

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

redatto in conformità alle disposizioni di cui al
Decreto Legislativo 30 giugno 2003, n° 196

INDICE DEL DOCUMENTO

1. PRESENTAZIONE DEL DOCUMENTO	2
2. SCOPO DEL DOCUMENTO	3
3. CAMPO DI APPLICAZIONE	4
4. ELENCO TRATTAMENTI DI DATI PERSONALI	6
4.1. Elenco dei trattamenti	6
4.2. Definizioni	6
4.3. Elenco trattamenti: informazioni essenziali	8
4.3.1. Elenco dei trattamenti: informazioni essenziali	9
4.4. Infrastruttura di rete	10
5. DISTRIBUZIONE COMPITI E RESPONSABILITA'	13
5.1. Titolare del trattamento	13
5.2. Responsabili del trattamento	13
5.3. Incaricati del trattamento	14
5.4. Strutture preposte ai trattamenti	15
5.4.1. Responsabile aziendale per la Sicurezza	15
5.4.2. Incaricati del trattamento dei dati personali	16
5.4.3. Criteri per i Responsabili di Unità Organizzativa	16
5.4.4. Amministratore di sistema	17
5.4.5. Criteri per i dipendenti incaricati al trattamento	18
5.4.6. Istruzioni per il trattamento dei dati personali comuni	19
5.4.7. Ulteriori istruzioni per il trattamento dei dati personali sensibili e giudiziari	20
5.4.8. Altre tipologie di dati e misure di sicurezza	20
5.4.9. Comunicazione di dati personali	21
5.4.10. Istruzioni per il trattamento dei dati personali comuni	21
5.4.11. Responsabili di direzione	22
6. ANALISI DEI RISCHI	23
6.1. Analisi dei rischi e Vulnerability Assessment	23
6.2. Controlli periodici	23
7. MISURE IN ESSERE E DA ADOTTARE	24
7.1. Misure di Sicurezza	24
7.1.1. Trattamento cartaceo	24
7.1.2. Trattamento informatico (hardware)	25
7.1.3. Organizzazione	25
7.1.4. Sicurezza Fisica Sedi	26
7.1.5. Trattamento Informatico (software)	27
7.2. Strumentazione di sorveglianza	31
7.2.1. Vigilanza	33
7.2.2. Chiusura degli uffici, degli armadi e gestione delle apparecchiature	33
7.2.3. Supporti di memorizzazione	34
7.2.4. Stampe ed archivi cartacei	34
8. CRITERI E PROCEDURE PER IL SALVATAGGIO ED IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI	36
8.1. Backup e restore dei dati	36
8.1.1. Criteri e procedure per il salvataggio ed il ripristino dei dati	36
8.1.2. Ripristino dei dati	37
9. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI	38
9.1. Formazione	38
10. TRATTAMENTI DI DATI AFFIDATI ALL'ESTERNO	39
10.1. Criteri in caso di trattamenti affidati all'esterno	39
10.1.1. Trattamenti affidati all'esterno	41
11. CIFRATURA DEI DATI	43
ALLEGATI	44

1. PRESENTAZIONE DEL DOCUMENTO

Il presente documento costituisce il Documento Programmatico sulla Sicurezza (DPS) predisposto dalla Azienda Sanitaria Locale 1 di Torino 1(d'ora in poi ASL TO1) ed è redatto ai sensi del Decreto Legislativo 30 giugno 2003, N. 196, "Codice in materia di protezione dei dati personali" (di seguito abbreviato in Codice), e dell'Allegato B, "Disciplinare tecnico in materia di misure minime di sicurezza", regola 19 (19.1-19.8) al Codice.

Il DPS è revisionato ed aggiornato con cadenza almeno annuale, a cura del Titolare, a far seguito alla verifica dell'efficacia delle misure di sicurezza previste ed all'adeguamento delle medesime, quando necessario.

2. SCOPO DEL DOCUMENTO

L' Azienda ASL TO1, in qualità di titolare di trattamenti di dati personali sensibili e giudiziari, è tenuta alla redazione del documento in oggetto entro il 31 marzo di ciascun anno e a darne comunicazione nella relazione accompagnatoria al bilancio di esercizio, come richiesto dall'allegato B al D.Lgs.196/03, Regola 19.1.

Il presente DPS è stato redatto secondo le indicazioni riportate nella "Guida operativa per redigere il Documento programmatico sulla sicurezza" diffusa nel giugno 2004 dal Garante per la protezione dei dati personali.

Per ogni regola dell'Allegato B (19.1-19.8), sono allegare una o più tabelle precedute dalla descrizione dei campi che le compongono, oppure i criteri descrittivi per assolvere a quanto stabilito dal decreto.

Il risultato di questo lavoro costituisce il presupposto per le azioni di miglioramento che l' Azienda intende svolgere nel corso del prossimo periodo, in aggiunta alle seguenti linee guida già definite e perseguite:

- formazione mirata alla diffusione dei principi e degli adempimenti prescritti dal Codice in materia di protezione dei dati personali (D.Lgs.196/2003) all'interno dell'Ente;
- costante adeguamento dell'infrastruttura informatica e logistica;
- aggiornamento ed adeguamento delle prassi organizzative.

Il trattamento dei dati personali di cui ASL TO1 è Titolare avviene nel rispetto e a garanzia dei seguenti principi:

- integrità dei dati: intesa come tutela dell'accuratezza e completezza delle informazioni, la salvaguardia della esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate;
- confidenzialità dei dati: intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate;
- disponibilità dei dati: intesa come assicurazione che l'accesso ai dati sia disponibile solo quando necessario, a garanzia per gli utenti della fruibilità dei dati e dei servizi, evitandone la perdita.

3. CAMPO DI APPLICAZIONE

Il presente documento si applica a tutti i trattamenti di dati personali comuni e sensibili/ giudiziari effettuati da ASL TO1, in tutte le aree fisiche occupate.

Le sedi sul territorio regionale sono così articolate:

Sedi dell'Azienda Sanitaria Locale TO1 di Torino
Via Agliè, 6
Via Alassio, 36 E
Via Avigliana, 13
Via Baretto, 36 Bis
Via Bellono, 1
Via Berutti e Ferrero, 3
Via Bertani, 80
Via Biscarra, 12/10
Via Monsignore, 1 D
Via Boston 152
Via Candiolo, 79
Via Carrera, 6
Via dellaConsolata, 10
C.so Corsica, 55
Via De Gasperi, 6
Via Donatore Sanguè, 3
Via Dorè, 4
Via Farinelli, 25
Via Farinelli, 40/1
Via Germagnano, 48
Via Ghedini, 19/31
C.so Giambone, 63
Via Gradisca, 10
Via Juvarra, 19
C.so Lecce, 25
Via Lombroso, 16
Via Madama Cristina, 76
Via Mazzini, 20
C.so Mediterraneo, 74
Via Monginevro, 130
Via Monte Ortigara, 95



A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

Via Montevideo, 21
Via Montevideo, 45
Via Moretta, 55
Via dei Mughetti, 12
Via Negarville, 8/28
Via Nizza, 138
Via Nizza, 17
Via Nuoro, 31
Via Ormea, 85
Via Parella, 6/35
Via Petitti, 24
Via Plava, 75
Via Poma, 2
Via Porta Palatina, 4
Via Pr. Tommaso, 4
C.so Racconigi, 96
Via Sabaudia, 64 - Grugliasco
Via Saluzzo, 101
C.so Salvemini, 25/15-16
Via S. Domenico, 34
Via S. Marino, 10
Via S. Secondo, 16
Via S. Secondo, 29
Via S. Secondo, 42
Via Santa Giulia, 11
Via Servasi, 92
Via Sidoli, 18
Via Silvio Pellico, 17
Via Silvio Pellico, 19
Via Spalato, 14
Via Spalato, 15
Via Tarocco, 6
Via Tofane, 71
C.so Unione Sovietica, 220
Via Vassalli Eandi, 18
Via Ventimiglia, 112
Via Ventimiglia, 76
C.so Vercelli, 15
Via Vigevano, 46

4. ELENCO TRATTAMENTI DI DATI PERSONALI

(Codice, Allegato B, regola 19.1)

4.1. Elenco dei trattamenti

Questa sezione riporta l'elenco dei trattamenti effettuati da ASL TO1, così come previsto dalla regola 19.1 (elenco dei trattamenti di dati personali) dell'Allegato B al Codice.

L'elenco dei trattamenti fornisce una visione esaustiva di tutti i trattamenti effettuati dall'Ente e permette di identificare chiaramente quelli che richiedono livelli di protezione più alti a causa della natura sensibile dei dati trattati.

4.2. Definizioni

Sono di seguito riportate alcune definizioni stabilite dal Codice, rilevanti ai fini della stesura del presente documento.

