

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

ANNO 2011

AZIENDA USL 12 DI VIAREGGIO

INTRODUZIONE	3
DISTRIBUZIONE DEI COMPITI	3
INTERVENTI FORMATIVI.....	3
INFORMATIVA SUL TRATTAMENTO DATI	3
SICUREZZA FISICA.....	4
Misure di sicurezza degli archivi cartacei.....	4
Protezione delle aree e dei locali interessati.....	4
APPARATI DI RETE	5
SICUREZZA DEL SOFTWARE.....	5
Procedure per assicurare l'integrità dei dati.....	5
Integrità dei dati gestiti direttamente dalle strutture	9
Integrità dei dati gestiti in ASP	10
Sistema di controllo, monitoraggio e politiche di accesso ai dati.....	10
Basi dati in produzione	11
Basi dati replicate	11
Antivirus centralizzato	11
Amministratori di sistema.....	12
Il progetto Repository Sanitario	12
SICUREZZA TRASMISSIONI DEI DATI	13
Controllo degli accessi	13
Accesso da parte dei fornitori che prestano assistenza.....	13
Trasmissione dei dati.....	14
Trasmissione dei dati in Regione Toscana.....	14
ALLEGATI.....	15

Introduzione

Scopo di questo documento è stabilire le misure minime di sicurezza da adottare affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dalla Legge 196/2003 sulla protezione dei dati personali.

Va notato che molti dei dati gestiti nel Sistema Informatico dell'Azienda USL 12 di Viareggio sono di tipo "sensibile" e pertanto devono opportunamente essere protetti, al di là degli obblighi derivanti dalla Legge sulla Privacy.

Distribuzione dei compiti

Per quanto riguarda la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati, l'Azienda ha provveduto, con provvedimento formale del direttore generale, ai sensi di quanto previsto dall'art.29 del D. Lgs 196/03, ad aggiornare l'elenco dei responsabili del trattamento. In termini generali all'interno di ogni struttura preposta al trattamento di dati la responsabilità del trattamento è in capo al responsabile di struttura (complessa o semplice).

Gli operatori di ogni struttura, qualora chiamati a compiti di trattamento, in relazione alle proprie mansioni ed alla più ampia missione istituzionale della azienda sanitaria, svolgono la funzione di incaricati al trattamento e vengono designati come tali per iscritto dal responsabile del trattamento.

L'elenco degli incaricati, le relative nomine con le istruzioni operative fornite agli stessi sono conservati a cura del responsabile del trattamento

L'Azienda ha inoltre provveduto alla ricognizione dei soggetti esterni con la quale la stessa intrattiene rapporti istituzionali. Nel caso in cui tali soggetti effettuino sistematicamente per conto dell'Azienda operazioni di trattamento di dati personali di soggetti terzi, gli stessi sono nominati responsabili esterni del trattamento con provvedimento formale del direttore generale.

E' il caso, a titolo esemplificativo, delle associazioni di volontariato, delle farmacie convenzionate, dei fornitori di servizi (ristorazione, trasporto barellati....)

Interventi formativi

E' emersa l'esigenza di riavviare ex novo un percorso formativo trasversale a tutti i settori di attività che da un lato assicurasse da parte degli operatori l'acquisizione delle conoscenze di base in tema di privacy, con particolare riferimento agli aspetti della tutela della riservatezza, dell'identità personale e della sicurezza e che nel contempo fornisse agli stessi le competenze per gestire e risolvere singole problematiche sull'argomento che potessero presentarsi nel corso dell'attività lavorativa.

E' stato deciso di strutturare un corso con nuove modalità attraverso un percorso misto composto da tre ore di corso in formazione a distanza (FAD) e due ore di corso in aula, da ripetersi in più edizioni nell'anno. La modalità in FAD e la breve (ma necessaria e imprescindibile) formazione in aula consente di formare un alto numero di dipendenti, di varie qualifiche e appartenenti a vari settori di attività

Informativa sul trattamento dati

E' stata redatta ed affissa nelle sedi aziendali l'informativa per il cittadino concernente la finalità di utilizzo dei dati, le modalità di trattamento, nonché la possibilità per il cittadino di richiedere informazioni che lo riguardano ed esprimere eventualmente il dissenso al trattamento.

