Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 6 "VICENZA"
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050 – COD. U.L.SS. 106 – COD.FISC. E P.IVA 02441500242

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Azienda Sanitaria ULSS 6 "Vicenza"

Versione	Data	Autore	Commenti
01	28/03/2011	Nicolò Salvato	
02	09/01/2015	Roberto Walczer	

Sommario

1. INTRODUZIONE

Allo scopo di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di dati personali nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali essi sono raccolti, l'ULSS Vicenza aveva provveduto ad approvare - con deliberazione 29.12.2000 n. 556 - le "misure minime di sicurezza" ed il "documento programmatico sulla sicurezza" (Allegato 1) in attuazione della legge n. 675/1996, documenti che pure il nuovo "Codice in materia di protezione dei dati personali" approvato con D. Lgs. 30.6.2003 n. 196 - in seguito denominato Codice - contempla al Titolo V e nell'annesso 'Disciplinare tecnico in materia di misure minime di sicurezza' ad esso allegato.

Alla luce delle prescrizioni del nuovo Codice, pertanto, i richiamati documenti hanno costituito oggetto di riesame e raffronto e, rilevata la sostanziale validità degli stessi, si è provveduto a redigere un nuovo Documento Programmatico sulla Sicurezza (DPS) che del precedente costituisce ulteriore specificazione e opportuno aggiornamento senza, peraltro, comportarne l'abrogazione se non per le parti incompatibili: va subito precisato che detta abrogazione deve intendersi senz'altro intervenuta per le figure dell' 'Amministratore di sistema' e del 'Preposto' contemplate dal D.P.R. n. 318/1999, normativa che il nuovo Codice ha espressamente abrogato senza riproporre le figure corrispondenti.

Il presente documento - diversamente da quello precedente, che si allega precisando che gli articoli della legge 675/96 in esso richiamati trovano corrispondente riscontro nelle disposizioni del Codice ora vigente - viene suddiviso in articoli per una più immediata e agevole comprensione.

Si ricorda che l'elenco dei trattamenti di dati sensibili e giudiziari d'interesse dell'ULSS è stato individuato e approvato, come richiesto dall'art. 20 del Codice, con deliberazione del Direttore Generale

2. OGGETTO E FINALITA'

Il Documento Programmatico sulla Sicurezza (DPS) viene redatto dall'ULSS, titolare del trattamento, in attuazione di quanto disposto dagli art. 33, 34, 35, 36 del D. Lgs. 30.6.2003 n. 196 "Codice in materia di protezione dei dati personali" e descrive le modalità tecniche da adottare - a cura del titolare, del responsabile e dell'incaricato - in caso di trattamento dei dati personali con strumenti elettronici.

Il trattamento deve avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, oltre che nel rispetto del principio di necessità.

Esso rientra tra le misure minime di sicurezza elencate dal Codice all'art. 34 e si accompagna ad una serie di altri adempimenti che il medesimo Codice pone a carico dell'azienda, tra i quali:
- la notifica al Garante
- la delibera aziendale per la nomina dei Responsabili del Trattamento e degli Incaricati
- l'approvazione del Regolamento contenente i tipi di dati sensibili e di operazioni eseguibili
- il Piano Formativo.

Il contenuto del DPS è definito nel punto 19 del Disciplinare tecnico allegato B al Codice.

3. ELENCO TRATTAMENTI DEI DATI PERSONALI (19.1)

Il DLgs. 196/03 (art. 4, comma 1) definisce come trattamento di dati qualsiasi operazione effettuata anche senza l'ausilio di strumenti elettronici concernente la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.
L'Azienda Sanitaria ULSS 6 Vicenza tratta per le sue finalità solamente dati personali, sensibili e giudiziari in ottemperanza a quanto previsto dal Codice.
La tabella 1 mette sinteticamente in relazione le strutture dell'Azienda ULSS 6 Vicenza con i tipi di trattamenti effettuati.

