PO01 – Linee Guida per il trattamento dei dati personali con strumenti elettronici

ASL. N. 3 NUORO
Via Demurtas, 1

SCOPO

Scopo del presente documento è fornire le linee guida per attuare in azienda un sistema di protezione dei dati personali trattati con l'ausilio degli strumenti elettronici ed adottare le misure minime di sicurezza previste dal D.Lgs. 196/2003

CAMPO APPLICAZIONE

La presente procedura si applica a tutti i trattamenti di dati personali effettuati con l'ausilio di strumenti elettronici.

RIFERIMENTI

D.Lgs. 196/2003 Artt. 31, 33, 34,
Allegato B al D.Lgs 196/2003 "Trattamenti con strumenti elettronici"
Asl. Nuoro del 29/03/2007 Protocollo interno N. 226 (Ing. Gianoglio)
Documento Programmatico per la Sicurezza dei Dati Personali

EMISSIONE VERIFICA E APPROVAZIONE

Responsabile dell'emissione della procedura è l'Amministratore di Sistema e il servizio di manutenzione
Responsabile della verifica è l'amministratore di sistema, il servizio di manutenzione e il Gruppo Lavoro Privacy (GLP)
Responsabile dell'Approvazione della Procedura è il Direttore Generale

RESPONSABILITÀ

Il responsabile della procedura e del coordinamento delle attività tecniche per la messa in sicurezza dei sistemi elettronici è l'Aministratore di Sistema (ADS)
Responsabili della implementazione e controllo delle misure minime nonché del rispetto delle procedure di gestione sono i responsabili del trattamento.

GENERALITÀ

L'accesso agli strumenti elettronici per il trattamento di dati personali può avvenire solo da parte di incaricati autorizzati e dopo aver superato una procedura di autenticazione. L'utente autorizzato e autenticato potrà avere accesso esclusivamente ai dati in modo corrispondente al suo profilo di autorizzazione. Sistemi di autenticazione e autorizzazione dovranno essere periodicamente controllati e aggiornati in funzione delle autorizzazioni stabilite nell'incarico al trattamento e alle mansioni dell'incaricato. Le credenziali e i profili di autorizzazione devono essere revocati o modificati in caso di perdita della qualità di incaricato del trattamento o cambiamento di mansione/funzione dell'incaricato al trattamento.
L'implementazione del sistema di misure minime per il trattamento con strumenti elettronici è coordinato dal servizio di manutenzione e dagli ADS che su richiesta e indicazione dei responsabili del trattamento provvede ad implementare il sistema idoneo a garantire la sicurezza dei trattamenti di dati personali con strumenti elettronici.

Compito del servizio di manutenzione è l'implementazione di tutte le operazioni tecniche necessarie ad assicurare accessi ai dati non autorizzati e l'implementazione delle misure minime conformi alle specifiche indicate nel DLgs 196/2003 e alle procedure di sicurezza interne approvate dal Titolare del Trattamento.

ELENCO DEGLI STRUMENTI ELETTRONICI PER IL TRATTAMENTO DEI DATI PERSONALI

Il Servizio della manutenzione degli strumenti elettronici tiene aggiornato l'elenco degli strumenti per il trattamento dei dati personali che trasmetterà annualmente entro il 28 febbraio al GLP, il quale provvederà ad allegarlo al DPS.

Per ogni strumento dovrà essere indicato:

- Il tipo di strumento
- La sua identificazione
- Il software di sistema installato e la versione
- La sua mappatura all'interno della Lan (l'indirizzo IP)
- Il luogo di utilizzo
- I software installati e le rispettive versioni
- Il tipo di antivirus installato e la versione

L'inventario degli strumenti elettronici in futuro verrà effettuato con specifici strumenti di Desktop Management che emetteranno report dinamici sullo stato dei client della rete.

ACCESSO AGLI STRUMENTI E AI DATI

L'accesso allo strumento deve avvenire con un codice per l'identificazione dell'incaricato (detta username o login name) associato ad una parola chiave (password). L'insieme di queste due componenti viene identificata come "credenziale".

Le credenziali vengono rilasciate in modo esclusivo ad ogni incaricato del trattamento il quale provvederà a modificare la componente riservata delle credenziali (password) al primo accesso al sistema.

Ogni incaricato può avere anche più di una credenziale di accesso ad uno o più sistemi di trattamento in dipendenza delle mansioni.

Lo strumento utilizzato per il trattamento dei dati deve forzare in modo automatico il cambio password ogni trimestre da parte dell'incaricato che ha ricevuto le credenziali di autenticazione.

Le sessioni di lavoro dovranno impedire l'accesso in caso di inoperatività superiore a 5 minuti. Per ripristinare una sessione sospesa occorre reinserire le credenziali.

