Regolamento per il rispetto degli obblighi in materia di protezione dei dati personali trattati con l'ausilio di strumenti elettronici, per la custodia degli strumenti elettronici, per il corretto uso della mailbox aziendale e per la navigazione online

Azienda
Ospedaliera
"S.Maria"
Terni

Via Tristano di Joannuccio
05100 Terni

Tel.: ***+39 0744.2051***
Fax: ***+39 0744.205006***

www.aospterni.it

Indice

Normativa di riferimento (in ordine cronologico)

- Legge 633/1941 e succ. modif., c.d. *"Legge sul diritto d'autore"*
- Artt. 2086, 2087, 2104, 2105, 2106 del codice civile;
- Art. 12 della *"Dichiarazione Universale dei Diritti dell'Uomo"* adottata dall'Assemblea Generale delle Nazioni Unite il 10 Dicembre 1948;
- Art. 8 della *"Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali"* (Roma, 4 Novembre 1950);
- Legge 300/1970, recante lo *"Statuto dei lavoratori"*;
- Paragrafi 2 e 3 della Raccomandazione n. R (89) 2 del Comitato dei Ministri agli Stati membri relativa alla protezione dei dati a carattere personale utilizzati ai fini dell'occupazione, adottata dal Comitato dei Ministri il 18/1/1989;
- Decreto Legislativo 518/1992, che riguarda la tutela giuridica del programmi per elaboratore;
- Legge 547/1993, che modifica il codice penale introducendo i crimini informatici;
- Decreto Legislativo 626/1994 in materia di sicurezza sul luogo di lavoro, Allegato VII, Paragrafo 3, lett. b)
- Art. 15, comma 2, della Legge 59/1997, che riconosce validità e rilevanza a tutti gli effetti di legge agli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, altresì ai contratti stipulati nelle medesime forme, nonché alla loro archiviazione e trasmissione con strumenti informatici;
- Decreto Legislativo 169/1999, che riguarda la tutela giuridica delle banche di dati;
- Artt. 7 e 8 della *"Carta dei diritti fondamentali dell'Unione Europea"* (Nizza, Dicembre 2000);
- Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, adottato il 29.05.2002 dal Gruppo di lavoro sulla protezione dei dati, ai sensi dell'art. 29 della direttiva 1995/46/CE (documento n. 5401/01/IT/def. - WP 55);
- *"Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione"* (Raccomandazione del Consiglio dell'OCSE, 25.07.2002);
- Decreto Legislativo 196/2003 e succ. modif., recante il *"Codice in materia di protezione dei dati personali"*;
- Allegato B al Decreto Legislativo 196/2003, concernente il *"Disciplinare tecnico in materia di misure minime di sicurezza"*;
- Decreto del Presidente del consiglio dei ministri 13.01.2004, concernente le *"Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici"*;
- Decreto del Presidente della Repubblica 11.02.2005, n. 68, concernente il *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3"*;
- Decisione Quadro 2005/222/GAI del Consiglio UE del 24.02.2005, relativa agli attacchi contro i sistemi di informazione;
- Art. 3 della Legge 43/2005, in materia di interventi per i beni e le attività culturali;
- Decreto Legislativo 82/2005 (come successivamente modificato dal Decreto Legislativo 159/2006), recante il *"Codice delle amministrazioni digitali"*;
- Legge 38/2006 lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche via Internet, che modifica la Legge 269/1998;
- Parere del 28 novembre 2006, Prot. n. 25/I/0006585, adottato dal Ministero del Lavoro e della Previdenza Sociale – Direzione Generale per l'attività ispettiva;
- Provvedimento generale del Garante per la protezione dei dati personali del 1.03.2007, Bollettino del n. 81/marzo 2007, pag. 0 [doc. web n. 1387522], concernente le *"Linee guida del Garante per posta elettronica e internet"*.
- Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 16 dicembre 2009 (G.U. n. 13 del 18 gennaio 2009 - suppl. ord. n. 12). In vigore fino al 30 giugno 2011.
- Direttiva n. 02/09 del 26/05/2009 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica. Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro.
- Regolamento del Procedimento Disciplinare per il comparto dell'A.O. "S. Maria" di Terni approvato con deliberazione del Direttore Generale n. 149 del 13.03.2010

