione sicura dei dati.

VISTO l'allegato testo del Regolamento in oggetto, come predisposto dalla UOC Servizi Informativi Aziendali in collaborazione con l'Ufficio Privacy (UOS Affari Legali) che aggiorna e sostituisce ogni altra disposizione in precedenza emanata con esso confliggente;

RITENUTO di approvare il testo del suddetto "Regolamento sulle modalità di custodia e sulle misure di sicurezza per la tutela degli archivi informatici: Rimozione sicura dei dati", allegato alla presente deliberazione quale parte integrante, unitamente ai suoi allegati;

ATTESO che dal presente provvedimento non derivano oneri a carico del bilancio aziendale, così come attestato dall'U.O.C. Bilancio e Risorse Finanziarie, nell'ultimo foglio allegato al presente provvedimento;

SU PROPOSTA del Responsabile della UOC Servizi Informativi Aziendali che attesta la legittimità e regolarità tecnico/amministrativa del presente provvedimento, come riportato nell'ultimo foglio;

PRESO ATTO del parere favorevole espresso, per quanto di rispettiva competenza, dal Direttore Amministrativo, dal Direttore Sanitario e dal Direttore Sociosanitario;

- d e l i b e r a -

per le motivazioni esposte in premessa:

1. di prendere atto delle attività aziendali svolte, in applicazione della normativa nazionale ed europea in tema di "protezione dei dati personali", descritte negli atti deliberativi citati in premessa;

2. di approvare l'allegato "Regolamento sulle modalità di custodia e sulle misure di sicurezza per la tutela degli archivi informatici: Rimozione sicura dei dati", revocando contestualmente ogni altra disposizione in precedenza emanata confliggente con detto regolamento;

3. di dare atto che il Responsabile del procedimento relativo al presente provvedimento è il Responsabile dell'UOC SIA ing. Pietro Lanzoni;

4. di disporre la pubblicazione del Regolamento che si approva con il seguente atto nella sezione amministrazione trasparente del sito web aziendale;

5. di dare atto che il presente provvedimento non comporta oneri di spesa;

6. di dare mandato al Responsabile del procedimento per tutti i necessari, successivi incombenti all'attuazione del presente provvedimento;

7. di dare atto che il presente provvedimento è immediatamente esecutivo ai sensi dell'art. 17, comma 6, della legge regionale 30 dicembre 2009, n. 33, e ss. mm.;

8. di disporre la pubblicazione del provvedimento all'Albo Pretorio on-line aziendale, ai sensi dell'art. 17, comma 6, della legge regionale 30 dicembre 2009, n. 33, e ss. mm.;

9. di trasmettere il presente provvedimento al Collegio Sindacale.

(atti n. 3/2021 tit.01/07/03)

Parere favorevole:

IL DIRETTORE SANITARIO
(d.ssa Anna Lisa Fumagalli)

IL DIRETTORE AMMINISTRATIVO
(dott. Giovanni Palazzo)

IL DIRETTORE SOCIOSANITARIO
(d.ssa Barbara Mangiacavalli)

IL DIRETTORE GENERALE
(d.ssa Elisabetta Fabbrini)

deliberazione del Direttore Generale n. 574 del 28 GIU. 2021, avente all'oggetto: "Regolamento sulle modalità di custodia e sulle misure di sicurezza per la tutela degli archivi informatici: Rimozione sicura dei dati dell'Azienda Socio Sanitaria Territoriale Nord Milano in ottemperanza al Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati – Applicazione delle misure tecniche previste dall'Art. 32".

* * * * * * * * * *

Il sottoscritto Responsabile della U.O.C. Servizi Informativi Aziendali e Responsabile del procedimento:

ATTESTA

la legittimità e regolarità tecnico/amministrativa del presente provvedimento;

DICHIARA

☒ che il presente provvedimento non comporta alcun onere.