Tabella 1. Elenco sintetico dei trattamenti effettuati

Struttura	**Trattamenti effettuati dalla struttura**	**Descrizione dei compiti effettuati dalla struttura**
Medici e Paramedici di: • Distretti • Ospedali • Dipartimenti Personale di segreteria espressamente autorizzato all'intermediazione tra medico e paziente.	Trattamento di dati di tipo sanitario.	Trattamento di dati per esecuzione delle obbligazioni di cui al rapporto di cura e assistenza richiesto. Acquisizione, consultazione, registrazione, aggiornamento dati su cartella clinica cartacea/elettronica. Comunicazione dei dati sanitari a soggetti indicati in consenso di Legge.
Personale amministrativo di: • Distretti • Ospedali • Dipartimenti Servizi amministrativi.	Trattamento di dati di tipo contabile e fiscale di fornitori, persone fisiche e giuridiche, pubbliche amministrazioni, enti e associazioni privati che	Responsabilità di tutte le attività amministrative. Acquisizione, consultazione, registrazione, aggiornamento,

	hanno o hanno avuto in qualche modo rapporti anche economici con l'Azienda.	cancellazione dati contabili e fiscali.
Servizi Amministrativi, Ufficio formazione e aggiornamento professionale; Ufficio qualità Servizio infermieristico.	Trattamento di dati di tipo contabile e fiscale. Trattamento di dati di dipendenti e professionisti associati.	Acquisizione, organizzazione e gestione delle risorse umane ed informative, finanziarie, patrimoniali e materiali.
Servizio per l'Informatica Generale	Trattamento di dati personali di tipo identificativi e sensibili (anche sanitari)	Predisposizione di misure di sicurezza dei dati trattati e conservati su supporti informatici. Salvataggio di dati su supporti informatici. Ripristino di dati su supporti informatici.

4. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' (19.2)

4.1 Titolare del Trattamento

Al Titolare del trattamento spettano le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il Titolare del trattamento dei dati personali contenuti nelle banche dati dell'Azienda Sanitaria ULSS 6 Vicenza è la stessa Azienda Sanitaria ULSS 6 Vicenza.

4.2 Responsabili Interni del Trattamento

Configurandosi l'Azienda ULSS, titolare del trattamento, quale struttura ad elevata complessità sia sotto il profilo organizzativo sia per la varietà di trattamenti, i Responsabili del trattamento sono individuati in numero adeguato e nominati dal Direttore Generale con propria deliberazione, nella quale sono pure specificati i relativi compiti.
La nomina è avvenuta con le allegate deliberazioni 27.3.1998 n. 459, 28.1.1999 n. 68, 27.7.2000 n. 392, 8.5.2001 n. 171, 25.3.2002 n. 92 e 12.8.2005 n. 319.[1]

4.3 Incaricati del Trattamento

Sono Incaricati del trattamento tutti gli operatori di qualsiasi livello e professionalità i quali vengono o possono venire a conoscenza - e quindi effettuano o possono effettuare trattamento in senso lato - di dati anche sensibili in forza del titolo che legittima la loro attività all'interno dell'ULSS (dipendenti e

[1] Ulteriori delibere da citare in relazione ai vari responsabili interni che cambiano causa pensionamenti, licenziamenti, trasferimenti ad altra sede, ecc..

non dipendenti, compresi pertanto consulenti, studenti, allievi, laureandi e specializzandi, tirocinanti, volontari, personale di servizi appaltati – portineria, pulizie, manutenzione, ecc -). La qualificazione di Incaricato e l'ambito del trattamento consentito sono contenuti nei singoli atti che ne legittimano la presenza nelle diverse strutture dell'Azienda.

4.4 Trattamento dei Dati Affidati all'Esterno

Qualora l'Azienda coinvolga nell'espletamento delle proprie funzioni soggetti terzi che si trovino a dover trattare dati riconducibili all'elenco dei trattamenti individuati nello specifico Regolamento, essa procederà alla loro nomina come "Responsabili esterni del trattamento".