* * *

1 Premessa di carattere generale

Oggetto del presente documento è l'armonizzazione e standardizzazione delle procedure per il corretto uso degli **strumenti informatici e telematici** messi a disposizione del personale, interno ed esterno, dall'Azienda Ospedaliera "S.Maria" di Terni (di seguito, per brevità, A.O.), in ogni suo aspetto (strutturale, funzionale, organizzativo) e in ogni sua componente (hardware, software). In particolare il Regolamento sarà sottoposto all'attenzione del personale sanitario (medico e paramedico, ivi inclusi stagisti e specializzandi) e di quello non sanitario (impiegati amministrativi, collaboratori, consulenti, personale del settore IT, tecnici, responsabili di uffici, organi di management), che prestino le loro attività per l'A.O., in modo tale che risultino informati sulle politiche di sicurezza e di protezione dei dati critici **[1]** adottate dall'A.O. stessa.

Tale documento avrà anche valore di *"Codice Etico"* per tutti i soggetti sopra indicati che, dopo adeguata informazione e dopo eventuali modifiche concordate con gli organi apicali, lo sottoscriveranno, personalmente ovvero tramite delega rilasciata alle rappresentanze sindacali o, in alternativa, alle commissioni interne, se presenti, salva interpello all'Ispettorato del Lavoro da parte dell'A.O. in caso di mancato accordo, ai sensi di quanto previsto dall'art. 4 dello *"Statuto dei Lavoratori"* (l. 300/1970).

Gli aspetti concernenti la protezione dei dati critici dell'A.O. contenuti su supporti cartacei o comunque archiviati/conservati/gestiti secondo modalità tradizionali potranno essere affrontati in un separato e specifico documento.

---

[1] **Sono definiti *"critici"* quei dati, la cui esposizione a indebite appropriazioni o sottrazioni ovvero a perdita, cancellazione, distruzione, alterazione, modifica, falsificazione o ad ogni altra operazione non autorizzata che ne determini l'indisponibilità, anche solo parziale o temporanea, potrebbe causare danno alla continuità e alla crescita dell'attività dell'A.O. ovvero potrebbe lederne l'immagine ovvero ancora determinare il mancato rispetto degli obblighi di legge o di quei valori etici e deontologici, ai quali l'A.O. stessa si ispira. L'accesso a tali dati è normalmente limitato e riservato, potendo le eventuali violazioni essere fonte di rischio per gli interessi e lo sviluppo delle attività.**

D'altra parte i dati ccdd. *pubblici* sono in quanto tali di pubblico dominio e destinati alla comunicazione a terzi e talora alla diffusione e meritano un livello minimo di protezione in quanto la loro perdita, distruzione, cancellazione etc. non determina nessun impatto sulle attività ovvero determina un impatto minimo. I dati possono considerarsi comuni pur sempre se divulgati senza preclusioni o divieti da parte dell'A.O. sia all'interno che all'esterno ovvero se pubblicamente disponibili al di fuori della realtà dell'A.O. oppure nei casi in cui si intendano di pubblico utilizzo.

Resta salvo l'assoluto divieto di diffusione dei dati idonei a rivelare lo stato di salute.

2 CAPO I – Privacy policy

2.1 Premessa

Tutti i messaggi inviati, ricevuti o archiviati, usando computer e sistemi di *processing* dell'A.O. oppure inviati sulla rete Intranet della medesima sono da considerarsi di proprietà o di pertinenza dell'A.O. stessa.

Gli utenti, interni o esterni, devono essere informati e resi edotti del fatto che le loro comunicazioni e relativi *file* possono essere oggetto di monitoraggio e di controllo da parte dell'A.O., al fine di verificarne la conformità alle proprie politiche interne e agli obblighi dei soggetti in quanto dipendenti o utenti dell'A.O.. In particolare gli account, le caselle di posta elettronica e le attività dell'utente possono essere monitorate dall'A.O. Quest'ultima si riserva altresì il diritto di filtrare i contenuti delle connessioni ad internet. Ovviamente monitoraggio e controllo verranno effettuati nel rispetto della privacy di ciascun utente, con particolare riferimento alla dignità, alla riservatezza, all'identità, al diritto alla protezione dei dati personali e agli altri diritti e libertà fondamentali dell'utente medesimo, in base alle leggi nazionali e locali, ai regolamenti, alla normativa comunitaria e ad altre normative rilevanti in materia di protezione dei dati personali. In particolare dovranno essere rispettati i principi di necessità, finalità, proporzionalità, liceità, correttezza, sicurezza e trasparenza nelle attività di controllo degli accessi e di monitoraggio.