Ai sensi del D.Lgs.196/03, si intende per:

- trattamento, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti 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 di dati, anche se non registrati in una banca di dati;
- dato personale, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- dati identificativi, i dati personali che permettono l'identificazione diretta dell'interessato;
- dati sensibili, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- dati giudiziari, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- titolare, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti

utilizzati, ivi compreso il profilo della sicurezza;

- responsabile, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- incaricati, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- interessato, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- comunicazione, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- dato anonimo, il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- banca di dati, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- comunicazione elettronica, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- reti di comunicazione elettronica, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- rete pubblica di comunicazioni, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- misure minime, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

4.3. Elenco dei trattamenti: informazioni essenziali

Nella tabella "Elenco dei trattamenti: informazioni essenziali" sono riportate le informazioni con significato di seguito descritto:

Descrizione sintetica del trattamento: descrive il trattamento attraverso l'indicazione della sua denominazione e della finalità perseguita (ad esempio, fornitura di beni o servizi, gestione del personale, ecc.);

Tipologia dati trattati: indica se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ai dati personali comuni (**P**: dati personali comuni; **S**: dati personali sensibili; **G**: dati personali giudiziari);

Natura del trattamento: indica se il trattamento è svolto su supporto cartaceo (archivio cartaceo) e/o con strumenti informatici (applicativo informatico, strumento office e così via);

Struttura di riferimento: indica la struttura all'interno della quale viene effettuato il trattamento;

Altre strutture che concorrono al trattamento (anche esterne): nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture, è indicato oltre a quella che primariamente detiene la responsabilità dell'attività, anche quelle che concorrono, siano esse interne od esterne all'organizzazione del titolare;

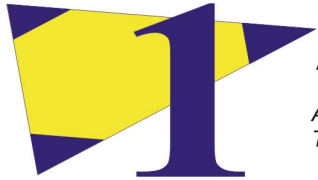
Tipologia dispositivi d'accesso ed interconnessione: elenco, rispettivamente, degli strumenti utilizzati per effettuare il trattamento (pc, palmare, ecc) e della rete che collega i dispositivi d'accesso ai dati (rete locale, Internet, ecc).

4.3.1. Elenco trattamenti: informazioni essenziali

L'elenco dei trattamenti: informazioni essenziali è visionabile sul sito aziendale www.aslto1.it nell'area riservata all'informativa privacy sotto la voce– "Elenco trattamenti"

4.4. INFRASTRUTTURA DI RETE

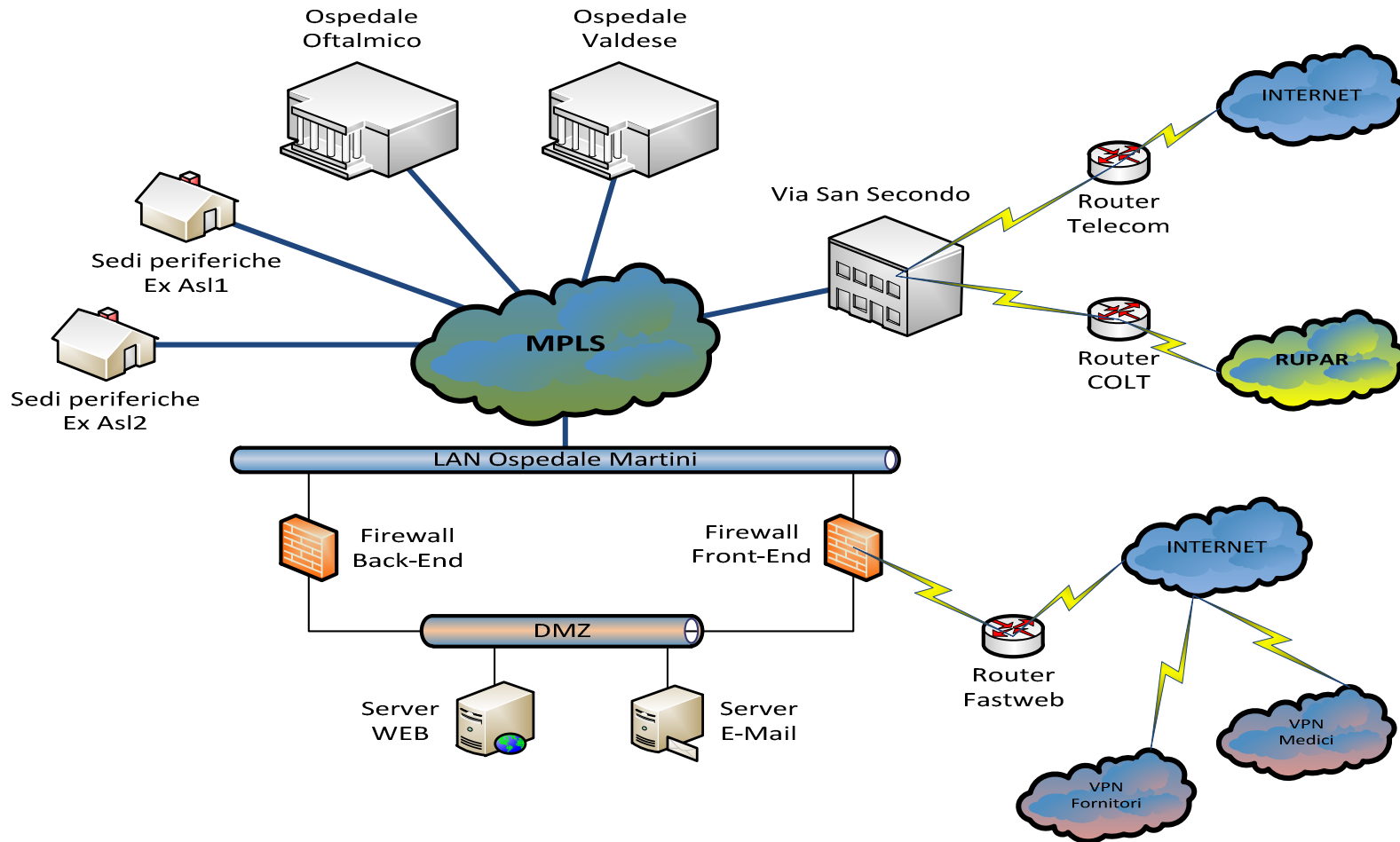
La rete dell' ASL TO1 è costituita da Internet, RUPAR e intranet locale secondo lo schema riportato qui di seguito:



A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**



Si evidenziano 2 livelli di firewalling, un nodo di comunicazione RUPAR, sistemi antivirus centralizzati e uno sbocco verso sedi ex ASL 1 e ex ASL2.

Come evidenziato nello schema precedente l'architettura di rete attraverso la quale vengono interconnessi i server delle varie sedi comprende:

- Un livello di firewalling di "front end". Il firewall è un componente di difesa perimetrale che normalmente collega due o più tronconi di rete, operando un filtraggio sul traffico transitante nei due sensi.
- Una DMZ (demilitarized zone), ovvero uno spezzone di rete che fornisce alla Intranet i servizi che necessitano di accesso verso Internet (web server, email server, ...)
- Un livello di firewalling di "back end", posto a protezione degli apparati server e di immagazzinamento dati (DB).

Ai dispositivi elencati si aggiungono:

- Antivirus centralizzati per servizi email (McAfee)
- Applicativi di gestione degli antivirus per postazioni client (McAfee ePolicy Orchestrator).

Le VPN sedi esterne e ditte esterne arrivano tramite Internet e terminano sul firewall di back end, mentre il firewall di front end è il terminatore della VPN medici.

Attacati alla LAN troviamo la WAN ex ASL 2 (sedi esterne collegate direttamente con linee Fastweb), la WAN con Via San Secondo.

5. DISTRIBUZIONE COMPITI E RESPONSABILITA'

(Codice, Allegato B, regola 19.2)

5.1. Titolare del trattamento

Titolare del trattamento dei dati personali è la ASL TO1, nella persona del Commissario in qualità di Legale Rappresentante pro-tempore, domiciliato per la carica presso la sede legale dell' Azienda in via San Secondo, 29 Torino, il quale si avvale operativamente del Gruppo aziendale per la Privacy .

Ai sensi dell' art. 4 primo comma, lettera f) del D.Lgs. 196/03, il Titolare del trattamento dei dati personali è *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza"*.

L' art. 28 D.Lgs. 196/03 dispone inoltre che *"quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l' entità nel suo complesso o l' unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza"*.

In particolare, oltre quanto più in generale disposto dal Codice, il Titolare del trattamento dei dati personali, ha il compito di:

- definire le politiche e le modalità organizzative attraverso cui rendere effettivi i principi fissati dal Codice
- redigere, anche attraverso un responsabile designato, entro il 31 marzo di ogni anno, il documento programmatico sulla sicurezza
- riferire, nella relazione accompagnatoria del bilancio d' esercizio, se dovuta, dell' avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza
- nominare eventualmente i Responsabili del trattamento, ai sensi dell' art. 29 del Codice

5.2. Responsabili del trattamento

Ai sensi dell' art. 4 primo comma, lettera g) del D.Lgs. 196/03, Responsabile è *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali"*.