Se più incaricati condividono uno strumento, ognuno ha una propria login e password che fa riferimento ad uno specifico profilo o anche allo stesso profilo di autorizzazione.

Il sistema deve essere configurato in modo da disabilitare le credenziali non utilizzate da più di sei mesi.

ASL. N. 3 NUORO
Via Demurtas, 1

MISURE DI SICUREZZA CONTRO ACCESSI NON AUTORIZZATI E CONTROLLI PERIODICI

Tutti i personal computer devono essere provvisti di antivirus aggiornati. L'aggiornamento può avvenire in modo automatico con sistemi tipo live update o a cura del servizio di manutenzione con cadenza almeno semestrale per quegli strumenti che non dispongono di sistemi di live update.

Almeno semestralmente il servizio di manutenzione verifica lo stato di aggiornamento dei software di base e dei altri programmi per elaboratore volti a prevenire vulnerabilità degli strumenti elettronici e a correggerne difetti.

FIREWALL E STRUMENTI ELETTRONICI CONTRO IL RISCHIO DI INTRUSIONE

Se lo strumento è connesso in LAN o WAN sono attivi e tenuti aggiornati firewall e altri strumenti idonei ad impedire il rischio di intrusione o l'azione di programmi di cui all'art. 615 quinquies del codice penale che dovranno essere controllati e aggiornati con cadenza almeno semestrale da parte del servizio di manutenzione.

ALTRE PROCEDURE PER LA SICUREZZA DEI DATI

Onde evitare perdite di dati o inaffidabilità o inconsistenza degli stessi occorre prevedere procedure di backup (salvataggio di una copia dei dati su un supporto diverso da quello utilizzato per il trattamento).

I backup sono centralizzati per le banche dati centralizzate e locali per le banche dati locali.

I backup centralizzati vengono effettuati una o più volte al giorno.

I backup locali dovranno essere effettuati almeno settimanalmente e comunque con cadenza adeguata in funzione dell'importanza dei dati che sono trattati. Le frequenze inferiori alla settimanale sono stabilite dal responsabile del trattamento competente.

Il servizio di manutenzione dovrà fornire strumenti e istruzioni per eseguire il backup locale.

Semestralmente il servizio di manutenzione controlla la consistenza dei backup con prove di ripristino.

I supporti utilizzati per i backup vengono custoditi in locali idonei diversi dai locali di trattamento.

GESTIONE DEI DATI PERSONALI ARCHIVIATI IN ALTRE BANCHE DATI

Sono vietati trattamenti di dati personali in banche dati locali a meno che non sia strettamente necessario (sedi distaccate non connesse in LAN, strumenti connessi a macchine diagnostiche, strumenti per la ricerca scientifica ecc..).

Tutti i dati devono risiedere su file server gestiti dall'incaricato della manutenzione degli strumenti elettronici. Per ogni banca dati verrà creato un profilo di autorizzazione come specificato nell'allegato ALL_A e ALL_A1 al DPS a cui saranno autorizzati gli utenti incaricati indicati dai vari responsabili del trattamento.

L'autorizzazione al trattamento in banche dati locali deve essere data dal responsabile del trattamento per iscritto. Copia dell'autorizzazione deve essere inviata al responsabile della

manutenzione degli strumenti elettronici affinché questi possa predisporre adeguate procedure per il backup.

ISTRUZIONI PER I BACKUP

L'incaricato del servizio di manutenzione in accordo con ADS per ogni banca di dati definisce :

- Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
- Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle Copie di sicurezza dei dati.
- Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati indicato eventualmente dal RSDP.
- Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

BACKUP DELLE BANCHE DATI CONDIVIDE DI MAGGIORE RILEVANZA

In azienda sono presenti banche dati di particolare rilevanza per le quali è previsto un backup giornaliero. Di seguito l'elenco delle banche dati di maggiore rilevanza:

- SIO Sistema Informativo Ospedaliero (SISaR)
  Elenco delle funzionalità principali:
  - Ricoveri ordinari
  - Day Hospital
  - SDO – Schede dimissione ospedaliera
  - DRG – Diagnosis Related Group

- CUP (SISaR)
- *Elenco delle funzionalità principali:*
  - Centro unico di Prenotazione
  - Accettazione sanitaria
  - Gestione Ticket

- Anagrafiche (SISaR)
- *Elenco delle funzionalità principali:*
  - Anagrafica Assistibili e Assistiti
  - Scelta e Revoca del Medico

- SFERA CARTA Software Gestione Veterinaria

- SOFTART – ALLPHARM Software gestione Farmacia e somministrazione diretta farmaci
- SISaR : Contabilità Generale e Analitica
- SISaR: Gestione Paghe e Stipendi e rilevazione presenze
- SISaR e ITALABCS DIANOEMA (Laboratorio San Francesco)
- SISaR e METAPHORA (Laboratorio Ospedale Zonchello)

Per queste banche dati, la frequenza di backup è giornaliera.