Gli stessi utenti interni sono tenuti a rispettare le regole sulla privacy individuale anche in ambiente lavorativo.

Gli utenti interni ed esterni non devono accedere intenzionalmente e senza autorizzazione ad informazioni personali, né copiare software, file, dati, password o codici d'accesso relativi a terze persone (siano essi utenti esterni o esterni), né assumerne l'identificativo.

Resta impregiudicato l'esercizio dei diritti da parte degli interessati (cioè delle persone alle quali software, file, dati etc. si riferiscono) ai sensi dell'art. 7 del D.Lgs. 196/2003, *"Codice in materia di protezione dei dati personali"* (di seguito, per brevità, Codice), che recita come segue:

> *"Art. 7 (Diritto di accesso ai dati personali ed altri diritti)*
>
> *1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.*
>
> *2. L'interessato ha diritto di ottenere l'indicazione:*
>
> *a) dell'origine dei dati personali;*
>
> *b) delle finalità e modalità del trattamento;*
>
> *c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;*
>
> *d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;*
>
> *e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.*
>
> *3. L'interessato ha diritto di ottenere:*
>
> *a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;*
>
> *b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;*
>
> *c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale*

adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale."

Le istanze di esercizio dei diritti sono rivolte senza formalità (via mail, tramite fax o telefono ovvero tramite corrispondenza tradizionale, ordinaria o raccomandata) all'A.O., in qualità di *"Titolare"* del trattamento dei dati personali degli interessati, ovvero a colui/coloro che sia/siano stato/stati designato/designati *"Responsabile"/ "Responsabili"* del trattamento, anche per il tramite di uno o più *"Incaricati"* del trattamento stesso (per le definizioni di *"trattamento"*, *"titolare"*, *"incaricato"* e *"responsabile"*, cfr. paragrafo successivo).

Nell'esercizio dei diritti di cui all'art. 7 cit. l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia. In tali ipotesi la persona che agisce per conto dell'interessato può agire secondo le seguenti modalità:

- esibizione o allegazione di copia della procura **[2]**;
- esibizione o allegazione della delega **[3]** sottoscritta in presenza di un incaricato;
- esibizione o allegazione della delega sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.

I diritti di cui all'art. 7 cit. riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

L'A.O. darà riscontro a tali istanze senza ritardo e comunque non oltre 15 giorni dalla ricezione delle medesime, salvo che le operazioni necessarie per un integrale riscontro siano di particolare complessità, ovvero ricorra altro giustificato motivo. In tali casi l'A.O. o il responsabile ne danno comunicazione all'interessato entro il termine di cui sopra e il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

I dati sono estratti a cura del responsabile o degli incaricati e sono comunicati al richiedente anche oralmente ovvero offerti in visione mediante strumenti elettronici secondo modalità trasparenti e in forma chiara e comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

Se vi è richiesta da parte dell'interessato, l'A.O. provvede alla trasposizione dei dati su supporto cartaceo o informatico ovvero alla loro trasmissione per via telematica.

Salvo che la richiesta sia riferita a un particolare trattamento o a specifici dati personali o a categorie di dati personali, il riscontro comprende tutti i dati personali che riguardano l'interessato comunque trattati dall'A.O..

Quando l'estrazione dei dati risulta particolarmente difficoltosa, il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi diversi dall'interessato, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

2.2 Definizioni rilevanti in materia di protezione dei dati personali

a) *"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;

---

[2] Il termine *"procura"* è qui da intendersi in senso tecnico quale atto formale di autorizzazione alla rappresentanza ed assistenza giudiziale, rilasciato a soggetti iscritti in appositi albi e abilitati *ex lege* a tale tipo di attività (es. avvocati).