L' art. 29 D.Lgs. 196/03 dispone che:

- *“Il responsabile è designato dal titolare facoltativamente.*
- *Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.*
- *Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.*
- *I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.*
- *Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni”.*

Il Responsabile del trattamento dei dati personali ha il compito di:

- provvedere a nominare per iscritto gli “Incaricati” al trattamento dei dati personali comuni e sensibili/giudiziari;
- individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli “Amministratori di Sistema” e il custode delle chiavi d’ accesso ai locali ed armadi;
- redigere ed aggiornare, ad ogni variazione, l’ elenco degli strumenti elettronici, nonché l’ elenco delle tipologie dei trattamenti effettuati;
- in caso di trattamento di dati personali con strumenti elettronici, attribuire, con l’ ausilio degli “Amministratori di Sistema”, un “Codice identificativo personale” (USER-ID) ad ogni Incaricato al trattamento dei dati personali, codice che deve essere associato univocamente all’ addetto e non riutilizzabile;
- garantire, più in generale, che tutte le misure di sicurezza riguardanti i dati personali siano applicate, anche qualora siano affidate a terzi quali Responsabili del Trattamento tutte o parte delle attività di trattamento;
- informare prontamente il Titolare nella eventualità che si siano rilevati rischi che incombono sui dati.

L’ elenco completo dei Responsabili del Trattamento dell’ ASL TO1 è visionabile sul sito aziendale www.aslto1.it nell’ area riservata all’ informativa privacy sotto la voce “elenco Responsabili dei Trattamenti”

5.3. Incaricati del trattamento

I responsabili del trattamento dell’ ASL TO1 provvedono a nominare gli incaricati del trattamento dei dati personali.

Ai sensi dell’ art.4 primo comma, lettera h) del D.Lgs 196/03, sono incaricati le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;

L’ art. 30 del Codice dispone che:

“le operazioni di trattamento possono essere effettuate solo da incaricati che operano

sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite; la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima”.

Agli incaricati sono attribuiti livelli d'accesso differenziati, sulla base del ruolo professionale ricoperto. Tale differenziazione degli accessi è garantita dal sistema di autenticazione e dal sistema di autorizzazione.

Il Responsabile impartisce le istruzioni necessarie a garantire la segretezza e la robustezza della componente riservata delle credenziali d'autenticazione.

5.4. Strutture preposte ai trattamenti

Questa sezione descrive sinteticamente l'organizzazione della struttura dell'Ente, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

5.4.1. Responsabile aziendale per la Sicurezza

Il Responsabile Aziendale della Sicurezza e del Trattamento Dati riferisce al Commissario ed ha i seguenti compiti e responsabilità:

- **rispondere dei Trattamenti dei dati personali ai sensi di quanto previsto all'art. 29 del D.lgs. 196/2003**
- garantire opportuno profilo di Sicurezza ai Trattamenti di dati personali e a tutti i servizi svolti in ASL TO1, riducendo al minimo, mediante idonee e preventive misure di sicurezza, secondo i perfezionamenti tecnici offerti dalle tecnologie correnti, i rischi di distruzione o perdita anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- rispondere agli interessati secondo quanto previsto dall'art. 7 del D.lgs. 196/2003;
- vigilare sull'osservanza delle disposizioni trasmesse agli incaricati;
- proporre le linee guida della Sicurezza alla Direzione Generale;
- promuovere lo sviluppo, la realizzazione ed il mantenimento delle linee guida di sicurezza definite;
- informare il Direttore sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- promuovere e garantire l'esecuzione di programmi di audit;

5.4.2. Incaricati del trattamento dei dati personali

Incaricato – è la persona fisica che, nell' ambito del trattamento dei dati, è tenuto a svolgere le sue attività secondo le istruzioni ricevute dal Titolare o dal Responsabile del Trattamento.

Tutti i dipendenti (compreso il personale esterno es. consulenti) dell' ASL TO1 sono incaricati del trattamento di dati personali con comunicazione sottoscritta dal Responsabile per il trattamento dei dati personali (copia della comunicazione controfirmata dal dipendente è custodita dall' Azienda)

La sussistenza della nomina e delle relative istruzioni deve essere verificata puntualmente dai Responsabili dell' area organizzativa a cui tali risorse umane sono destinate. con particolare attenzione verso le persone destinate a svolgere attività di amministratore di sistema.

Gli incaricati devono salvaguardare i Trattamenti di competenza dei seguenti Rischi:

- Distruzione/perdita dei dati;
- Accesso non autorizzato
- Trattamento non consentito o non conforme alle finalità della raccolta.

E' prescritta a tutto il Personale incaricato dello svolgimento di Trattamenti dati l' adozione delle misure di sicurezza riportate all' Allegato B del D.Lgs. 196/03

Ciò premesso si prosegue più specificatamente proprio sull' osservanza dei criteri richiesti da tale decreto.

5.4.3. Criteri per i Responsabili di Unità Organizzativa

Ogni responsabile di U.O., deve provvedere a verificare che i trattamenti effettuati sui dati personali rispettino le modalità esposte nel presente documento.

In particolare il D.Lgs. 196/03, richiede che i dati personali siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- esatti ed aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o trattati;

- conservati in forma che consenta l' identificazione dell' interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o trattati.

Circa le misure minime riportate nell' allegato B del D.Lgs. 196/03, presso ciascuna area i responsabili devono in particolare:

- vigilare affinché le parole chiave ed i codici identificativi personali dei dipendenti, degli interinali, tirocinanti, consulenti siano disattivati nel caso in cui i medesimi collaboratori non siano più in forza presso l' Azienda.
- aggiornare, quando occorra, e comunque almeno annualmente, il profilo delle autorizzazioni all' accesso a disposizione di ciascun collaboratore (dipendente o esterno)
- aver garanzia circa l' esecuzione effettiva dei back-up dei dati personali se mantenuti in modo esclusivo presso gli Hard-Disk dei PC dell' ufficio (non già nei server che usufruiscono di salvataggi centralizzati).
- integrare, ove il caso lo richiedesse, le istruzioni nel seguito riportate con altre indicazioni a seconda delle attività svolte e delle competenze di collaboratori dipendenti, consulenti ed interinali al fine di osservare e fare osservare le disposizioni del D.Lgs. 196/03.

Nella esecuzione delle attività di trattamento, occorre seguire criteri specifici per ciascuna tipologia di dati che tengano conto:

1. gli aspetti di Legge che possono regolarmente l' uso di questi oggetti (ad es. il Codice in materia di protezione dei dati personali D.Lgs. 196/03);
2. le circolari/regolamenti interni aziendali;

Infine, qualora presso l' area vengano svolte attività di apertura, chiusura o modifica di credenziali di accesso (amministrazione di sistema) o si provveda alla custodia di password occorre seguire le istruzioni relative riportate a par. 5.4.4

5.4.4. Amministratore di sistema

Amministratore di sistema è l' incaricato che sovrintende le operazioni di apertura, chiusura, modifica dei codici di accesso ai sistemi operativi, alle procedure applicative e alle banche dati.

In altre parole, è la persona che ha la possibilità di attribuire, revocare o modificare credenziali di accesso e/o i profili di utilizzo associati a tali credenziali, intervenendo direttamente sui sistemi informatici.

E' responsabilità dell' Amministrazione di Sistema (sia esso di sistema operativo, data-base o procedura applicativa) verificare con periodicità almeno annua la ragion d' essere delle chiavi di accesso assegnate chiudendo d' ufficio quelle

relative a personale dimesso, trasferito ecc.

L'attività di **amministrazione di sistema** comprende:

- l'assegnazione e la gestione di codici personali in modo che ne sia prevista la disattivazione sia in caso di perdita della qualità che ne consentiva l'accesso all'elaboratore sia in caso di mancato utilizzo dei medesimi;
- l'associazione delle credenziali ad opportuni e giustificati profili di utilizzo coerente con le mansioni dell'utente;
- il sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati ed al loro utilizzo, attenendosi ai criteri previsti dalla normativa vigente sulla tutela dei dati personali e sulle misure di sicurezza ed altresì ai regolamenti e alle modalità tecniche adottate dall'azienda per la creazione, la modifica, l'inserimento ecc. dei dati personali;

Il Provvedimento del Garante per la protezione dei dati personali pubblicato sulla Gazzetta Ufficiale n. 300 del 24 Dicembre 2008, ha stabilito che tutte le Aziende pubbliche e private hanno l'obbligo di registrare e conservare i dati relativi agli accessi degli Amministratori di Sistema, al fine di agevolare la "verifica delle loro attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici".

Per ottemperare al provvedimento del Garante della Privacy, l'ASL TO1 ha provveduto a dotarsi di un sistema di Log Management in grado di tracciare con modalità automatiche gli accessi degli operatori ai dispositivi e alle applicazioni che gestiscono.

Il Log Management conserva i dati in maniera sicura per un periodo minimo di sei mesi e può essere consultabile dall'Azienda e dalle Autorità preposte.

5.4.5. Criteri per i dipendenti incaricati al trattamento

Per ciascun incaricato, finalità e modalità di trattamento devono essere unicamente quelle connesse alle mansioni assegnate e comunque congruenti con quanto specificato nel presente documento.

L'incaricato è responsabile dell'integrità, rintracciabilità, e riservatezza dei dati cui ha accesso.