In allegato il testo integrale dell'informativa

Ulteriori specifiche informazioni sono fornite al cittadino in merito alla RTRT, Rete Telematica Regione Toscana struttura attivata dalla Regione , per garantire la sicurezza dei dati, attraverso l'autenticazione e l'accesso ai servizi ed alle informazioni. Le informazioni viaggiano all'interno di, utilizzando protocolli di trasporto tipo VPN. La modalità di autenticazione degli utenti è tramite i certificati digitali, basati su crittografia a chiave pubblica, utilizzati all'interno di applicazioni web-oriented sfruttando il protocollo SSL, oppure per accedere al sistema di cooperazione applicativa. Dal 2010 è attivo il progetto regionale Fascicolo Sanitario Elettronico, che prevede una incrementale disponibilità di documenti sanitari visualizzabili dal cittadino che si autentica al sistema tramite la Tessera Sanitaria Elettronica. Le Tessere Sanitarie, rispondenti agli standard delle CNS (Carte Nazionali dei Servizi), vengono attivate presso le USL di residenza dei cittadini, ai quali viene chiesto anche il consenso alla costituzione del Fascicolo Sanitario Elettronico. E' stata predisposta un'apposita sezione "privacy" sul sito aziendale all'interno della quale sono stati inseriti documenti e legislazione utile.

Sicurezza Fisica

Misure di sicurezza degli archivi cartacei

Gli archivi sono situati in locali non esposti a rischi ambientali e custoditi con modalità atte a garantire le misure minime di sicurezza come da DPR 28.07.99 n. 318.

L'accesso agli archivi aziendali è controllato e vi possono accedere soltanto soggetti autorizzati.

Con riferimento agli archivi amministrativi la responsabilità della conservazione e sicurezza dei medesimi spetta al Responsabile cui i dati oggetto del trattamento sono di competenza.

Gli archivi delle cartelle cliniche sono sotto la responsabilità del Direttore Medico del Presidio Ospedaliero.

Per le cartelle sanitarie e la documentazione equipollente giacente presso strutture non ospedaliere la responsabilità fa capo ai Responsabili dei Presidi distrettuali e ai Direttori delle strutture cui gli archivi afferiscono.

Nel caso di documentazione archiviata presso soggetti esterni, nominati responsabili esterni del trattamento, gli stessi sono responsabili della conservazione e della sicurezza.

Protezione delle aree e dei locali interessati

Il furto od il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre l'Azienda al rischio di violare la Legge sulla Privacy.

Per tale motivo sono istituiti controlli per limitare l'accesso fisico ad alcune aree.

Le macchine server principali sono collocate in un apposito locale (sala macchine presso il Sistema Informativo e Tecnologie).

La sala macchine è dotata di:

- Impianto antincendio;
- Impianto di condizionamento ambientale
- Impianto elettrico a norma;
- Gruppo di continuità

Non sono presenti porte e finestre blindate.

L'accesso alla sala macchine è consentito solamente alle persone espressamente autorizzate (individuate nel personale del Sistema Informativo e Tecnologie e nel personale addetto alla manutenzione degli impianti elettrici). In assenza del personale autorizzato, la sala macchine è tenuta chiusa a chiave. La sala macchine non è dotata di controllo badge per l'accesso ai locali.

I supporti di backup sono tenuti in una cassaforte, posta in un diverso locale rispetto alla sala macchine, la cui chiave è custodita all'interno dell'ufficio Sistema Informativo e Tecnologie. Le chiavi dei locali dello stesso ufficio sono custodite dalla vigilanza e dal personale del Sistema Informativo e Tecnologie.

Il controllo e la gestione dei documenti stampati è responsabilità degli incaricati al trattamento in particolare la stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Particolare attenzione viene posta ai computer portatili contenenti dati sensibili o password di accesso alle basi dati aziendali, sensibilizzando i diretti interessati per la corretta gestione degli stessi.

Apparati di Rete

I collegamenti di rete dell'Azienda USL 12 di Viareggio sono di varia tipologia (prevalentemente cablaggi strutturati ma anche reti wireless). Il tutto ha una struttura di tipo a stella facente capo alla sala macchine.

Per la parte relativa ai cablaggi gli armadi che contengono gli apparati di rete sono tenuti chiusi a chiave e gli stessi armadi si trovano in stanza a loro volta chiuse a chiave. Le chiavi sono custodite sia dalla vigilanza sia dal personale del Sistema Informativo e Tecnologie sia dal personale che si occupa del settore telefonico.

In generale le porte degli apparati di rete (in particolare degli "switch") che non sono utilizzate non sono fisicamente collegate.

L'indirizzamento degli apparati di rete si trova su una rete IP (VLAN) distinta.

E' in fase di realizzazione una rete wireless, aggiuntiva rispetto alla rete cablata, per i reparti di degenza ospedaliera. Tale infrastruttura ha l'obiettivo di consentire a medici ed infermieri di utilizzare le procedure ospedaliere al letto del paziente (es. richieste alle diagnostiche, consulenze, cartella infermieristica). L'accesso alla rete wireless per il momento sarà limitato a qualche decina di Tablet PC acquisiti allo scopo.

Il progetto della rete wireless prevede l'adozione di politiche di sicurezza basate su standard IEEE 802.11i (WPA2, RSN) e di autenticazione ed autorizzazione basate su standard IEEE 802.1x e Radius.