[3] Il termine *"delega"* è da intendersi in senso lato (v. art. 1387 e ss. del codice civile), quale atto di autorizzazione alla rappresentanza rilasciato dall'interessato ad altro soggetto anche non iscritto in appositi albi o comunque non abilitato all'attività di assistenza giudiziale.

b) *"dato personale"*: qualunque informazione, contenuta in supporti cartacei o elettronici, 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. Esempi: nome, cognome, pseudonimo, denominazione e ragione sociale, ditta, codice fiscale, partita IVA, account di posta elettronica, password, codice PIN, userID etc.;
c) *"dato identificativo"*: dato personale, su qualsiasi supporto contenuto, che permette l'identificazione diretta dell'interessato. Esempi: nome e cognome, impronte digitali etc.
d) *"dati sensibili"*: dati personali, in qualunque supporto contenuti, 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. Esempi: certificati medici, cartelle cliniche, passaporti, tessere di partiti politici o di sindacati, tessere di associazioni religiose etc.;
e) *"dati giudiziari"*: 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. Esempi: certificato del casellario giudiziale dal quale emergano precedenti penali;
f) *"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. Esempio: una società, un qualsiasi datore di lavoro (imprenditore individuale, anche piccolo o agricolo), il proprietario di un pubblico esercizio, un ente pubblico territoriale come il Comune o la Provincia etc.;
g) *"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. Esempi: un capo-ufficio, un capo-reparto, un distretto, un dipartimento, un ufficio centrale o periferico di un ente pubblico, un'azienda controllata o collegata etc.;
h) *"incaricato"*: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile. Esempio: dipendenti, collaboratori, operatori di sistema, impiegati, funzionari etc.
i) *"interessato"*: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali. Esempi: clienti, consumatori, utenti, fornitori, dipendenti di un'azienda o di ente pubblici i cui dati vengano trattati etc.
j) *"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. Esempio: telefonata, fax, mail, corrispondenza cartacea, chat etc.
k) *"diffusione"*: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Esempi: pubblicazione su giornali o su siti web, cartelloni pubblicitari etc.;
l) *"blocco"*, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
m) *"banca di dati"*, qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

NOTE

1. **Il presente regolamento si applica a tutte le operazioni con l'ausilio di strumenti elettronici, che coinvolgono informazioni identificabili come personali, come per esempio: pagamenti, registrazioni, archiviazioni, consultazioni, uso, e/o recupero informazioni (riferito in generale al trattamento).**
2. **Il presente regolamento è volto a far sì che ogni membro dell'A.O. rispetti completamente le normative, i regolamenti e le direttive governative in tema di privacy e protezione dei dati applicabili nelle varie unità operative.**

2.3 Aspetti generali in materia di protezione dei dati personali

I dati personali possono essere trattati solo dopo che i soggetti interessati (o i rappresentanti legali di essi, debitamente autorizzati) siano stati adeguatamente informati:

- delle modalità e delle finalità del trattamento;
- della natura obbligatoria o facoltativa del conferimento dei dati;
- delle conseguenze di un eventuale rifiuto di rispondere;
- dei soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- dei diritti di cui all'art. 7 cit.;
- degli estremi identificativi del titolare e, se designato, del responsabile.

Possono essere previste forme semplificate di informativa, secondo una valutazione effettuata caso per caso, tenendo conto della natura del dato trattato, delle modalità utilizzate, degli scopi perseguiti e delle disposizioni del Garante per la protezione dei dati personali.

Il dato personale può essere trattato solo per gli adempimenti degli obblighi derivanti da leggi, regolamenti, normative comunitarie, per l'erogazione dei servizi e delle attività garantite dall'A.O., nonché per gli obiettivi di business e di ricerca specificati nell'informativa; qualsiasi altro trattamento su quei dati, al di fuori delle previsioni fatte, richiede l'immediato consenso informato, spontaneo, libero e consapevole da parte del soggetto (o del suo rappresentante legale), divenendo altrimenti **illecito**. Il trattamento sarà invece **non conforme**, se devia dalla direzione o dagli scopi originari per i quali era stata data l'informativa e legittimamente raccolto il consenso dell'interessato.

Ai sensi dell'art. 11 del Codice i dati personali oggetto di trattamento devono essere:

- 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 e, se necessario, aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una 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 successivamente trattati.