Deve adottare tutte le misure opportune, come da istruzioni, al fine di prevenire la diffusione di "virus", le intrusioni di esterni o lo smarrimento dei dati.

L'incaricato, specie nell'ambito di trattamento dei dati sensibili, deve attenersi rigorosamente alle finalità ed alle modalità approvate dalla Direzione responsabile dello specifico servizio, ricordando costantemente quanto disposto dal Codice in merito alle misure di sicurezza relative al Trattamento di dati personali.

Di seguito, si riportano istruzioni specifiche per le varie tipologie di dati formulate sia riprendendo le prescrizioni di legge fondamentali sia ricordando le precauzioni d'obbligo

più ovvie e le vigenti disposizioni aziendali.

5.4.6. Istruzioni per il trattamento dei dati personali comuni

I dipendenti, gli interinali e i consulenti svolgeranno le **sole operazioni** di trattamento e/o manutenzione **necessarie, pertinenti e non eccedenti** in relazione alle finalità e modalità perseguite dalla Direzione di appartenenza ed alle mansioni assegnate dal Responsabile della struttura.

Le operazioni di trattamento dei dati affidate loro dovranno essere eseguite con la massima diligenza applicando quanto qui di seguito richiamato:

- i supporti cartacei e/o informatici, contenenti dati personali e le loro copie, devono essere custoditi in archivi chiusi a chiave;
- per l'accesso ai dati personali contenuti in banche dati informatiche presenti su elaboratori accessibili in rete è necessario utilizzare un codice identificativo personale (user-id, login ecc.) univoco e non precedentemente utilizzato da altri incaricati o utenti;
- la password obbligatoria in accompagnamento al codice identificativo deve avere le caratteristiche riportate nell'allegato B al D.Lgs. 19/603;
- in caso di allontanamento, anche temporaneo dalla stazione di lavoro (PC), non lasciare il sistema operativo aperto con la propria password inserita in modo da evitare che persone estranee effettuino trattamenti non permessi;
- copie e riproduzioni di dati personali su supporti amovibili sono permesse solo se costituiscono parte del trattamento;
- non disattivare i programmi antivirus installati sul proprio elaboratore, salvo temporaneamente ed in casi di necessità dettati da manutenzione, particolari e limitate elaborazioni o simili;
- se il trattamento di dati concerne la loro raccolta, informare oralmente o per iscritto gli interessati ai sensi dell'art. 13 del D.Lgs. 196/2003, salvo che l'informativa medesima sia già stata fornita direttamente dal Titolare ed, inoltre, raccogliere il consenso scritto degli interessati, salvo che questo sia escluso ai sensi dello stesso decreto o comunque vi abbia già provveduto il Titolare;
- garantire la riservatezza sui dati personali dei quali si abbia conoscenza nello svolgimento del proprio incarico ed anche successivamente al termine dello stesso;
- in caso in cui si constatino situazioni non conformi alle prescrizioni in materia di sicurezza e di protezione dei dati personali, comunicarle immediatamente al Responsabile del trattamento dei dati;

5.4.7. Ulteriori istruzioni per il trattamento dei dati personali sensibili e giudiziari

Per ciascun incaricato o per gruppi di incaricati l' eventuale accesso a dati sensibili e giudiziari deve essere noto al proprio responsabile e da questi autorizzato mediante l' attribuzione di uno specifico e aggiornato profilo organizzativo ed informatico di trattamento di tali dati. All' incaricato deve essere noto, in aggiunta alle disponibilità pratiche ed accessi, l' ambito delle sue mansioni, limiti e caratteristiche di interazione con le informazioni ad elevata criticità.

Nell' ambito del trattamento di dati sensibili o giudiziari i dipendenti, gli interinali ed i consulenti devono applicare le seguenti istruzioni (**aggiuntive** rispetto a quelle già esposte a par. 5.4.4 che regolano il trattamento di dati personali comuni):

- custodire i supporti cartacei e/o informatici contenenti dati personali sensibili e giudiziari e le loro copie in contenitori muniti di serratura la cui chiave è messa a disposizione, da parte del Responsabile, all' incaricato/i specificatamente autorizzato per le sole operazioni di trattamento affidate;
- l' accesso agli archivi fuori dell' orario usuale deve essere noto al Responsabile della struttura e da questi approvato;
- per le banche dati informatiche contenenti dati sensibili e/o giudiziari utilizzare unicamente il codice di accesso assegnato, evitando anche di operare contemporaneamente su più stazioni di lavoro mediante un medesimo codice di accesso;

Occorre, in generale, adottare ogni accortezza per evitare rischi di divulgazione delle informazioni nell' ambito di attività di trattamento dei dati sensibili e/o giudiziari.

5.4.8. Altre tipologie di dati e misure di sicurezza

Oltre ai dati di cui sopra (dati personali comuni e dati personali sensibili/giudiziari), possono essere oggetto di autonoma classificazione i dati riservati.

Per dato riservato deve intendersi quella categoria di dati che, in origine o a seguito di trattamento, può essere divulgata esclusivamente ad un numero predefinito ed identificato di soggetti.

Il dato riservato può rivestire anche la qualifica di dato personale o, al contrario non essere associabile, neanche indirettamente, a nessuna persona fisica o giuridica.

Si tratta infatti di una classificazione non individuabile in assoluto né identificabile in base a prescrizioni di legge, ma lasciata alla discrezionalità e all'autonomia decisionale delle diverse strutture aziendali.

Sarà cura di ciascuna direzione individuare i dati aziendali riservati di propria competenza e le istruzioni da impartire ai collaboratori che li trattano.

5.4.9. Comunicazione di dati personali

La comunicazione di dati personali all' interno dell' ASL TO1 (quindi da incaricato a incaricato) può avvenire solamente nell' ambito delle mansioni attribuite e secondo criteri di necessità ed indispensabilità.

Comunicazioni di dati al di fuori dell' ASL TO1:

- la comunicazione dei dati al di fuori dell' ASL TO1 è **vietata** senza specifica autorizzazione;
- la trasmissione e la comunicazione di dati "dati personali, sensibili e giudiziari" mediante posta, all' interno o all' esterno dell' ASL TO1, dovrà avvenire sempre mediante supporti (cartacei, magnetici...) confezionati in buste o pacchi chiusi.
- per i dati sensibili e giudiziari la comunicazione all' interno dell' ASL TO1 è ammessa solo se rigorosamente attinente e necessaria al corretto svolgimento del trattamento.

La comunicazione di credenziali e password deve seguire prassi adeguate e sicure, in modo che tali strumenti non possano essere utilizzati illegittimamente.

Le password in particolare possono essere rese note unicamente al destinatario e non a terzi.

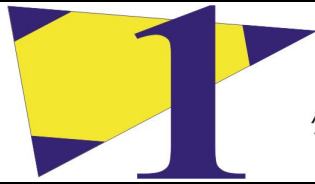
5.4.10. Istruzioni per il trattamento dei dati personali comuni

Secondo quanto prescritto dalla *Legge sul Diritto d' Autore n. 633/41 e s.m.i.* **copiare o utilizzare un software senza regolare licenza è reato.**

E' quindi vietato esplicitamente a dipendenti e collaboratori di installare e fare uso di prodotti software acquisiti senza licenza ovvero di acquisire qualsiasi prodotto in modo non autorizzato ricordando che la non osservanza di ciò comporta per l' autore del fatto la responsabilità personale e diretta relativa sia a quanto sopra esposto sia per le conseguenze derivanti (es. introduzione di VIRUS nelle procedure aziendali).

L' uso diligente degli strumenti di lavoro assegnati (con particolare riferimento all' uso di Internet e degli strumenti di posta elettronica) è strettamente finalizzato e limitato alle attività di competenza.

E' inoltre richiesta una gestione scrupolosa di tali strumenti evitando la comunicazione ad altri delle proprie password ed utilizzando, nel caso di accesso e gestione di dati od informazioni riservate, tutte le misure a completamento, come ad es.: l' uso della chiave hardware, scollegamento durante le assenze anche temporanee, chiusura dell' ufficio in assenza di presidio.



A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

Qualsiasi possibilità consentita dalle autorizzazioni di accesso ricevute, va sempre utilizzata per finalità strettamente limitate all' assegnatario: tali autorizzazioni non devono essere utilizzate per consentire l' accesso a terzi (non parimenti autorizzati).

Si raccomanda anche di evitare di lasciare incustodite stampe relative a dati riservati o personali: occorre soprattutto fare attenzione a quanto si lascia esposto sulla propria scrivania.

I raccoglitori con documenti cartacei contenenti dati riservati o personali devono essere riposti, dopo il loro utilizzo, in armadi chiusi.

Al termine dell' orario di lavoro il dipendente, nell' abbandonare il proprio posto di lavoro, deve lasciare la scrivania sgombra e con tutti i cassetti/armadi chiusi a chiave.