Sicurezza del software

Procedure per assicurare l'integrità dei dati.

Per le banche dati gestite su server centralizzati sono state implementate specifiche procedure di backup attraverso le quali viene giornalmente effettuata una copia dei dati presenti sui sistemi. Il salvataggio avviene in maniera automatizzata tramite l'utilizzo di un software che gestisce una libreria di dieci cartucce magnetiche di tipo DLT. Ogni lunedì e giovedì mattina, a cura del responsabile della gestione del backup centralizzato o suoi incaricati, vengono estratte dalla libreria le cassette utilizzate i giorni precedenti e conservate in una cassaforte ignifuga collocata nello stesso edificio della sala macchine ma in altro locale, sempre allo stesso piano. *Non è prevista nessuna forma di custodia remota delle cassette in locali geograficamente separati, né alcuna forma di replica completa degli archivi su server separati e collocati in un altro edificio.*

La procedura attualmente posta in essere consente, in caso di crash dei sistemi, di ripristinare i dati almeno ad una settimana precedente, *ma non tutela dal caso di distruzione dei server posti nell'edificio e in caso di copie difettose in quanto non vengono fatte doppie copie giornaliere su supporti separati.*

Sempre con cadenza giornaliera, vengono controllati da operatori incaricati i log per verificare che ogni job di salvataggio pianificato sia andato a buon fine e che non si siano presentati errori. Non sono invece previste prove di ripristino a cadenza regolare ma solamente una tantum.

Ogni situazione anomala viene tempestivamente comunicata dagli stessi addetti al responsabile che si occupa di intraprendere tutte le azioni eventualmente necessarie a riportare la situazione alla normalità qualora si verificano dei malfunzionamenti.

Il salvataggio delle configurazioni dei server è pianificato invece con cadenza mensile o qualora si verifichi un qualche cambiamento sostanziale nelle configurazioni stesse.

Architettura Server

Per quanto riguarda l'infrastruttura hardware è stata utilizzata un'architettura di storage in rete in fibra ottica (StorageAreaNetwork) di circa 3Terabyte di spazio complessivo, formata da dischi FiberChannel configurati in RAID5 per rispondere con efficienza sia al requisito di sostituzione Hotplug che di ottimizzazione dello spazio. E' gestita da due controller HP Eva4000, le cui componenti hardware sono completamente ridondate per ridurre l'incidenza di problemi legati a possibili guasti hardware. A questa infrastruttura fanno capo due gruppi di cluster, uno attivo/attivo, con servizi assegnati in modo preferenziale all'uno oppure all'altro nodo, formato da due nodi HP-RS3600 che gestiscono la maggior parte dei servizi di database Oracle; l'altro attivo/passivo formato da due nodi HP-RS2600 dedicato alla gestione del DataRepository aziendale. Utilizzano sempre la stessa SAN una serie di lame Blade Dell 8100 che gestiscono circa 30 server virtuali.

Backup dei dati

L'architettura del backup centralizzato è in fase di migrazione su nuova piattaforma, al momento è ancora in piedi su motore Unix Tru64 su hardware Compaq ES40, il quale provvede ogni notte alla copia su nastro degli export full dei database che vengono eseguiti e posizionati in directory del filesystem dei server di produzione. Ciò avviene utilizzando il software di backup centralizzato BrightStor ARCserve Backup ver. 11.5. Quest'ultimo, utilizzando cassette di tipo DLT, provvede anche a fare il backup di basi dati stand-alone gestite da macchine Windows, tramite specifici agenti che colloquiano con i singoli server e vengono copiati direttamente dai filesystem degli stessi.

La maggior parte dei backup, tranne le basi dati della radiodiagnostica, sono gestite senza chiusura del database relativo; ciò ha come svantaggio il fatto che in caso di ripristino si perde la consistenza dell'ultima transazione ma ha il vantaggio di non interrompere l'attività dei client collegati, essendo la maggior parte dei servizi a carattere continuativo. Solo un'istanza (Data Repository) fa uso di sistemi di back up nativi di Oracle (RMAN) i cui file vengono prima appoggiati su disco e poi copiati su nastro.

Il salvataggio delle configurazioni dei cluster per reinstallare tutto il sistema in caso di disaster-recovery viene effettuato ogni qualvolta viene variata una configurazione essenziale del sistema stesso, non utilizzando il software del backup centralizzato ma direttamente il dump del sistema operativo. Tale procedura, posta l'integrità di almeno una copia del supporto, assicura di poter reinstallare i server nel più breve tempo possibile senza necessità di reinstallare l'ambiente di backup. Le cassette sono verificate dopo il dump e custodite in doppia copia nella cassaforte ignifuga. Inoltre, all'inizio di ogni mese viene salvata tramite il software di backup centralizzato il contenuto delle directory di sistema e custodite insieme alle cassette dei salvataggi notturni.