Il soggetto (o il rappresentante legale di esso) avrà diritto ad accedere alle proprie informazioni personali all'interno degli archivi che custodiscono i dati personali dei membri e degli utenti dell'A.O.. Restano ovviamente sempre salvi i diritti di cui all'art. 7 cit., secondo le forme, le modalità, i termini e le garanzie viste nel paragrafo precedente.

I dati personali cc.dd. sensibili saranno trattati come informazioni *"classificate"* e quindi strettamente *"confidenziali"* di pertinenza dell'A.O.; quest'ultima svilupperà appropriate misure tecnico-organizzative per proteggere comunque ogni dato personale da cancellazioni, alterazioni, modifiche, accessi o diffusioni non autorizzati.

L'A.O. deve ricevere idonea garanzia dalle terze parti, alle quali devono essere trasferiti dati personali (*"Outsourcing"*), a conferma del rispetto degli obblighi di legge in materia di finalità e modalità del trattamento dei dati, nonché per quel che concerne il profilo della sicurezza degli stessi. La garanzia si traduce in un **accordo formale** che sancisce il rispetto delle restrizioni imposte per le modalità dello specifico trattamento.

Il trasferimento di dati personali a terze parti sarà consentito nelle seguenti ipotesi:

- quando il soggetto è stato informato contestualmente al momento della raccolta della possibilità del trasferimento e/o cessione dei dati e abbia prestato il proprio consenso in modo espresso, libero, consapevole e specifico;
- in seguito alla vendita, al trasferimento o alla cessione di risorse ai quali è collegato il dato;
- nei casi in cui il trasferimento risulti obbligatorio, perché esplicitamente previsto da leggi nazionali o locali, normative regolamentari o comunitarie o prescrizioni delle Autorità (giudiziaria, amministrativa, sanitaria, militare etc.).

Il trasferimento avverrà nella forma ordinaria della comunicazione. La diffusione di dati è ammessa solo nei casi espressamente previsti dalla legge o dai regolamenti. **I dati idonei a rivelare lo stato di salute non possono essere diffusi**.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

2.4 Procedure per la designazione dei responsabili

L'A.O., in qualità di titolare del trattamento, ha la facoltà di nominare uno o più responsabili.

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 con apposita lettera di designazione.

Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal **titolare** il quale, **anche tramite verifiche periodiche**, **vigila sulla puntuale osservanza delle istruzioni da lui dettate**.

2.5 Procedure per la nomina degli incaricati del trattamento – Profili di autorizzazione

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 con apposita lettera d'incarico e individua puntualmente l'ambito del trattamento consentito o profilo di autorizzazione. 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.

Per ***"profilo di autorizzazione"*** si intende l'**insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti** (art. 4, comma 3, lett. f) del Codice). Ogni profilo dunque indica il tipo di dati che possono essere trattati e il tipo di trattamenti che possono essere effettuati sugli stessi: rappresenta dunque l'ambito operativo per ogni singolo incaricato, i diritti e privilegi di cui gode (lettura, scrittura, aggiornamento, modifica, rettifica, cancellazione etc.).

Ogni incaricato ha il suo "profilo", gode quindi di determinati privilegi o diritti e può così effettuare specifiche attività rispetto a determinati dati. Per quel che concerne le attività svolte sui sistemi informatici, computer, elaboratori etc., ad ogni operatore corrisponderà un "applicativo" cui corrisponderà a sua volta un determinato profilo. In tal senso ogni operatore, dopo aver acceduto alla macchina, avrà la possibilità di accedere al proprio profilo tramite password personale. Pertanto solo sul suo profilo (e quindi sul proprio applicativo) ogni operatore potrà trattare i dati personali di terzi (che dunque non risiedono sulla macchina, in locale), compiendo le operazioni per le quali ha i necessari e specifici diritti, secondo i principi della *"separazione"* e del *"privilegio minimo"*. Gli applicativi (coi rispettivi profili) sono gestiti a livello centralizzato, in modalità *"server"*, onde agevolare il controllo, anche automatizzato, sul rispetto dei diritti spettanti all'operatore/incaricato. Purtuttavia il **controllo** non potrà mai essere "mirato", ma potrà avvenire **solo per settori**, **reparti** o **aree di riferimento** o d'intervento (su tali aspetti si tornerà successivamente).