E' inoltre vietato trasmettere o trasportare senza autorizzazione esplicita all' esterno dell' Azienda prodotti e risultati del lavoro svolto all' interno del rapporto di collaborazione prestato; il D.Lgs. 518/92 all' art. 3 specifica che: *“qualora un programma per elaboratore sia creato dal lavoratore dipendente nell' esecuzione delle sue mansioni o su istruzioni impartite dal suo datore di lavoro, questi è titolare dei diritti esclusivi di utilizzazione economica del programma creato”*. è pertanto fatto divieto di accedere od usare o diffondere applicazioni o dati ed informazioni in contrasto con le istruzioni di lavoro e gli incarichi ricevuti.

5.4.11. Responsabili di direzione

I Responsabili delle S.C., S.S., S.S.D. dell' ASL TO1 assicurano che le operazioni di loro competenza avvengono in modo conforme alle prescrizioni del presente documento in modo particolare per quanto riguarda le leggi e le norme citate.

Essi, nell' ambito della propria organizzazione, opereranno anche in modo da contribuire all' opportuna diffusione ed al controllo di quanto qui riportato.

6. ANALISI DEI RISCHI

(Codice, Allegato B, regola 19.3)

6.1.1. Analisi dei rischi e Vulnerability Assessment

L'analisi dei rischi ha come obiettivo l'individuazione degli eventi potenzialmente dannosi per la sicurezza dei dati, la valutazione della gravità, delle possibili conseguenze e la pianificazione delle misure di sicurezza adeguate e disponibili allo stato dell'arte.

6.1.2. Controlli periodici

Periodicamente, ovvero con tempistiche correlate alla esecuzione delle sessioni di analisi dei rischi, verranno effettuate le seguenti attività:

- Verifica dell'applicazione delle misure minime;
- Verifica della coerenza di ogni profilo di accesso al sistema, con autorizzazione ad accedere ai soli dati la cui conoscenza sia necessaria per l'espletamento delle mansioni assegnate;
- Verifica delle procedure a protezione degli archivi anche cartacei;

7. MISURE IN ESSERE E DA ADOTTARE

(Codice, Allegato B, regola 19.4)


7.1. Misure di sicurezza

Nelle tabelle seguenti sono riportate le misure che sono state individuate per contrastare i rischi evidenziati nell' Analisi dei Rischi: tutto il Personale dell' Azienda è tenuto, ove applicabile, all' adozione delle misure sotto riportate a protezione dei trattamenti di dati Personali.

Segue la legenda che riporta la descrizione dei codici delle minacce contrastate.

7.1.1. Trattamento cartaceo

Misure di sicurezza	Stato attuale	Minaccia contrastata
E' fissato il periodo di conservazione dei documenti cartacei	Adottata	G23
L'archivio cartaceo è custodito in arredi chiusi a chiave	Adottata	G17, G19, G20, G22,
Gli arredi contenenti l'archivio cartaceo sono a loro volta posti in locali chiusi a chiave	Adottata	G17; G19; G20; G21
Esistono dei referenti che detengono le chiavi di accesso al materiale cartaceo conservato	Adottata	G15; G16; G17; G19
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	Adottata	G23
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Adottata	G23
La validità delle richieste di accesso ai dati è verificata prima di consentire l'accesso stesso	Adottata	G19
Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate	Adottata	G19, G23

 <p>A.S.L. TO1 Azienda Sanitaria Locale Torino</p>	<p align="center">DOCUMENTO PROGRAMMATICO SULLA SICUREZZA</p>
---	--


<p>Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate (SCRIVANIA PULITA)</p>	Adottata	G18; G20; G23
<p>La produzione di stampe, relative a dati Personali avviene sotto il controllo del Personale incaricato</p>	Adottata	G18; G20
<p>L'efficacia delle misure di sicurezza adottate è controllata con periodicità almeno annuale</p>	Adottata	G23

7.1.2. Trattamento informatico (hardware)

Misure di sicurezza	Stato attuale	Minaccia contrastata
<p>Contratti di assistenza per i sistemi hardware con intervento entro 12/48 ore.</p>	N.A.	
<p>Prima della dismissione o della riassegnazione degli elaboratori, gli hard disk vengono formattati con sovrascrittura totale</p>	Adottata	G11
<p>Generatori di corrente elettrica</p>	Adottata	G13
<p>Sistemi di continuità (UPS) per garantire la continuità della erogazione della corrente</p>	Adottata	G13
<p>Gli assets specie quelli informatici sono catalogati e ne è noto l'assegnatario</p>	Adottata	G2, G7

7.1.3 Organizzazione

Misure di sicurezza	Stato attuale	Minaccia contrastata
<p>E' stato individuato il/i Responsabile del trattamento dati Personali</p>	Adottata	G23
<p>Ogni persona ha sempre chiaro qual è il suo diretto responsabile</p>	Adottata	G2
<p>Sono chiaramente individuati i responsabili delle singole attività</p>	Adottata	G2

 <p>A.S.L. TO1 Azienda Sanitaria Locale Torino</p>	<p>DOCUMENTO PROGRAMMATICO SULLA SICUREZZA</p>
---	---

<p>Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali</p>	<p>Adottata</p>	<p>G23</p>
<p>Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione</p>	<p>Adottata</p>	<p>G23</p>
<p>Esiste una procedura di richiesta con tracciatura della conferma del responsabile per l'assegnazione di credenziali di accesso ad una procedura/servizio informatico</p>	<p>Adottata</p>	<p>G2, G3</p>
<p>Immediata segnalazione di problemi relativi alla sicurezza informatica</p>	<p>Adottata</p>	<p>G5, G6, G9</p>
<p>Regolamento aziendale circa l'uso degli strumenti in dotazione</p>	<p>Adottata</p>	<p>G3, G5, G6</p>
<p>Sono erogati corsi di formazione finalizzati alla comprensione della normativa in ambito sicurezza, trattamento dati e privacy</p>	<p>Adottata</p>	<p>G23</p>

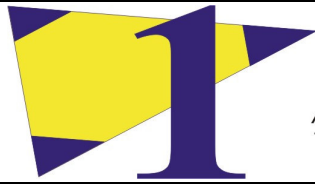
7.1.4 Sicurezza Fisica Sedi

<p>Misure di sicurezza</p>	<p>Stato attuale</p>	<p>Minaccia contrastata</p>
<p>Il pubblico non può accedere liberamente agli uffici</p>	<p>Adottata</p>	<p>G8</p>
<p>L'accesso ai locali critici avviene sempre congiuntamente alla persona che ha la responsabilità delle chiavi di accesso all'archivio</p>	<p>Adottata</p>	<p>G8;</p>
<p>Le chiavi dei locali tecnologici sono custodite</p>	<p>Adottata</p>	<p>G10</p>
<p>Apparati di rete e server, presenti presso la sede al di fuori dei locali tecnologici, sono protetti in armadi chiusi a chiave</p>	<p>Adottata</p>	<p>G3, G6, G9, G11</p>
<p>L'accesso ai locali al di fuori dell'orario di lavoro è controllato</p>	<p>Adottata</p>	<p>G3, G11</p>
<p>I supporti magnetici e ottici sono posti in arredi chiusi a chiave</p>	<p>Adottata</p>	<p>G3, G11</p>
<p>Le chiavi degli arredi (supp. magnetici) sono a disposizione unicamente del Personale autorizzato</p>	<p>Adottata</p>	<p>G3, G11, G14</p>
<p>Gli arredi contenenti i supporti magnetici sono a loro volta posti in locali chiusi a chiave</p>	<p>Adottata</p>	<p>G3, G11, G14</p>
<p>Le chiavi degli uffici sono a disposizione unicamente del Personale addetto autorizzato</p>	<p>Adottata</p>	<p>G3, G14</p>

I Pc degli incaricati sono posti in locali chiusi a chiave al di fuori del normale orario di lavoro	Adottata	G11, G14
Sistema antiincendio	Adottata	G12, G21
Sono identificabili chiaramente le uscite in caso di incendio	Adottata	G23
Sono previste delle esercitazioni a scadenze prefissate (allarme incendio, evacuazione, ecc.)	N/A	G23
Sono previste delle norme antincendio e tali misure sono pubblicate nei luoghi di lavoro	Adottata	G23
Presso le sedi c'è allarme antiintrusione e/o vigilanza notturna.	Adottata	G14, G19, G20, G22
La sede è dotata di sistemi di sorveglianza	Adottata	G14, G19, G20, G22
Copia dei backup dei server sono custoditi in altra sede	N/A	

7.1.5 Trattamento informatico (software)

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (FW etc.)	Adottata	G8
Sistemi IDS (Intrusion Detection System) verso la rete esterna	N.A.	
I PC sono tutti collegati tramite rete LAN aziendale	Adottata	G3, G8, G9
Sono attuate distinte LAN aziendali anche a seconda dei Trattamenti svolti	N/A	
E' prevista, nella rete aziendale, una DMZ per eventuali Web server o server acceduti comunque dall'esterno della rete	Adottata	G5, G8
Sistemi anti-spam e anti-relay aggiornati quotidianamente	Adottata	G5, G6
L'accesso a internet dalla rete aziendale è limitato con sw opportuni	Adottata	G5
I sistemi server ed i firewall sono tenuti costantemente aggiornati (patch e hardening)	Adottata	G5, G8
Sulle postazioni di lavoro ad alto rischio è installato un personal Firewall	N/A	
L'utilizzo dell'elaboratore è protetto da screen saver protetto da password o bloccato manualmente dall'Incaricato	N/A	
L'accesso ai PC a disposizione del personale è regolato tramite un sistema di autenticazione	Adottata	G8