Analisi delle politiche di backup per ogni Base Dati gestita in modo centralizzato

Vediamo ora di dettagliare in maniera analitica per ogni base dati la cadenza del salvataggio ed i fattori di rischio che si possono eventualmente presentare.

Contenuto della base dati	Tipologia di backup	Frequenza di backup/verifica	Ubicazione copie	Struttura incaricata
Dati di analisi patologie e screening	Export su file system del cluster temporizzato da sistema operativo e copia su nastro	Notturna	Libreria /cassaforte ignifuga	SIT
Dati inerenti l'accettazione amministrativa dei ricoveri e relativi DRG	Idem	Idem	Idem	SIT
Accessi al dipartimento di emergenza e medicina d'urgenza	Idem	Idem	Idem	SIT
Turni infermieristici	Idem	Idem	Idem	SIT
Anatomia Patologica	Idem	Idem	Idem	SIT
Assistenza Territoriale	Idem	Idem	Idem	SIT
Anagrafe sanitaria assistiti ASL ed anagrafe dei contatti	Idem	Idem	Idem	SIT
Anagrafe vaccinale	Idem	Idem	Idem	SIT
Prenotazioni per le prestazioni ambulatoriali e visite specialistiche (CUP) e refertazione ambulatoriale	Idem	Idem	Idem	SIT
Dati relativi al registro operatorio	Idem	Idem	Idem	SIT
Scelta e revoca del medico di base e gestione esenzioni	Idem	Idem	Idem	SIT
Gestione archiviazione delle delibere del Direttore Generale e delle determinazioni dei dirigenti	Export su file system per il DB e copia dei dati dal file-server al server di backup via rete interna. Successivamente copia su nastro	Idem	Idem	SIT

Contenuto della base dati	Tipologia di backup	Frequenza di backup/verifica	Ubicazione copie	Struttura incaricata
Gestione apparecchiature elettromedicali	Export su file system della SAN, temporizzato da sistema operativo e successiva copia su nastro	Notturna	Libreria /cassaforte ignifuga	SIT
Gestione economato, magazzini e contabilità analitica	Idem	Idem	Idem	SIT
Archiviazione dati clinici relativi agli episodi di ricovero e di pronto soccorso (data repository aziendale)	Attivato RMAN di Oracle che scrive su filesystem e poi copia su nastro	Idem	Idem	SIT
Archiviazione dati db locale dei middleware di integrazione Spagic e Picasso	Export su file system della SAN, temporizzato da sistema operativo e successiva copia su nastro			
Archiviazione dati analisi di laboratorio	Idem	Idem	Idem	SIT
Registro di protocollo della corrispondenza in entrata e in uscita	Idem	Idem	Idem	SIT
Archiviazione dati indagini radiologiche (RIS)	Copia fisica del DB di Oracle sul file-system e dei files di configurazione. Copia manuale a cura del Sistemista Siemens su supporto magnetico esterno di tipo DAT.	Notturna, con accoramento su file system locale di 3 giorni precedenti.	Sala macchine/cassaforte	Sistemista Siemens
Archiviazione dati immagini radiologiche (PACS) suddivise nel sottosistema IMS (Image Management System) e PDIR (raccolta di anagrafiche paziente)	Tramite appositi script vengono esportati i due DB su file-system con accodamento di più giornate. Copia manuale su DAT a cura Sistemista Siemens	Notturna, con trasferimento su un diverso DAT per il DB IMS e PDIR. Mensilmente vengono copiate due cassette contenenti tutto quanto è necessario al ripristino dei dati entro una settimana in caso di disaster-recovery	Sala macchine/cassaforte	Sistemista Siemens
Dati relativi alla rilevazione oraria	Export su file system del server locale e copia dei dati via rete interna verso la SAN. Successivamente copia su nastro di tipo DLT da parte dell'agente di backup centralizzato	Notturna	Libreria /cassaforte ignifuga	SIT
Gestione cartelle per soggetti tossicodipendenti	Gestito direttamente da agenti del backup centralizzato	Idem	Idem	SIT

Contenuto della base dati	Tipologia di backup	Frequenza di backup/verifica	Ubicazione copie	Struttura incaricata
Raccolta dati dei donatori, virologie e gruppaggio	Idem	Idem	Idem	SIT
Raccolta dati chiamate verso la centrale operativa del 118	Avviene in tre momenti: <ul style="list-style-type: none"> - manutenzione del DB e degli indici con cadenza giornaliera - esportazione dati su file-system ogni sei ore con accodamento dei file in apposita cartella per sette giorni - backup su nastro del contenuto delle cartelle suddette effettuato ogni tre giorni. (LUN-MER-VEN) 	Ogni tre giorni. La cassetta del lunedì mattina viene archiviata in cassaforte ignifuga presso il locale dell'UOSI	Presso centrale operativa 118	Personale della centrale operativa 118
Archivio Dipartimento Prevenzione	Export su file system di un altro server locale. Copia su nastro setti	Ogni giorno	Sala server Pietrasanta/cassaforte	SIT
Archivio attività territoriale	Export su file system del server locale. Contestuale copia su nastro sostituito ogni tre giorni	Ogni giorno	Sala macchine/cassaforte	idem