Possono esservi più incaricati aventi lo stesso profilo. Si parla in tal caso di *"classi omogenee"* di incaricati (gruppi, reparti, distretti, dipartimenti etc.). Pertanto i **profili di autorizzazione** possono essere stabiliti non solo per unità (ossia per singolo incaricato), ma anche **per reparto** o **per gruppo** (sempre che gli incaricati del reparto o del gruppo svolgano i medesimi trattamenti in relazione ai medesimi dati). L'A.O. ha valutato positivamente (v. il § 1.3 a pag. 10 del presente documento) l'ipotesi di conferire profili di autorizzazione per gruppi omogenei di incaricati, anche in virtù dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per l'esercizio dei diritti da parte degli interessati, nonché per l'adempimento degli obblighi previsti dalla legge (art. 2, comma 2, del Codice)

I profili vanno preventivamente individuati, in modo che si sappia fin da principio *"chi-deve fare-cosa"*, così come vanno preventivamente configurati i sistemi e cioè implementati secondo i profili individuati (si pensi alla configurazione dei *firewall* per l'attribuzione e per la gestione dei privilegi).

Periodicamente, e comunque **almeno annualmente**, **è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione**. In tal senso si provvederà ai necessari e opportuni aggiornamenti dei profili autorizzatori ai sensi del Punto 15 dell'Allegato B al Codice (recante il *"Disciplinare tecnico in materia di misure minime di sicurezza"*; v. anche art. 34, lett. d) del Codice).

Il rispetto del principio della prevenzione nell'individuazione dei profili e nell'implementazione dei sistemi è funzionale al trattamento di quei soli dati indispensabili al raggiungimento delle finalità del trattamento stesso (principi di necessità, di non eccedenza e di pertinenza dei dati rispetto alle finalità da perseguire; v. artt. 3 e 11 del Codice).

2.6 Terze parti

Onde evitare eventuali responsabilità, l'A.O., in fase di accordo con i collaboratori/fornitori attuali o potenziali, dovrà esaminare e valutare in via preventiva, durante la fase di formalizzazione della collaborazione, le misure di sicurezza e le *"best practices"* adottate dai collaboratori/fornitori.

3 CAPO II – Security Policy

3.1 Premessa

Il trattamento dei **dati personali** di utenti interni o esterni dell'A.O. è consentito solo se sono adottate adeguate misure di sicurezza a protezione dei dati stessi.

Pertanto i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico (secondo quindi un approccio *"dinamico"*), alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, 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 (art. 31 del Codice).

In ogni caso dovranno essere almeno predisposte le cc.dd. *"misure minime di sicurezza"*, intendendosi per tali il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il **livello minimo di protezione** richiesto in relazione ai rischi di cui sopra. **L'omessa adozione delle misure minime comporta responsabilità penale ai sensi dell'art. 169 del Codice**.

Analisi, architettura, implementazione di sicurezza e misure protettive devono essere perfezionate nel rispetto delle politiche dell'A.O. relative alla classificazione e valutazione degli *asset* (o beni preziosi) informatici e telematici di proprietà o pertinenza dell'A.O. stessa (risorse hardware, risorse software, supporti di backup e di memorizzazione, documentazione cartacea inerente i sistemi informatici, risorse di rete e soprattutto i dati e le informazioni memorizzati, archiviati, conservati su dispositivi e strumenti elettronici).

Le informazioni devono essere classificate (in base alla natura intrinseca di esse) prima della loro acquisizione al fine di determinarne i relativi criteri di protezione.

Le informazioni critiche devono poter essere valutate, valorizzate e classificate dal responsabile del trattamento dei dati, con cadenza almeno annuale.

Al fine di assicurare una efficace protezione, il valore da attribuire ai dati dovrà essere determinato prima che questi siano rilasciati o trasmessi, con qualsiasi forma di comunicazione, in rete.

Tutte le singole unità dell'A.O. devono effettuare l'inventario delle proprie risorse interne (gli *asset* per l'appunto), valutarne la criticità, determinare quali di esse richiedono una protezione particolare e garantire, per ognuna, l'adeguata procedura di sicurezza. Di tutto ciò dovrà essere redatta e adeguatamente tenuta idonea documentazione.