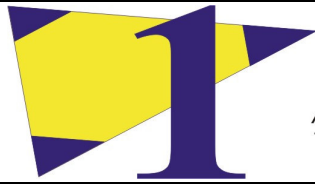


A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti	Adottata	G23
Funzione centralizzata di autenticazione nell'accesso ai dati	Adottata	G5, G8
Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione	Adottata	G23
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi	Adottata	G23
Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica	Adottata	G23
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	Adottata	G23
Le utenze "non necessarie" sono tempestivamente bloccate dagli Amministratori di sistema	Adottata	G3, G8
L'utilizzo del codice d'accesso è protetto da una parola chiave (password)	Adottata	G3, G23
La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.	Adottata	G23
Il sistema obbliga al cambio password al primo utilizzo delle credenziali di autenticazione	Adottata	G3
Il sistema obbliga automaticamente l'utente a cambiare la propria password con opportuna frequenza	Adottata	G3, G23
E' previsto l'obbligo di non riutilizzare le ultime password inserite	Adottata	G3, G8
Il sistema controlla la scelta della password per evitare la scelta di password banali (es. uguale a username, uguale a nome o cognome, ecc.)	Adottata	G3, G8

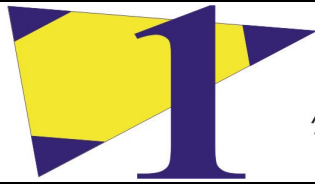


A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

Gli archivi elettronici locali sono opportunamente protetti da password	Adottata	G3, G8
Le password non sono scritte su carta, fogliettini etc. disponibili a colleghi o a terzi	Adottata	G3, G8
Memorizzazione di password/certificati di autenticazione su supporto fisico (Smart Card)	N/A	
Non esiste un archivio informatico in cui è possibile reperire le password degli utenti non crittografate	Adottata	G8; G10
Sono proibiti nei locali di lavoro documenti che riportano in chiaro le password di accesso alle procedure	Adottata	G3
La validità delle richieste di accesso ai dati è verificata prima di consentire l'accesso stesso	Adottata	G23
Esiste un sistema di profilo degli utenti del sistema informatico	Adottata	G23
I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento	Adottata	G23
Procedura organizzativa gestione profili trattamento dati personali	Adottata	G23
Tenuta LOG (Proxy, FireWall, Posta)-	Adottata	G23
Esiste un elenco/schema delle procedure/applicativi informatici utilizzati complessivamente dal personale	Adottata	G4
I dipendenti che possono avere profilo di amministratore operano seguendo precise disposizioni	Adottata	G23
Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Adottata	G23
I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale (antivirus)	Adottata	G5, G23
Su ogni postazione di lavoro è installato un antivirus	Adottata	G5
Aggiornamento automatico e giornaliero dell'antivirus	Adottata	G5
Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (restore dei dati)	Adottata	G4, G23
Backup quotidiano dei dati	Adottata	G4, G6



A.S.L. TO1


Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

Esiste un backup periodico dei dati custoditi nelle postazioni	N/A	
Esistono "share" di rete per la condivisione di materiale di lavoro	Adottata	G4
E' accertata la conformità delle procedure informatiche con il DLgs 196/03	Adottata	G23
Non esistono dipendenti che utilizzano postazioni libere (anche solo saltuariamente)	Adottata	
Sono installate, sulle diverse postazioni, in modo costante le patch di sicurezza del sistema operativo	Adottata	G9, G23
Attenzione quotidiana verso le minacce provenienti dalla rete	Adottata	G8, G9
Controllo periodico delle regole di accesso (policy, acl etc.) ai dati condivisi e alle applicazioni	Adottata	G8
Controllo periodico dello stato delle vulnerabilità mediante strumenti automatizzati e/o tentativi di intrusione	Adottata	G5, G8
L'efficacia delle misure di sicurezza adottate è controllata con periodicità almeno annuale	Adottata	G23

LEGENDA MINACCE CONTRASTATE

Codice	Tipo di trattamento	Minacci
G1	Trattamento dati in formato elettronico	Sottrazione di credenziali di autenticazione
G2		Carenza di consapevolezza, disattenzione o incuria
G3		Comportamenti sleali o fraudolenti
G4		Errore
G5		Azione di virus informatici o di programmi suscettibili di recare danno
G6		Spamming o altre tecniche di sabotaggio
G7		Malfunzionamento, indisponibilità o degrado degli strumenti
G8		Accessi esterni non autorizzati
G9		Intercettazione di informazione in rete
G10		Accessi non autorizzati ai locali/reparti ad accesso ristretto
G11		Sottrazione di strumenti contenenti dati
G12		Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria
G13		Guasto ai sistemi complementari (impianto elettrico, climatizzazione _)
G14		Errori umani nella gestione della sicurezza fisica
G15	Trattamento dati in formato cartaceo (o floppy/cd/tape)	Sottrazione di chiavi di accesso ai locali e/o armadi
G16		Carenza consapevolezza, disattenzione o incuria
G17		Comportamenti sleali o fraudolenti
G18		Errore
G19		Accessi non autorizzati ai locali/reparti ad accesso ristretto
G20		Sottrazione di
G21		Eventi distruttivi, naturali o artificiali, dolosi, accidentali, o dovuti ad incuria

 <p>A.S.L. TO1 Azienda Sanitaria Locale Torino</p>	<p>DOCUMENTO PROGRAMMATICO SULLA SICUREZZA</p>
---	---

G22		Errori umani nella gestione della sicurezza fisica
G23		Prescrizioni di

7.2 Strumentazione di sorveglianza

Criterio Generale

Gli impianti TVCC installati presso tutte le strutture aziendali, sono necessari a garantire la tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, atti di vandalismo, prevenzione di incendi, nonché la sicurezza dei lavoratori.

E' necessario proteggere gli accessi pedonali e carrabili con TVCC oltre che per la sicurezza anche per esigenze di servizio.

Possono essere installati impianti di videosorveglianza anche a protezione di aree interne destinate ad attività lavorativa, ma attivabili solo fuori orario di servizio.

Principi generali in materia di videosorveglianza

Nel trattamento dei dati conseguente all' attivazione della videosorveglianza, vengono adottati i seguenti criteri:

- La raccolta e l' uso delle immagini sono consentiti solo se necessari allo svolgimento di funzioni istituzionali e per il perseguimento di finalità di pertinenza dell' Azienda, tra i quali vi sono la sicurezza degli impianti, dei pazienti e degli operatori;
- I lavoratori ed i cittadini che transitano nelle aree sorvegliate sono informati dalla rilevazione dei dati mediante affissione di specifico cartello secondo il modello preposto dal Garante;
- Va limitata rigorosamente la creazione di banche dati quando è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini senza la loro registrazione;
- Le Telecamere di Videosorveglianza a circuito chiuso (TVCC) nelle sedi dell' ASL TO1, sono poste in opera e tenute in esercizio in stretta aderenza ai principi di legge e alle norme in vigore;
- Le TVCC sono installate all' esterno degli edifici e presso i varchi di accesso e sono gestite in via autonoma e disgiunta da altri sistemi attivi all' interno dell' impresa (es: accesso; cartellino presenza);
- Le TVCC sono presenti all' interno degli edifici solo in alcuni specifici casi e precisamente nelle aree di particolare rischio (corridoi di transito e nelle zone in cui sono trattati dati sensibili della cittadinanza);
- Riprese e videoregistrazioni saranno utilizzati solo per compiti inerenti alla sicurezza dei dipendenti, dei beni e delle sedi aziendali. I dati raccolti sono trattati e

conservati a norma delle disposizioni di legge in materia di protezione dei dati personali, ovvero consultati previa autorizzazione presso locali controllati, conservati con criteri di sicurezza per i tempi indicati dal Garante;

- Le procedure di video-registrazione sono conservate per un tempo non superiore a 7 giorni. Trascorso tale periodo i dati vengono “soprascritti” dalle nuove immagini.
- Le immagini potranno essere visionate solo dalle autorità competenti;

Principi in materia di videosorveglianza inerenti i diritti dei pazienti

Il controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (es. unità di rianimazione), stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di stretta indispensabilità e circoscrivendo le riprese solo a determinati locali e a precise fasce orarie; devono essere inoltre adottati tutti gli ulteriori accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate, anche in attuazione delle doverose misure che il Codice prescrive per le strutture sanitarie (art.83 Codice della privacy).

L’ Azienda deve garantire che possano accedere alle immagini solo i soggetti specificamente autorizzati (es. personale medico ed infermieristico) e che le stesse non possano essere visionate da estranei (es. visitatori). Particolare attenzione deve essere riservata alle modalità di accesso alle riprese video da parte di familiari di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente (es. rianimazione), ai quali può essere consentita, con gli adeguati accorgimenti tecnici, la visione dell’ immagine solo del proprio congiunto.