In tali ipotesi verrà inserita nel contratto/convenzione un'apposita clausola di garanzia con la quale il soggetto esterno si impegna ad osservare compiutamente quanto disposto in materia di protezione dei dati dal Codice e dalle disposizioni aziendali.

Il Responsabile esterno potrà provvedere all'individuazione di Incaricati con specifica lettera che ne individua i compiti, copia della quale sarà inviata al Servizio dell'ULSS direttamente interessato.

5. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (19.3)

Sulla base delle indicazioni fornite dal Garante, le categorie e gli eventi che possono generare danni sono così elencati:

1. comportamenti degli operatori**:**
   a. sottrazione di credenziali di autenticazione
   b. carenza di consapevolezza, disattenzione o incuria
   c. comportamenti sleali o fraudolenti
   d. errore materiale
2. eventi relativi agli strumenti:
   a. azione di virus informatici o di programmi suscettibili di recare danno
   b. spamming o tecniche di sabotaggio
   c. degrado degli strumenti
   d. accessi esterni non autorizzati
   e. intercettazione di informazioni in rete
3. eventi relativi al contesto fisico-ambientale:
   a. ingressi non autorizzati a locali/aree ad accesso ristretto
   b. sottrazione di strumenti contenenti dati
   c. eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali), nonché dolosi, accidentali o dovuti ad incuria
   d. guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
   e. errori umani nella gestione della sicurezza fisica

Il rischio di evento è poi classificato in quattro possibili valori: 0=trascurabile, 1=basso, 2=medio, 3=elevato. I casi in cui non ha senso rilevare il rischio sono stati indicati come "NP" (Non Pertinente).

La figura cui compete in via principale il monitoraggio dei rischi è il Responsabile del trattamento.

Per ciascuno degli eventi individuati nell'articolo precedente il valore di rischio è così quantificato:
Punto 1.a *sottrazione di credenziali di autenticazione:*
Si è considerato il rischio elevato (=3) laddove gli operatori della singola unità operativa non hanno partecipato al Corso di formazione specifico sul trattamento dei dati e sulla privacy (CPDS). In caso contrario si è ritenuto il rischio trascurabile (=0).
Punto 1.b *carenza di consapevolezza, disattenzione o incuria*
Se il personale della singola unità operativa ha partecipato al CDPS ed è stato redatto il manuale operativo per lo specifico trattamento dei dati (MOT) e sono attive le verifiche campione (VC) attivate dal responsabile del trattamento, il rischio è trascurabile (=0). Nel caso non fossero attivate le VC, il rischio è basso (=1). Nel caso in cui il personale non abbia partecipato al CDPS o non sia redatto il MOT, il rischio è elevato (=3).
Punto 1.c *comportamenti sleali o fraudolenti*
Trattandosi di fattispecie difficilmente definibile e valutabile oggettivamente a priori, l'Azienda si tutela attraverso l'adozione di appropriati strumenti di *audit* concordati, come previsto dalla normativa vigente, con le OO.SS.
Punto 1.d *errore materiale*
Se esiste il MOT il rischio è trascurabile (=0), altrimenti risulta elevato (=3).
Punto 2.a e 2.b *azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio*
In ogni computer collegato in rete è stato installato il software antivirus e antispamming. Tali politiche di sicurezza sono altresì rinforzate a livello di firewall. La situazione è tenuta sotto continuo controllo da parte del Servizio Risorse Informatiche attraverso software di monitoraggio dedicati.
Punto 2.c *degrado degli strumenti*
Le apparecchiature/procedure obsolescenti da non permettere l' adeguata applicazione delle normative sono stati sostituiti.
Punto 2.d *accessi esterni non autorizzati*
La strategia di gestione della sicurezza contro tali eventi prevede il presidio a livello centrale mediante l'utilizzo del firewall e dei software specifici per la gestione e il monitoraggio degli accessi. Non è consentito in Azienda l'utilizzo di modem che non siano quelli installati dal Servizio Informatica o ditte esterne , Responsabile esterni per Nomina, su disposizione del Servizio Informatica. Sotto tali condizioni il rischio è trascurabile.
Punto 2.e *intercettazione di informazioni in rete*
Il rischio è basso per utenti non autorizzati alla connessione agli appartati di rete; alto per operatori che agiscono, per manutenzione, sugli appartati stessi; tuttavia tali operatori rientrano tra i Responsabili e Incaricati individuati negli articoli precedenti.
Punto 3.a *ingressi non autorizzati a locali/aree ad accesso ristretto*