La sicurezza dei dati è diretta a proteggere:

- la **riservatezza** o confidenzialità: protezione dall'altrui curiosità ovvero da accessi abusivi o da comunicazioni, diffusioni e divulgazioni non lecite o comunque non consentite;
- l'**integrità**: garanzia da modificazioni e cancellazioni non autorizzate, nonché da alterazioni e falsificazioni e protezione contro rischi di distruzione e perdita (anche accidentali) di dati (*"data authentication"*);
- l'**autenticità**: paternità dei dati e delle informazioni, ossia la certezza della loro provenienza (*"entity authentication"*);
- la **disponibilità** dei dati: accessibilità, fruibilità, utilizzabilità;
- la ***business-continuity***, cioè la continuità operativa e istituzionale dell'A.O.

Tutti gli utenti che utilizzano risorse dell'A.O., aventi accesso ad informazioni interne, devono aderire alle politiche dell'A.O. relative alla protezione del patrimonio informatico ed informativo. Tutte le soluzioni di sistema per la protezione delle informazioni trattate dall'A.O. devono rispettare le normative, le leggi, i regolamenti, le direttive e le discipline vigenti. La privacy del personale, dei clienti e dei collaboratori dell'A.O., deve necessariamente essere protetta.

Prima della stessa adozione di misure di protezione delle informazioni, è necessario verificare se gli strumenti elettronici utilizzati:

- siano opportunamente configurati e protetti e dunque in grado di assicurare un elevato livello di tutela e di protezione dei dati, soprattutto in relazione ai diritti e alle libertà fondamentali della persona i cui dati sono trattati;
- siano affidabili, e quindi sicuri, in termini di efficienza e velocità di elaborazione e trasmissione e, nel contempo, siano dotati della manualistica idonea e delle certificazioni di qualità e delle altre omologazioni che ne attestino la conformità agli standard e alle normative tecniche nazionali (es. disposizioni tecniche dettate dal CNIPA) e internazionali (es. standard ISO);

- siano rispettosi del principio di necessità ai sensi dell'art. 3 del Codice, laddove, sempre nell'ottica di minimalizzazione del rischio, si prescrive che *«i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità».*

3.2 Controllo degli accessi logici dei dipendenti – Autenticazione

3.2.1 Definizioni

L'**autenticazione informatica** è presupposto necessario per procedere al trattamento dei dati, quale **primo anello della catena della sicurezza logica**. Per autenticazione si intende *"quell'insieme di strumenti elettronici e di procedure per la verifica anche indiretta dell'identità"* (cfr. l'art. 4, comma 3, lett. c) del Codice) **[4]** ed altro non è che un procedimento automatico per il **riconoscimento o identificazione del soggetto che accede** ad un sistema, computer o elaboratore **per effettuare un trattamento di dati** e cioè per porre in essere concrete operazioni sugli stessi, in virtù dei privilegi attribuitigli con lettera d'incarico (cfr. il paragrafo sulle procedure di nomina degli incaricati a pag. 7 e sg. del presente documento). Quindi l'incaricato prima accede legittimamente al sistema (1° anello: autenticazione), poi può operare sui dati (2° anello: autorizzazione).

Normalmente per accedere al computer ogni incaricato avrà una credenziale di autenticazione costituita dall'**associazione logica** di un identificativo con una parola-chiave, e precisamente dalla **combinazione di *userID* e *password***.

3.2.2 Identificativi

Per quanto riguarda gli "identificativi" o *userID*, è stata adottata una procedura di verifica che consenta di rispettare il precetto secondo il quale un medesimo codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri utenti neppure in tempi diversi.

Il servizio che ne effettua la generazione deve, pertanto, predisporre dei meccanismi di conservazione degli elenchi dei codici identificativi in uso o già assegnati precedentemente.