Il Responsabile della U.O.C. Servizi Informativi Aziendali
e Responsabile del procedimento
(ing. Pietro Lanzoni)

Il Responsabile della U.O.C. Bilancio e Risorse Finanziarie conferma:

☐ la copertura economica del presente provvedimento e l'annotazione a bilancio sopra riportata

☒ che dal presente provvedimento non derivano oneri a carico del bilancio.

Il Responsabile della U.O.C. Bilancio e Risorse Finanziarie
(d.ssa Domenica Luppino)

Sistema Socio Sanitario
Regione Lombardia
ASST Nord Milano

REGOLAMENTO SULLE MODALITA' DI CUSTODIA E SULLE MISURE DI SICUREZZA PER LA TUTELA DEGLI ARCHIVI INFORMATICI:

RIMOZIONE SICURA DEI DATI

Riservatezza

Il presente documento è da intendersi ad uso interno e pertanto deve essere trattato come materiale riservato. Non devono essere distribuite copie a terzi non incaricati al trattamento.

PREMESSA

La seguente procedura pone l'attenzione circa la gestione del problema "**e-waste**" che riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a sé o a terzi.

È compito infatti del possessore dei dati di assicurare che questi non possano andare dispersi e acquisiti anche in modo incontrollato da estranei. La semplice cancellazione dei file o la formattazione dell'hard disk, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.

I dischi virtuali dovrebbero essere considerati come parte di qualsiasi processo di eliminazione dei dati. I fornitori di servizi di terze parti in particolare utilizzano l'infrastruttura virtualizzata per ripartire lo spazio storage su più clienti, al fine di ottenere delle economie di scala.

Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

- preventivamente, con tecniche di memorizzazione sicura;
- immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti software di cancellazione sicura (a condizione che l'apparato sia funzionante);
- al momento della cessione o dismissione, con la demagnetizzazione (degaussing), che azzera tutte le aree di memoria elettronica e rende l'apparato inutilizzabile o con la distruzione fisica del dispositivo di memorizzazione.

Per ciascuna delle opzioni citate si forniscono qui di seguito delle informazioni per la messa in pratica o per il reperimento di informazioni più dettagliate.

Nel caso di dismissione di un computer, l'amministratore, a prescindere dall'utilizzo futuro dei dispositivi di archiviazione (riciclo o distruzione), provvede a rimuoverli dall'hardware stesso. Questa procedura permette che i supporti di memorizzazione ed eventuali i dati in essi contenuti non vengano trasportarti esternamente all'azienda.

DESTINATARI

- Amministratore di sistema
- Dipendenti incaricati della gestione, verifica e manutenzione della procedura di rimozione sicura

TECNICHE DI MEMORIZZAZIONE SICURA

La memorizzazione sicura dei file (adottata come tecnica preventiva) si può realizzare sui più diffusi sistemi operativi con l'attivazione di funzionalità crittografiche proprie del sistema, se disponibili, o con l'installazione di prodotti software aggiuntivi. Le concrete modalità dipendono fortemente dallo specifico sistema operativo utilizzato, e talvolta anche dalla sua versione o dall'applicazione di patch e aggiornamenti.

I possessori di personal computer sono pertanto esortati a rivolgersi alle case produttrici del proprio hardware o del sistema operativo in uso per ottenere indicazioni dettagliate.

- Si rinviano, in particolare, gli utenti di sistemi operativi Windows alla consultazione delle pagine informative predisposte, in lingua italiana, dalla casa produttrice Microsoft (http://www.microsoft.com/italy/pmi/sicurezza/privacy/).
- Per i sistemi Apple, le pagine consultabili sul sito italiano del produttore illustrano le funzionalità FileVault disponibili nel sistema operativo Mac OS X per la protezione di intere directory o di volumi di dati.

Tra i sistemi "multipiattaforma" (non dipendenti da uno specifico sistema operativo e perciò utilizzabili in ambiente Windows, Mac OS, Unix, Linux...), è disponibile il software TrueCrypt, che offre funzioni di cifratura con strong encryption di partizioni e interi dischi, comprese le partizioni "di sistema".