Miglioramenti futuri:

Tutto l'ambiente di backup centralizzato sarà ristrutturato in modo da implementare un piano di disaster-recovery più organico, compresa la valutazione della possibilità di custodia di copie dei supporti in una sede esterna, misura necessaria per garantire la salvaguardia dei dati in caso evento disastroso che colpisca l'attuale edificio che ospita la sala macchine.

L'ipotesi più probabile è che il Disaster recovery venga gestito in un sito unico per tutte le Aziende dell'Area Vasta Nord Ovest.

Integrità dei dati gestiti direttamente dalle strutture

Per le procedure installate su computer "stand-alone" presso le strutture (ovvero che non sono gestite in modo centralizzato a cura dell'Ufficio Sistema Informativo), sono state, *in parte*, attivate le seguenti misure per l'integrità dei dati:

1. Il responsabile del trattamento, in collaborazione con il personale dell'Ufficio Sistema Informativo e Tecnologie, dovrà mantenere un elenco, da aggiornare con cadenza almeno semestrale, di tutte le attrezzature informatiche dell'Unità Operativa, dello scopo cui sono destinate, della loro locazione fisica, delle misure di sicurezza su esse adottate e delle eventuali misure di adeguamento pianificate.
2. Il responsabile del trattamento individua le aree di disco da sottoporre a backup, sui vari server ed gli eventuali incaricati alla gestione di tale backup;

3. Gli incaricati al backup effettuano le seguenti operazioni:

- esecuzione almeno settimanale del backup, eventualmente attraverso procedure automatiche;
- verifica almeno settimanale della corretta esecuzione dei backup;
- mantenimento di un elenco dei backup effettuati;
- archiviazione dei supporti e distruzione degli stessi in caso di non necessità;
- effettivo ripristino dei dati in caso di necessità.

Integrità dei dati gestiti in ASP

Continua anche nel 2011 l'affidamento in ASP di alcune procedure, su server collocati in server farm esterne all'Azienda. Il servizio offerto dai fornitori prevede l'uso di sistemi ad alta affidabilità in strutture in cui sono garantiti elevati standard di controllo di accesso e sicurezza dell'ambiente.

I fornitori in questione vengono incaricati del trattamento dei dati, al pari di tutti i fornitori di procedure sw. Gli stessi dichiarano di operare nel rispetto delle vigenti disposizioni in materia di protezione di dati personali in base a quanto disposto dal D.L. 196/2003, dando comunicazione al Garante per la Protezione dei Dati Personali.

In particolare, con l'istituzione degli ESTAV, le procedure amministrative gestite da tali Enti (Stipendi del personale e giuridico, gestione magazzino centralizzato, Sovracup) sono collocate presso il Centro Servizi TIX della Regione Toscana. Per queste procedure la responsabilità del trattamento dati non è più delle Aziende Sanitarie ma di Estav.

E' attivo un impianto/sistema di videosorveglianza sul Presidio Ospedaliero Versilia. L'impianto è costituito da n. 6 videoregistratori digitali e circa 70 telecamere. I videoregistratori sono interconnessi tramite rete LAN in fibra ottica dedicata e completamente separata dalla LAN aziendale. Gli apparati sono ubicati in rack posti in locali tecnici a cui ha accesso solo personale autorizzato. I locali tecnici non sono quelli dove sono ubicate le apparecchiature della rete aziendale. Il sistema software gestisce gli accessi al sistema e le relative autenticazioni. La gestione del sistema è completamente affidata alla Ditta vincitrice dell'appalto.

Dal mese di Maggio 2010 è stato attivato il progetto regionale Fascicolo Sanitario Elettronico, analogo ai progetti di Regione Lombardia, Friuli Venezia Giulia, Emilia Romagna.

Riguardo al trattamento dati per tale progetto l'Azienda USL, titolare dei dati, ha nominato tre responsabili esterni, Telecom, HP e Engineering Ingegneria Informatica, che si occupano rispettivamente della infrastruttura tecnologica e del software di gestione del fascicolo. In allegato le nomine.

Sistema di controllo, monitoraggio e politiche di accesso ai dati

E' stato attivato un processo di controllo e verifica della sicurezza del sistema informatico, attraverso l'utilizzo di appositi strumenti a livello di sistema, di gestione delle basi dati e di applicazioni. In particolare, per le basi dati presenti sui server della sala macchine sono attivi i sistemi di controllo e le politiche di accesso meglio specificate in seguito.