Le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse (art. 22, comma 8 e 167 del Codice della Privacy). Va assolutamente evitato il rischio di diffusione delle immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico.

Protezione delle aree e dei locali

I criteri relativi al controllo dell’ accesso fisico alle diverse aree dell’ ASL TO1, sono finalizzati a definire:

- La sicurezza di area che ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi sanitari, alla sicurezza dei locali del Sistema Informatico rispetto a danneggiamenti accidentali o intenzionali e alla protezione fisica dei supporti.
- La sicurezza delle apparecchiature che è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall’ altro alla sicurezza degli impianti di alimentazione e condizionamento. Anche la manutenzione delle attrezzature rientra in

questa area, come anche la protezione da manomissione e furti.

7.2.1 Vigilanza

Il servizio di Vigilanza (Sorveglianza) consiste nell' assicurare la tutela della sicurezza dei beni e del personale dell' ASL TO1 e viene svolto con idoneo personale presso le sedi e secondo le modalità ed orari di seguito indicati.

- Servizio di Sorveglianza ed accoglienza (filtro utenza accessi) presso il Pronto Soccorso dell' Ospedale Martini attuato mediante Guardia Giurata con il seguente orario:

dalle ore 14.00 alle ore 8.00 di tutti i giorni feriali
dalle ore 14.00 del sabato alle ore 8.00 del lunedì
dalle ore 8.00 alle ore 8.00 del giorno successivo, per i giorni festivi infrasettimanali

- Servizio di Sorveglianza presso l' Ambulatorio preposto alla somministrazione del metadone Ospedale Martini mediante Guardia Giurata per il controllo dell' afflusso dell' utenza e per far fronte ad eventuali problemi, di qualsiasi natura, che dovessero sorgere legati alla tipologia degli utenti che si rivolgono a tale struttura.

Il Servizio è attuato con il seguente orario:

dalle ore 06.50 alle ore 10.45 e dalle ore 11.55 alle 15.15 dal lunedì al venerdì
dalle ore 08.00 alle ore 12.30 il sabato e giorni festivi

7.2.2 Chiusura degli uffici, degli armadi e gestione apparecchiature

Il Personale tutto sia interno sia esterno (collaboratori e consulenti) è tenuto ad osservare opportune cautele a salvaguardia soprattutto dell' acquisizione di documentazione, uso o furto delle apparecchiature presenti soprattutto presso gli uffici di competenza.

Sono in particolare da osservare le seguenti norme:

- non estendere per alcun motivo senza autorizzazione le possibilità di accesso a disposizione. Tali possibilità (es. chiavi di locali ed armadi) non possono essere condivise da terzi non autorizzati;
- provvedere alla chiusura degli uffici in assenza di presidio conferendo la chiave alla Portineria e segnalando eventuali malfunzionamenti di chiavi e serrature;
- segnalare tempestivamente il verificarsi di comportamenti sospetti e di furti specie a carico di apparecchiature informatiche. Ciò al fine di attuare quanto immediatamente possibile e procedere nel caso con la denuncia presso l' Autorità

- di Polizia Giudiziaria);
- utilizzare la chiave hardware e/o chiave bios quali forme di sicurezza aggiuntiva sulla propria postazione di lavoro ad evitare l'accesso a eventuali dati localmente custoditi;
- sgomberare la scrivania (in caso di prolungata assenza) da stampe contenenti dati riservati e personali;
- al termine della giornata di lavoro spegnere il PC;
- Se si dispone di un portatile riporlo sotto chiave;
- In viaggio tenere il portatile sotto controllo evitando di lasciarlo incustodito in auto o in albergo;
- Eventuali informazioni riservate o sensibili su qualsiasi supporto informatico o disco fisso di PC portatile devono essere possibilmente tutelate con la crittografia

7.2.3 Supporti di memorizzazione

Sono considerati supporti di memorizzazione i nastri magnetici,cartrige, i dischi magnetici o ottici amovibili, i CD-ROM che contengono informazioni personali.

I supporti contenenti dati sensibili devono (D.lgs 196/03) essere custoditi in un' area ad accesso controllato o in un ufficio che sia chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

I supporti usati per i backup, devono essere custoditi presso la S.C. Sistema Informatico, in armadio chiuso a chiave.

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento (es. nastri, dischi magnetici, dischi ottici, ecc)

Per riutilizzare un supporto di memorizzazioni contenenti dati personali, occorre rendere impossibile il recupero dei dati precedentemente memorizzati, anche mediante processi di sovrascrittura o formattazione a basso livello.

Gli Hard-Disk devono essere formattati prima della rassegnazione del pc ad altro Utente. Dischi ottici e CD devono essere distrutti alla fine del trattamento.

7.2.4 Stampe ed archivi cartacei

Relativamente agli archivi cartacei sono definiti i seguenti Criteri:

- le stampe relative a dati personali devono essere eseguite dagli incaricati presso stampanti presidiate per evitare la divulgazione di quanto riportato;
- le stampe o i documenti cartacei riportanti dati personali devono al termine del loro



A.S.L. TO1

*Azienda Sanitaria Locale
Torino*

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

- utilizzo o essere archiviate in contenitori o in locali provvisti di serratura: deve essere evitata la consultazione od appropriazione indebita di qualsiasi stampa;
- in aggiunta a quanto sopra le stampe o i documenti cartacei riportanti dati personali, sensibili o giudiziari devono essere custoditi in contenitori chiusi a chiave all' interno di locali chiusi a chiave in assenza di presidio.

8. CRITERI E PROCEDURE PER IL SALVATAGGIO ED IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI

(Codice, Allegato B, regola 19.5)

In questa sezione sono descritti i criteri e le procedure adottate per il backup ed il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci.

Vengono anche definiti i tempi certi compatibili con i diritti degli interessati, che devono essere non superiori a sette giorni, come definito dal D.Lgs. 196/2003.

A garanzia di ciò, si individuano le linee guida di seguito indicate.

8.1. Backup e Restore dei dati

8.1.1. Criteri e procedure per il salvataggio ed il ripristino dei dati

Al fine di garantire nel tempo l'integrità e la disponibilità dei dati, vengono effettuati periodicamente i salvataggi degli stessi.

Per realizzare il processo di salvataggio dei dati e per monitorarne la corretta esecuzione è utilizzata un'applicazione software a questo dedicata.

Vengono quindi effettuate quotidianamente copie di salvataggio incrementali dei dati residenti sui sistemi server in gestione presso l'ASL TO1.

Nel caso in cui occorra ripristinare un singolo file o documento, il sistema recupera l'ultima versione salvata oppure consente di effettuare una scelta tra le versioni conservate.

La seguente tabella illustra la pianificazione dei backup:

Tipo di Backup	Frequenza	Note
Backup giornaliero	Ha una frequenza giornaliera, di norma serale, dal lunedì al venerdì	Il backup raccoglie tutte le variazioni prodotte, durante una giornata. E' anche detto incrementale.

Più in generale, si individuano le seguenti linee guida:

- l'ASL TO1 è responsabile delle procedure di salvataggio su nastro (o altro

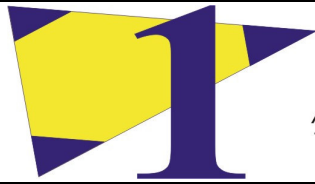
- opportuno supporto) delle basi dati contenenti dati personali residenti sui sistemi server, con opportuna frequenza;
- Gli incaricati che trattano dati personali su archivi residenti in locale sulle proprie postazioni di lavoro sono responsabili del salvataggio periodico di tali archivi sulle risorse di rete o su supporti rimovibili (floppy, cd-rom, ecc.); tali supporti rimovibili andranno custoditi in sicurezza.

8.1.2. Ripristino dei dati

I salvataggi sono registrati su cassette.

Le cassette dei salvataggi sono custodite in appositi locali di sicurezza, in sede diversa da quella che ospita la sala macchine.

Prima di introdurre nuove procedure e/o nuove architetture di backup, si effettuano prove di salvataggio e ripristino, a garanzia dell' integrità e della disponibilità dei dati.



A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

9. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

(Codice, Allegato B, regola 19.6)

9.1. Formazione

Il Codice, alla regola 19.6 del suo Allegato B, introduce l'obbligo di previsione di interventi formativi per gli incaricati del trattamento, al fine di renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Per il biennio 2011/2012 la formazione, per gli incaricati del trattamento dei dati è prevista in FAD (Formazione a distanza).

10. TRATTAMENTI DI DATI AFFIDATI ALL' ESTERNO

(Codice, Allegato B, regola 19.7)

Obiettivo di questa sezione è redigere un quadro sintetico delle attività trasferite a terzi che comportano il trattamento di dati personali con l' indicazione del riferimento giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in relazione agli impegni assunti per garantire la protezione dei dati personali stessi.

10.1. Criteri in caso di trattamenti affidati all' esterno

Come principio generale, l' affidamento di trattamenti, anche parziali, all' esterno deve avvenire in modo tale da garantire che i criteri di sicurezza che l' Ente ha adottato al suo interno continuino ad essere rispettati.