Il backup avviene su server in modo automatizzato su nastro.

Giornalmente gli incaricati del backup cambiano il nastro inserendo il nastro con il giorno della settimana archiviando il precedente in luogo sicuro. Ci sono 5 nastri disponibili:

lunedì,
martedì,
mercoledì,
giovedì
venerdì

Il sabato e la domenica vengono automaticamente backuppati sul nastro del venerdì.

L'incaricato provvede ad archiviare in luogo sicuro i nastri con i dati di backup facendoli ruotare nell'arco della settimana.

Ogni sei mesi i nastri vengono sostituiti non nuovi nastri ed i vecchi nastri vengono distrutti.

L'incaricato del backup provvede almeno una volta al mese ad effettuare le prove di ripristino per controllare l'effettiva validità dei backup o controllare la consistenza dei dati di backup con i mezzi più opportuni assicurandosi appunto che i dati nei nastri siano corretti e consentano un recupero dei dati in caso guasti ai sistemi. Proprio in caso di disaster recovery gli incaricati del backup o gli incaricati della manutenzione o le ditte appaltatrici del servizio di manutenzione devono essere in grado di ripristinare le funzionalitàdel sistema al massimo entro 7 giorni dal guasto e comunque in tempi compatibili con i diritti degli interessati.

APPLICAZIONI AUTORIZZATE

L'incaricato del servizio di manutenzione degli strumenti elettronici redige un elenco di tutti i software in uso in azienda e dunque autorizzati.

Ogni software installato deve essere certificato dall'incaricato della manutenzione degli strumenti elettronici prima della sua installazione.

E' fatto assoluto divieto installare strumenti e software non certificato.

La certificazione del software consiste nel controllare ed identificare:

- la compatibilità del software con l'infrastruttura tecnologica
- i requisiti di sicurezza ai fini di prevenire accessi non autorizzati ai dati
- il grado di importanza del software
- la disponibilità di documentazione a corredo
- la disponibilità del fornitore a risolvere problemi tecnici e di affiancare il servizio di manutenzione
- gli standard industriali di prodotto
- i tempi di intervento compatibili con il grado di importanza (SLA Service Level Agreement)

INSTALLAZIONE DI APPLICAZIONI

Gli strumenti elettronici sono configurati in modo da impedire l'installazione di qualsiasi software da parte degli incaricati del trattamento o di personale non autorizzato. Ogni nuova richiesta va inoltrata al servizio della manutenzione degli strumenti elettronici.

La richiesta dovrà essere firmata dal responsabile del trattamento.

Se si tratta di un software certificato, il servizio di manutenzione provvederà alla installazione presso l'utente che ne ha fatto richiesta.

Se si tratta di software non certificato, si dovranno effettuare tutte le verifiche di compatibilità e sicurezza con l'infrastruttura tecnologica della ASL. In caso di superamento dei requisiti di compatibilità e sicurezza il software viene inserito nell'elenco dei software certificati ed il servizio di manutenzione provvederà alla sua installazione.

E' fatto divieto a chiunque al di fuori degli incaricati del servizio di manutenzione di installare o tentare di installare software sui PC aziendali. I fornitori di software dovranno fornire adeguata documentazione e istruzioni per l'installazione e configurazione dei software. In caso di installazioni particolarmente complesse il tecnico del fornitore dovrà assistere il personale del servizio di manutenzione durante l'installazione. Il servizio di manutenzione dovrà essere messo in grado di poter effettuare tutte le operazioni che richiedono accessi al registro di sistema o credenziali con privilegi amministrativi.

NUOVI UTENTI

Tutte le richieste di autorizzazione per la creazione di nuovi utenti o modifica dei profili di autorizzazione vanno inoltrate al servizio di manutenzione degli strumenti elettronici il quale darà seguito alle attività solo previa autorizzazione del responsabile del trattamento.

ASL. N. 3 NUORO
Via Demurtas, 1

NUOVO HARDWARE

Come per il software anche l'hardware deve essere certificato dal servizio di manutenzione degli strumenti elettronici.

L' hardware dovrà seguire il principio di "omogeneità del parco macchine" in modo da semplificare le operazioni di manutenzione tecnica.

La certificazione dell'hardware deve soddisfare in generale i seguenti requisiti:

- compatibilità con l'infrastruttura tecnologica dell'ASL
- compatibilità con i sistemi di sicurezza