Per le basi dati che invece si trovano direttamente presso le varie Unità Operative è in fase di verifica l'attivazione di un sistema di monitoraggio dell'accesso ai dati. Il responsabile del trattamento individuerà uno o più incaricati per la verifica degli accessi.

L'individuazione delle responsabilità connesse a modifiche o letture non autorizzate viene effettuata su richiesta del responsabile del trattamento.

Basi dati in produzione

La maggior parte delle basi dati gestite in modo centralizzato utilizza Oracle versione 10g come sistema di gestione. In massima parte, le basi dati sono direttamente gestite dagli applicativi, con meccanismi di accesso implementati nelle specifiche procedure. L'amministratore configurato su ogni istanza di database è protetto da password ed utilizzato esclusivamente per operazioni di manutenzione del DB e operazioni di backup. L'ambiente di management utilizzato per le suddette operazioni è quello del Sistema Operativo Linux Red Hat, gli accessi sono quindi validati dai meccanismi propri di tale sistema. La maggior parte degli applicativi accede ad Oracle tramite un unico utente con specifica password, in tal caso la procedura stessa si fa carico di memorizzare l'utente applicativo che ha effettuato determinate operazioni. In altri casi invece l'applicativo usa i meccanismi di validazione di Oracle per l'accesso alla procedura stessa. Tramite questi strumenti, è possibile tracciare gli accessi, riusciti e falliti, a livello di sistema, di base dati e di applicativo.

Vengono utilizzati anche altri sistemi di gestione di Base Dati: Lotus Notes, 4Dimension, My SQL. Lotus Notes nel corso dell'anno verrà migrato su Oracle, 4Dimension su SQL Server. Tutti gli accessi a tali sistemi sono gestiti dalle procedure, l'ambiente di management è utilizzato per i salvataggi solo nel caso del database 4Dimension. Negli altri ambienti vengono salvate solo le directory contenenti i files di archiviazione dei dati.

Evoluzioni migliorative:

Con la versione Oracle 10g sarà possibile utilizzare meccanismi di protezione degli accessi più avanzati rispetto agli attuali, disponibili nelle suddette versioni, tipo "Connection Manager", "Advanced Security", "Data Guard", che consentono di specificare dei criteri di accesso molto più selettivi, ad esempio abilitare la specifica postazione client fisica alla connessione allo specifico servizio; criptare una particolare connessione, tipo quelle presso soggetti esterni all'azienda, nonché meccanismi di replica per aumentare la sicurezza in caso di "crash recovery".

Basi dati replicate

Questo paragrafo elenca le basi dati che derivano da elaborazioni a partire dai database in produzione, aggiornati a diverse cadenze temporali e copiati su specifici server.

Database Flussi Ministeriali e regionali: contiene le fonti dati e le elaborazioni per produrre i flussi informativi verso la Regione.

Data warehouse aziendale. Contiene i dati di produzione certificati dell'Azienda che vengono messi a disposizione, per consultazione, ai responsabili delle strutture di tutti i livelli aziendali (Direttore Generale, Direttore Amministrativo, Direttore Sanitario, Responsabili di Area, Direttori di UOC).

Repository Sanitario: contiene i referti (Laboratorio Analisi, Radiologia, Anatomia Patologica, Ambulatoriali) e i documenti sanitari (Verbal di pronto Soccorso, Registro operatorio, Lettere di Dimissione) prodotti all'interno delle strutture della USL, organizzati per utente.

Antivirus centralizzato

E' stato acquistato ed installato un server antivirus per sistemi operativi Microsoft Windows che distribuisce con cadenza giornaliera gli aggiornamenti (reperiti automaticamente dal sito del produttore) delle "firme" dei virus ai Personal Computer client presenti sulla rete aziendale. Ad oggi su circa il 90% dei client effettivamente in rete è stato installato il client Antivirus.

Il software in questione consente anche una gestione centralizzata per bloccare "attacchi" alla rete da parte di malware di tipo Worm, inibendo l'accesso a porte di rete normalmente utilizzate per l'utilizzo quotidiano in una rete aziendale di computer.

E' stato successivamente installato un modulo aggiuntivo Anti Spyware per i client. Sono comunque presenti applicativi AntiSpyware ed AntiSpammer sui server Mail e gateway Internet).

Amministratori di sistema

A partire dal 1° Febbraio 2010, il personale della UOC Sistema Informativo e Tecnologie della USL di Viareggio è stato trasferito in Estav (Ente Tecnico Amministrativo di Area Vasta), unitamente al personale ICT delle altre Aziende Sanitarie dell'Area Vasta Nord Ovest.

Con la designazione (o nomina) di Estav Area Nord-Ovest quale Responsabile Esterno del Trattamento Dati, a tale Ente sono anche attribuiti gli adempimenti richiesti dal Provvedimento a Carattere Generale del Garante in merito alla individuazione degli Amministratori di Sistema.