Per alcuni dispositivi di archiviazione di massa removibile, invece, la funzione di crittografia viene offerta direttamente dal prodotto attraverso un sistema proprietario sviluppato direttamente dalla casa madre e preventivamente installato sul dispositivo stesso.

Il sistema di crittografia può essere adottato secondo due modalità:

- Interamente sul dispositivo di archiviazione (hard disk, pen-drive, CD-ROM, etc)
- Singolarmente su ciascun file.

CANCELLAZIONE SICURA DISPOSITIVO FUNZIONANTE

In caso di reimpiego e/o riciclaggio di rifiuti di apparecchiature elettroniche, sarà compito del Titolare del trattamento, avvalendosi della collaborazione dell'amministratore del sistema ed eventualmente degli incaricati al trattamento e/o della manutenzione, dare indicazioni agli incaricati al fine di garantire la sicurezza dei dati in queste precedentemente contenuti.

Gli utenti di sistemi operativi Microsoft Windows possono far riferimento alle già menzionate pagine

informative pubblicate dal produttore (http://www.microsoft.com/italy/pmi/sicurezza/privacy/), che illustrano nel dettaglio le modalità per affrontare il problema della cancellazione di interi volumi di dati qualora non sia stata preventivamente adottata la soluzione della memorizzazione sicura.

Gli utenti del sistema operativo Apple Mac OS X, che incorpora una funzione di "svuotamento del cestino in modalità sicura", potranno trovare dettagliate informazioni sul sito del produttore www.apple.it oppure ricorrere a utility di tipo "open source" come Permanent Eraser, che consente di effettuare cancellazioni sicure con un algoritmo avanzato.

Al termine della procedura di cancellazione di ogni singolo dispositivo viene generato un documento e/o compilato un file Excel dove vengono tracciati: modello, numero di serie dello stesso, la procedura utilizzata e il risultato della stessa, garantendo che la cancellazione sia avvenuta definitivamente e a norma di legge permettendo il totale rispetto delle normative vigenti.

Tecnologie utilizzate

Nella cancellazione software, sono possibili le seguenti metodologie:

- **US DoD 5220.22-M**: Ogni settore viene riscritto tre volte, la prima volta inizializzandolo con la stringa 0x00, la seconda volta con la stringa 0xFF, e la terza volta con valori casuali. Viene inoltre effettuata una lettura finale per verificare la casualità dei dati memorizzati.
- **US DoD 5220.22-M (ECE):** Ogni settore viene riscritto sette volte, rispettivamente con le stringhe 0x00, 0xFF, Random (casuale), 0x96, 0x00, 0xFF, Random (casuale). Viene inoltre effettuata una lettura finale per verificare la casualità dei dati memorizzati.
- **Gutmann**: Ogni settore viene riscritto complessivamente 35 volte, rendendo questa metodologia la più sicura in assoluto. Va considerato però il dispendio di tempo per tale metodologia, che non migliora in modo sostanziale il risultato, riducendo inoltre la vita utile del dispositivo.

Utilizziamo preferibilmente le prime due metodologie, che risultano essere quelle usate anche dal Dipartimento della Difesa Americano, come il nome stesso (DoD) indica.

Al termine dell'esecuzione dell'attività l'amministratore procede alla compilazione del modulo allegato "elenco_attivita_rimozione_sicura".

DEMAGNETIZZAZIONE (DEGAUSSING) E DISTRUZIONE FISICA

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano

pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (degausser), o con la distruzione fisica.

I degausser permettono l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.

In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con apposite macchine analoghe ai "trita carta" in uso negli uffici.

Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.

Al termine dell'esecuzione dell'attività l'amministratore procede alla compilazione del modulo allegato "elenco_attivita_rimozione_sicura".

ALLEGATI

elenco_attivita_rimozione_sicura .xlsx

A_Allegato 1_elenco_attivita_rimozione_sicura

tipologia di dispositivo	modello	numero di serie	procedura utilizzata	esito	data esecuzione	incaricato	soggetto incaricato
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							
Server							