Tale evento si riferisce alle unità operative presso le quali esistono archivi cartacei. Nel caso che la struttura sia protetta mediante sistemi anti-intrusione e il dato sia custodito in archivio sotto chiave, il rischio è trascurabile (=0), altrimenti si ritiene elevato (=3).
Punto 3.b *sottrazione di strumenti contenenti dati*
Se lo strumento ove è custodito il dato è collocato in una struttura protetta mediante sistemi anti-intrusione, o se è riposto all'interno di un armadio blindato, il rischio è trascurabile (=0). In caso contrario il rischio è elevato (=3).
Punto 3.c *eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria*
La sicurezza per tali tipologie di eventi rientra negli ambiti coperti dai *Piani di* Emergenza Aziendali, e nel PIANO DI CONTINUITA' OPERATIVA E DISASTER RECOVERY (Allegato B)
Punto 3.d *guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)*
Se l'ubicazione del server che contiene i dati è la sala macchine del Servizio Informatica e la banca dati è sottoposta al backup centralizzato il rischio è trascurabile (=0). Nel caso di ubicazione diversa in presenza di backup non centralizzato il rischio è basso (=1). Nel caso di ubicazione periferica e in assenza di backup, il rischio è elevato (=3).
Punto 3.e *errori umani nella gestione della sicurezza fisica*
Si rimanda al punto 1.b.

6. MISURE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI (19.4)

Le misure di sicurezza che l'Azienda Sanitaria ULSS 6 Vicenza che ha adottato, sono state scelte con riferimenti a criteri a procedure tecniche, informatiche, organizzative, logistiche e procedurali che configurano il livello standard di protezione richiesto in relazione ai rischi relativi all'art. 31 e segg. del Codice della Privacy rivolti a ridurre i rischi di distruzione o di perdita anche accidentale di dati, accesso non autorizzato, trattamento non consentito o non conforme alla finalità della raccolta.

6.2 Autenticazione procedure

L'accesso degli Incaricati alle banche dati centrali, contenenti dati sensibili, deve avvenire tramite l'uso di un account personale (identificativo utente e password, o tramite SmartCard+ PIN o TOKEN+PIN), con le modalità specifiche di utente di dominio ulssvicenza.intra (LDAP) o dove non fosse possibile con le modalità descritte dalla ditta esterna che gestisce il servizio nella documentazione conservata presso il Servizio per l'Informatica Generale.

6.3 Integrità dei server e degli apparati di rete

Al fine di garantire le adeguate misure di tutela fisica degli apparati sono predisposti la compilazione e l'aggiornamento dei seguenti elenchi:
- elenco dei server (apparati di elaborazione multiutente) e loro rispettiva collocazione;
- elenco degli apparati attivi di rete e loro rispettiva collocazione.

Tali elenchi e la documentazione integrativa fornita dalle ditte esterne che gestiscono il servizio sono disponibili presso il Servizio per l'Informatica generale.