Secondo quanto previsto dal D.Lgs. 196/2003, l' affidamento, anche solo parziale, del trattamento di dati personali all' esterno della struttura dell' Ente deve avvenire in maniera tale da garantire che il Fornitore rispetti le misure minime di sicurezza definite dalla legge.

A tal fine, i contratti di fornitura dovranno contenere apposite clausole.

Se il Fornitore è italiano o comunque soggetto alla Legge italiana: specifica dichiarazione formale con impegno del Fornitore a trattare di cui l' Ente è Titolare in conformità al Decreto Legislativo 196/2003 e di adottare al minimo i criteri e le misure minime di sicurezza ivi identificate, nonché di effettuare i trattamenti secondo le istruzioni e per le finalità indicate dal Titolare; tale dichiarazione sarà parte integrante del contratto.

Se, al contrario, il Fornitore non è italiano o comunque non soggetto alla Legge italiana: specifica dichiarazione formale con impegno del Fornitore a trattare i dati all' interno dell' Unione Europea, rispondendo alle linee guida Comunitarie in materia di Privacy ed in conformità alla Legge Nazionale del paese in cui il Fornitore opera, nonché di effettuare i trattamenti secondo le istruzioni e per le finalità indicate da Titolare. Tale dichiarazione sarà parte integrante del contratto.

Inoltre, l' Ente si riserva contrattualmente la possibilità formale e sostanziale di riscontrare quanto dichiarato dal Fornitore con riferimento alla conformità al D.Lgs. 196/2003 (diritto di Audit ed Ispezione).

Il Titolare del trattamento e quanti nell' ambito dell' Ente siano delegati ad impegnarsi in contratti con terze parti, sono tenuti a verificare che i nuovi contratti di fornitura di servizi, che implicino il trattamento di dati personali di cui l' Ente è Titolare del trattamento, soddisfino questi requisiti.

I contratti attualmente in essere alla loro scadenza naturale saranno rinnovati solo previa integrazione.

Se vengono adottate misure minime di sicurezza avvalendosi di soggetti esterni alla struttura dell' Ente, il Titolare si fa rilasciare una descrizione scritta dell' intervento effettuato che ne attesti la conformità alle disposizioni del Disciplinare tecnico contenuto nell' Allegato B del D.Lgs. 196/2003.


Affinchè sia garantito un adeguato trattamento dei dati è necessario che il soggetto esterno a cui viene affidato il trattamento si assuma alcuni impegni, cioè:

1. di essere consapevole che i dati che tratterà nell' espletamento dell' incarico ricevuto sono dati personali e, come tali, sono soggetti all' applicazione del Codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere;
4. di riconoscere il diritto del committente a verificare periodicamente l' applicazione delle norme di sicurezza adottate.

Nella successiva tabella sono riportate, con significato di seguito descritto, le seguenti informazioni:

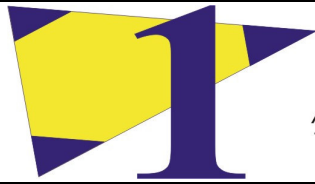
Descrizione sintetica dell' attività "esternalizzata": indica l' attività affidate all' esterno;

Soggetto esterno delegato: indica la società, l' ente o il consulente cui è stata affidato l' incarico per svolgere l' attività, e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali;

 <p>A.S.L. TO1 Azienda Sanitaria Locale Torino</p>	<p align="center">DOCUMENTO PROGRAMMATICO SULLA SICUREZZA</p>
---	--

10.1.1 Trattamenti affidati all'esterno

Soggetto esterno	Descrizione sintetica dell'attività esternalizzata
BIM s.r.l.	Manutenzione "Multiservice Quani"
Bitelo	Assistenza e manutenzione sw: Saofarm; Gepasti; Incentivi; Saoc4; Reld; Saoodo; Saouro; Saoope; Saouvg; Saograd; Saoordine; Saoconsulto; Saopsiche; Saoadi; Saovaso; Saoute; Saoinge; Saovaccino; Saiva; Saoinve
Cedaf	Assistenza e manutenzione sw applicativo gestione Segreteria, delibere e determine e albo pretorio
Consorzio Mosaico	<ul style="list-style-type: none"> - Assistenza e manutenzione ordinaria al sw HIS-SITA (Sistema Informativo TossicoAlcolico dipendenze) - Manutenzione ordinaria della procedura "SERENA" - Assistenza e manutenzione applicativi: <ul style="list-style-type: none"> - gestione visite fiscali del servizio di Medicina Legale - gestione DL 81/08 del servizio di Sorveglianza Sanitaria - gestione DL 81/08 ed estensioni territorio del Servizio Medico Competente
CSI PIEMONTE	Assistenza e manutenzione per applicativi in virtual farm (SGP –FirstAid, Ris, Adtweb, Immagini in rete, Oliamm, Lapis Web; Stipendi ecc...)
Cyberdyne	Assistenza, manutenzione, e aggiornamento programmi Arcos – Arcgin –ed Eco Store con immagini installati presso i reparti di Ostetricia, Ginecologia e Pediatria
Dedalus s.p.a.	<ul style="list-style-type: none"> - Assistenza e manutenzione software applicativo: Infoclin XP; Applicativi AS/400 e Concerto; Firstaid Clinical data ware house – Integrazioni con S.I. - Assistenza e manutenzione al sistema informativo del Laboratorio Analisi Osp. Oftalmico e servizio di Anatomia Patologica Osp. Martini
Ebon s.a.s..	Assistenza, manutenzione e aggiornamento software di gestione Hospice installati presso S.C. Sistema Informatico e Presidio Valletta
Eldasoft s.p.a.	Manutenzione e assistenza sw Alice: Alice PL Web Alice GA Web
Infogramma s.r.l.	Assistenza e manutenzione al sistema di Cartella Clinica Informatizzata Galenus per la S.C. Nefrologia e Dialisi Ospedale Martini
Innovo s.a.s.	Assistenza alla procedura di gestione service modulo ABACO
Jergosoft s.n.c.	Assistenza programma gestionale Dentus per gli ambulatori di odontostomatologia ASL TO1
MondoEdp s.r.l.	Manutenzione e assistenza al sw IrisWin – Gestione



A.S.L. TO1

Azienda Sanitaria Locale
Torino

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA**

	presenze, assenze del personale
NBS	Assistenza e sviluppo del "Sistema informatico per la gestione dell'accreditamento delle attività formative dei provider e monitoraggio della formazione continua ECM e non
NoemaLife	Help Desk e manutenzione del sw applicativo Windopath
Paolo Tartari	Assistenza informatica e sviluppo al programma di gestione Ambulatorio di Pneumologia
Praim technologies	Supporto software Master Printer Server – Osp. Valdese
Pubblidata	Assistenza e coordinamento attività per l'ASL TO1
STUDIO PRO sas	Assistenza alla procedura di gestione dei servizi relativi al Modulo Cedolini, al Modulo OSRU, e del Modulo Stampe installati presso la S.C. Risorse Multiprofessionali
T.M. S.r.l.	Assistenza e manutenzione per sistema di refertazione vocale Phoneidos-DI
TSD Projects	Manutenzione e assistenza sw per applicazione Wincare – Otorino Osp. Martini
Unicomp Informatica s.r.l.	Servizio di Assistenza – Medicina Integrativa Protesica e Medicina sportiva
M.C.E. s.r.l.	Gestione sistema TVCC e videosorveglianza

11. CIFRATURA DEI DATI

(Codice, Allegato B, regola 19.8)

11.1. Criteri per la cifratura o separazione dei dati sensibili

Nel caso in cui siano trattati dati personali idonei a rilevare lo stato di salute e la vita sessuale (art. 22 del DLgs 196/2003), l'incaricato deve provvedere a separare tali dati da tutti gli altri dati personali qualora ciò non sia già previsto dalla procedura informatica di supporto al trattamento, conservandoli in tabelle o database diversi e collegandoli, se necessario, solo ai fini del trattamento.

Nel caso in cui non sia possibile provvedere alla separazione dei dati, si deve provvedere alla cifratura dei dati rilevanti lo stato di salute e la vita sessuale.

Gestione dei log

Le apparecchiature di controllo agli accessi (firewall e proxy) ed i dispositivi IPS (anti intrusione) producono file di log.

Il personale dell' ASL TO1 addetto alla gestione delle Reti può visionare tali supporti solamente se indispensabile:

- per finalità statistiche e consuntive sull'uso delle macchine a fronte di necessità interne;
- per l'individuazione delle cause di problemi di funzionamento dei sistemi gestiti.

I log verranno conservati per un periodo coerente con le vigenti disposizioni di legge. La finalità della conservazione di questi dati, che possono contenere informazioni sensibili riconducibili a specifici utenti, è specificamente e unicamente finalizzata a supporto di eventuali verifiche disposte dalla magistratura.

Le attività appena elencate non consentono di risalire ai siti visitati dal personale (nel rispetto quindi della privacy dell'utente e di quanto stabilito dall'art. 4 dello Statuto dei Lavoratori).