Il progetto Repository Sanitario

Nel Luglio 2009 all'Ospedale Versilia è stata avviata una consistente informatizzazione dei reparti ospedalieri. I primi moduli software attivati sono stati la gestione delle richieste alle diagnostiche e ai servizi (Order Entry) e il Repository Sanitario.

Il Repository contiene al momento i seguenti documenti sanitari:

Accessi di Pronto Soccorso e Verbali

Accessi di Laboratorio e Referti

Accessi di Anatomia Patologica

Accessi di Radiologia e Referti

Accessi di Ricovero, Referti e Verbali Operatori

Accessi Ambulatoriali e Referti

La logica di accesso al Repository da parte del personale medico è la seguente:

La visualizzazione è consentita ai medici del reparto dove il paziente è ricoverato.

E' consentita ai medici dei reparti dove il paziente viene trasferito nell'ambito dello stesso episodio di ricovero.

E' consentita alla Radiologia nel caso che vengano richieste TAC e Risonanze magnetiche.

La visualizzazione è consentita per un periodo di 30 giorni successivi alla dimissione del paziente.

Accessi ambulatoriali: si pensa di legare la visualizzazione del Repository alle agende CUP degli specialisti, ovvero lo specialista potrà visualizzare il Repository se il paziente è presente nelle agende a cui lo specialista può accedere. Al momento attuale la visualizzazione del Repository legata alle visite ambulatoriali non è attiva, ma la sua realizzazione è prevista nel corso dell'anno.

L'informativa generale sul trattamento dati ed il relativo consenso degli utenti coprono anche le necessità derivanti dall'attivazione del progetto di Fascicolo Sanitario Aziendale.

Il Fascicolo infatti impiega trattamenti dati previsti dalla Legge 196/2003; infatti quando si parla di interconnessione e raffronto come tipologie di trattamento si fa riferimento ad alcuni tipici obiettivi raggiungibili con un fascicolo sanitario elettronico.

In presenza della richiesta del cittadino di non divulgare un particolare documento sanitario questo non verrà inserito nel Repository. In assenza del consenso del cittadino al trattamento dati generico il Repository non verrà attivato.

Sicurezza trasmissioni dei dati

Controllo degli accessi

Tutte le stazioni di lavoro sono protette tramite un nome utente e una password di accesso al Sistema Operativo.

L'inserimento del nome utente e della password di accesso viene effettuato dall'utente stesso a cui sono state impartite le opportune misure da adottare per non lasciare incustodita la postazione di lavoro.

Ai fini dell'assistenza sistemistica da parte di ditte esterne, la password di accesso viene modificata e ripristinata al termine dell'intervento.

La password di accesso va modificata con cadenza semestrale.

Il processo di autenticazione/autorizzazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico. A ciascun profilo è associato un gruppo di utenti, che condividono gli stessi privilegi di accesso e utilizzo.

Il responsabile del trattamento fornisce ai preposti alla custodia delle parole chiave i nominativi e la qualifica degli utenti autorizzati, nonché i loro privilegi di utilizzo del sistema informatico. I preposti provvedono:

- *A definire, per ciascun utente, il nome utente e la password per il primo accesso;*
- *A definire i gruppi necessari per rispettare i privilegi di utilizzo;*
- *A consegnare agli interessati il nome utente e la password, eventualmente assieme ad una copia del manuale interno per la sicurezza predisposto dal Sistema Informativo e Tecnologie.*

Gli applicativi utilizzati per il trattamento sfruttano un loro sistema di autenticazione basato sempre su di un nome utente e una password.

Per gli applicativi che si trovano direttamente presso le varie Unità Operative è in fase di verifica l'attivazione di tale autenticazione per l'accesso ai dati. Il responsabile del trattamento verificherà il sistema di autenticazione/autorizzazione presente. Per gli applicativi che non consentano di automatizzare i controlli di cui sopra va previsto un adeguamento nel breve periodo.

Nome utente e password sono strettamente personali e perciò l'utente viene informato di:

- non comunicare a terzi le password;
- non annotare le password su supporti posti in vicinanza della propria postazione di lavoro, o comunque incustoditi;

Gli amministratori degli applicativi provvedono, con cadenza semestrale, alla verifica degli elenchi degli utenti, e provvedono, previa verifica con il responsabile del trattamento, alla disattivazione delle utenze.

Per gli applicativi che si trovano direttamente presso le varie Unità Operative è in fase di verifica l'attivazione di tale procedura per la verifica della gestione degli utenti.

Con la distribuzione delle Carte Operatore da parte del Servizio Sanitario Regionale (consegne della prima tranche di Carte giugno 2011) utilizzabili per la firma digitale e l'autenticazione sugli applicativi regionali, a livello aziendale l'obiettivo è quello di utilizzarle come Badge per la rilevazione presenze e, nel tempo, come modalità di autenticazione anche sugli applicativi aziendali.