Tutti gli apparati di categoria server – apparati di elaborazione multiutente - dovranno essere collocati in locali che presentino almeno le seguenti caratteristiche di sicurezza:

- *chiusi ad accesso controllato*: l'accesso ai locali nei quali siano ospitati i sistemi di elaborazione o i sistemi di comunicazione dovrà essere interdetto a chiunque, fatta eccezione per il personale autorizzato. Se eventualmente si rendesse necessario l'accesso a detti locali da parte di personale non autorizzato - per es. da parte di tecnici della manutenzione di ditte fornitrici, ecc… -, i visitatori andranno opportunamente identificati e accompagnati durante tutta la loro permanenza in detti locali da personale autorizzato. Deroghe a tale regola potranno essere concesse solo dietro precisa motivazione e andranno comunque segnalate ai responsabili della gestione dei server e/o degli apparati di comunicazione. La regolamentazione degli accessi ai locali e ai server è definita nel documento "Gestione e controllo accesso sale server" presente presso il Servizio per l'Informatica Generale.
- *dotati di alimentazione elettrica tutelata*: dovrà essere garantita presenza di gruppo di continuità in grado di fungere da backup per brevi interruzioni di energia elettrica. Nel caso non sia possibile porre sotto gruppo di continuità l'alimentazione dell'intero locale, potranno essere utilizzati gruppi di continuità singoli per singole macchine; NOTA BENE: il gruppo di continuità – o UPS – dovrà essere predisposto anche nel caso il locale o l'intero fabbricato sia servito da un gruppo elettrogeno – è infatti noto che il gruppo elettrogeno ha dei tempi di attivazione dell'ordine dei 10/15 secondi che non sono compatibili con le esigenze dei sistemi di elaborazione dati e di comunicazione -; la presenza del gruppo elettrogeno potrà comunque essere tenuta presente nel dimensionamento del gruppo di continuità che potrà essere pensato per tamponare solo il breve intervallo di tempo intercorrente fra la caduta della alimentazione di rete e l'entrata in funzione del gruppo elettrogeno;
- *dotati di opportuno condizionamento*: i locali dovranno possedere condizioni idonee di microclima - in termini di temperatura, polverosità, umidità - e nel caso questo non sia garantibile attraverso misure passive, andranno predisposte le adeguate misure attive di condizionamento;
- *dotati di impianto antincendio*: i locali dovranno essere dotati di un adeguato impianto antincendio e possibilmente dovranno essere

monitorati in continuo attraverso sensori per la rilevazione precoce degli aumenti di temperatura e di fumo

Tutti gli apparati attivi di rete andranno collocati in armadi chiusi a chiave che garantiscano le seguenti caratteristiche di microclima:
valori corretti di temperatura;
valori corretti di polverosità;
valori corretti di umidità.

La situazione attuale, che presenta ancora condizioni di minore tutela, sarà valutata e adeguata in sede di approvazione del bilancio di esercizio, sulla base delle proposte che saranno formulate congiuntamente dai Direttori del Servizio per l'Informatica generale ed il Servizio Tecnico patrimoniale.

6.4 Caratteristiche minime dei server

Tutti i sistemi di elaborazione di categoria server in uso in azienda a qualsiasi titolo dovranno presentare le seguenti caratteristiche:
- configurazioni hardware che garantiscano la continuità di servizio (business continuity) tramite elementi critici ridondati in modo da garantire funzionalità di cluster, fail-over o balancing;
- supporti di memoria permanenti e non trasportabili destinati a contenere dati, tutelati da misure di ridondanza con tecniche di RAID;
- dispositivo di backup di adeguate dimensioni e velocità, nel caso non sia implementabile il backup centralizzato aziendale (tale informazione andrà dettagliata nella scheda che accompagna i server aziendali).

È responsabile della messa in atto e della gestione delle opportune tutele hardware dei server il Servizio per l' Informatica Generale

6.5 Ulteriori documenti

In riferimento all'integrità e alla disponibilità dei dati, così come per l'autenticazione e l'accesso agli strumenti informatici aziendali, si faccia riferimento al documento "Regolamento Aziendale per il corretto funzionamento degli strumenti informatici".

7. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI (19.5)

7.1 BACKUP

Al fine di tutelare adeguatamente i dati presenti nei vari sistemi di elaborazione saranno predisposti e resi operativi i necessari piani di backup a cura degli incaricati e dei responsabili del trattamento o delle Ditte esterne che gestiscono i servizi.

7.2 DISASTER RECOVERY

L'Azienda Sanitaria ULSS 6 Vicenza ha predisposto un PIANO DI CONTINUITA' OPERATIVA E DISASTER RECOVERY (Allegato B), che prevede la dislocazione di DataCenter esterni dei sistemi ad alto impatto Aziendale e per rimanenti sistemi interni, da dicembre 2015, un'architettura di sistemi di virtualizzazione in Business Continuity in grado di coprire il 95% dei dati presenti nel SIO (Sistema Informativo Ospedaliero), con l'obiettivo entro giugno 2015 di assicurare tramite idonei sistemi di repliche dati, un DR presso l'Ospedale di Noventa a più di 30 Km di distanza.
La priorità verrà data ai dati ritenuti indispensabili per l'erogazione dei servizi sanitari.
E' inoltre previsto un progetto, più a lungo termine, di business continuity e DR per garantire non solo l'integrità dei dati ma anche la loro disponibilità anche in caso di eventi avversi, in un DataCenter esterno

7.3 GESTIONE DEI GUASTI

Per tutti i trattamenti che occorre tutelare da minacce alla disponibilità si adottano le seguenti misure:
- server: predisposizione di contratti di manutenzione che garantiscano tempi di intervento compatibili con la velocità di ripristino necessaria, o server muletto ;
- client: predisposizione a priori di stazioni di lavoro alternative e di stazioni muletto da usare al bisogno;
- rete di comunicazione – locale e geografica: tutte le linee che sono funzionali all'utilizzo di trattamenti che occorre tutelare da guasti bloccanti devono avere un adeguato backup, gli apparati di rete locale devono essere coperti da contratti di manutenzione che garantiscano un tempo di ripristino adeguato;
È responsabile della formulazione di adeguate politiche di gestione dei guasti il Servizio per l'Informatica generale dell'Azienda.

8. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI (19.6)

La formazione in materia di sicurezza dei dati è dall'Azienda così articolata:
- azioni generali di informazione e formazione sugli aspetti di sicurezza;
- azioni specifiche di informazione e formazione su aspetti di sicurezza propri dei vari ambiti professionali;
- predisposizione di manuali di comportamento e di gestione corretta dei dati;
- pubblicazione in intranet aziendale di una specifica sezione dedicata all'argomento;
Per l'attività di formazione l'Azienda si avvale di Agenzia esterna in base ad apposita convenzione gestita dal Servizio Risorse Umane.

9. TRATTAMENTI AFFIDATI ALL'ESTERNO (19.7)

Nell'atto di nomina, l'Azienda Sanitaria ULSS 6 Vicenza informa il Responsabile esterno circa i compiti che gli sono affidati in relazione a quanto previsto dalla normativa in vigore.

Il Responsabile esterno di impegna a condurre su base periodica, almeno annuale, verifiche in merito all'osservanza della legge e delle istruzioni nelle operazioni di trattamento dei dati personali forniti dall'Azienda.
Il Titolare si riserva la facoltà di verificare l'efficacia delle misure predisposte per la tutela dei dati dal Responsabile esterno.

10. CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI (19.8)

Nelle procedure informatiche del SIO, la riservatezza dei dati sensibili è garantita concedendo, al profilo di ogni utente, solamente i privilegi per accedere ai dati che sono indispensabili per svolgere il suo lavoro.
Per tutte le banche dati importanti ed acquisite da fornitori esterni, al fine di ottemperare a quanto previsto dal codice in materia di protezione dei dati personali, è stato chiesto ad ogni fornitore un adeguamento dei sistemi, qualora non lo fossero, ed una dichiarazione che attestasse la conformità degli stessi a quanto previsto dalla normativa vigente.