Accesso da parte dei fornitori che prestano assistenza

L'accesso da parte dei fornitori di software/hardware avveniva tradizionalmente attraverso una connessione remota via modem.

Le maggiori necessità di connessione più performanti derivanti dal numero sempre crescente di sw/apparecchiature elettromedicali/hw in Azienda, ci ha portati ad attivare connessioni in modalità VPN.

Per la richiesta di collegamento esiste un modulo firmato attraverso cui il fornitore si impegna anche ad adottare comportamenti corretti in fase di connessione.

Trasmissione dei dati

L'accesso ad Internet dai computer della rete interna viene effettuato tramite un unico punto di accesso ed attraverso un Proxy server che controlla l'accesso dei vari client e che si trova dietro ad un firewall.

Il firewall è configurato in maniera tale da consentire alle postazioni di lavoro interne dell'ufficio di accedere solamente ad alcuni dei servizi disponibili sulla rete, bloccando i tentativi di accesso provenienti dall'esterno verso la rete interna.

Qualora si vogliano rendere disponibili dei servizi interni alla rete Aziendale, sarà necessario richiedere al Responsabile della UOC Sistema Informativo e Tecnologie l'apertura dei canali di comunicazione necessari sul firewall.

Le procedure per la sicurezza delle connessioni sono stabilite dal responsabile del trattamento. Qualora le postazioni pubbliche consentano l'accesso ai dati sensibili occorrerà stabilire rigorose procedure per l'autenticazione degli utenti (firma digitale, personale di presidio alla postazione, o simili). L'utilizzazione dei certificati digitali per la firma con valore legale per il momento è abbastanza ridotta, ma prevediamo che si espanderà rapidamente. Le applicazioni attualmente presenti nella nostra Azienda riguardano la refertazione (Radiologia e Laboratorio Analisi), l'Ufficio Ragioneria per i mandati di pagamento.

Non sono autorizzati collegamenti telematici distinti da quelli previsti ai punti precedenti. In particolare, non sono autorizzate connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio.

Trasmissione dei dati in Regione Toscana

Tra le Aziende Sanitarie e la Regione c'è un intenso scambio di informazioni su varie aree: Attività Sanitarie, Formazione, Residenze per Anziani, etc. Con riferimento agli scambi informativi sono state sviluppate forme di cooperazione organizzativa e tecnologica tra i diversi attori (vedi sistema NAL – NAR).

Allegati

a. Informativa al trattamento dati per il cittadino



informativa PRIVACY

Gentile Signore/a,
l'Azienda USL 12 La informa su come usa i Suoi dati sanitari
(ai sensi dell'art. 13 del D.lgs. n. 196 del 30 giugno 2003 "Codice in materia di protezione dei dati personali")

IDATI SONO UTILIZZATI PER

- Tutelare la salute e l'incolumità fisica
- Condurre ricerche scientifiche e statistiche in forma anonima
- Svolgere gli adempimenti amministrativo-contabili
- Verificare il gradimento dei servizi e delle prestazioni erogate

IDATI RACCOLTI SONO

- Impiegati in modo corretto, nel rispetto del segreto professionale e di ufficio
- Trattati sia manualmente che con procedure informatiche
- Conservati con cura, in ambienti idonei e con adeguate misure di sicurezza
- Comunicati ad altri solo se previsto dalla legge

TITOLARE DEL TRATTAMENTO È

Il Direttore Generale dell'Azienda USL n.12 di Varese

PER TRATTAMENTO SI INTENDE

(art.4 D.lgs.196/03): qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici (raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione o distruzione di dati, anche se non registrati in una banca dati).

MEDIANTE RICHIESTA SCRITTA ALL'UFFICIO RELAZIONI CON IL PUBBLICO (URP) AUSL 12

Lei può esercitare i Suoi diritti (art.7 D.Lgs 196/03) quali:

- conoscere se e come i Suoi dati sono utilizzati
- conoscere il nome del responsabile del trattamento
- conoscere a chi sono comunicati i Suoi dati
- avere ogni ulteriore informazione sul trattamento dei dati

PRESSO L'URP, INOLTRE, LEI PUO'

- presentare eventuali segnalazioni sul mancato rispetto della normativa in tema di "privacy";
- esprimere, su apposito moduli, l'eventuale dissenso al trattamento di tutti o parte dei dati da Lei forniti: in tal caso Lei ricordiamo che il trattamento dei Suoi dati è condizione necessaria per consentire all'Azienda di erogare al meglio i propri servizi.

Indirizzo:
AUSL12 - URP - Via Aurelia 335 - 55041 Lido di Camaiore, (LU) - Numero verde 800.297211 - E-mail: urp@usl12.toscana.it

Rev0