Ogni volta che deve essere rilasciata un nuovo userID occorre:

- generare il codice identificativo secondo le modalità per esso stabilito (per es. ***nome. cognome*** oppure ***iniziale del nome. cognome*** etc.);
- verificare che il codice identificativo così generato non sia stato già precedentemente assegnato ad altra persona;
- se l'esito del controllo è positivo, lo userID può essere generato e attribuito alla persona che ne ha fatto richiesta;
- nel caso in cui si accertasse che il codice identificativo sia già in uso o sia stato in precedenza assegnato ad altra persona occorre predisporre una combinazione che consenta univocità dell'assegnazione.

Inoltre ad opera del CED viene predisposta una procedura di attivazione al fine di:

- verificare, con cadenza almeno semestrale, la validità di ogni userID: quelli non utilizzati da almeno 6 mesi devono essere sospesi;
- sospendere immediatamente uno userID nel momento in cui viene a cessare il diritto di accesso ai sistemi (per es. in caso di licenziamento, pensionamento, cambiamento di ruolo che non rende più indispensabile l'accesso al sistema);

Le utenze che durante i controlli precedenti sono già state sospese possono essere rimosse o disabilitate solo dopo aver verificato, insieme con il Responsabile dell'utente, a cui si riferisce, la cessazione del diritto che consentiva l'accesso al sistema.

---

[4] Un'altra definizione di autenticazione è offerta dall'art. 1, lett. b) del D.Lgs. 82/2005 e succ. modif., cd. *"Codice delle amministrazioni digitali"*, a mente del quale l'autenticazione consiste nella *"validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso"*.

3.2.3 Password

Per il primo accesso la password sarà fornita dall'amministratore di sistema.

La procedura da seguire per il primo accesso è la seguente:

- il responsabile competente richiede al settore IT (preventivamente e formalmente autorizzato) di associare lo userID alla password iniziale e di creare il profilo di autorizzazione con poteri di accesso ai dati e ai programmi differenziati in base alle effettive mansioni e responsabilità assegnate, come risultanti da lettera d'incarico;
- il responsabile competente richiede al settore IT di associare l'incaricato al **profilo di autorizzazione corrispondente alla classe omogenea** cui l'incaricato stesso appartiene.

Dopo il primo accesso la password dovrà essere sostituita dall'incaricato.

Per quel che concerne nello specifico gli incaricati del trattamento di ogni singolo reparto dell'A.O., è stato previsto un doppio livello di autenticazione secondo la seguente procedura:

- dapprima l'incaricato accede al sistema tramite la password di reparto (quindi condivisa tra i vari incaricati che vi appartengono) che consente semplicemente l'accesso alla macchina;
- una volta acceduto alla macchina, ogni singolo incaricato digiterà la password personale di accesso al proprio profilo o "applicativo", in cui sono presenti i dati personali che egli, come da formale designazione attraverso lettera di incarico, è autorizzato a trattare, ovviamente potendo porre in essere solo quelle operazioni consentite e previste per il suo profilo.

In tal modo i dati non sono mai trattati sulla macchina, e quindi in modalità locale o su *desktop*, bensì solo sui profili di ogni singolo incaricato gestiti in forma centralizzata in modalità *server*. La presente policy vieta espressamente di elaborare e trattare i dati personali in modalità locale o comunque su desktop (es. attraverso l'uso di *editor* o *utilities* di testo come *word* o fogli elettronici come *excel*), valutandosi il contrario comportamento da parte dell'A.O. anche come illecito disciplinare, con conseguente possibilità di irrogazione di sanzioni.

La password di accesso al proprio profilo o applicativo costituisce la **componente riservata** ed assolutamente **esclusiva** della credenziale, pertanto essa non può essere rivelata o comunicata ad altri, né tanto meno diffusa o divulgata, nemmeno se già utilizzata o non più in uso. Nemmeno potrà essere condivisa con altri. V'è dunque l'assoluto divieto di scambio di password o di codici identificativi riservati (es. codici PIN) e di assegnazione della stessa credenziale a più incaricati (divieto di credenziali d'accesso cd. di gruppo o di reparto, salvo che per meri accessi alla macchina per l'uso della stessa, non certo per il trattamento dei dati, per il quale, come detto, esiste un applicativo protetto da password segreta per ogni incaricato).

Ogni incaricato deve custodire gelosamente la propria password. A tutela della segretezza delle credenziali, è fatto assoluto divieto di scrivere la propria password o codice PIN su fogli di carta che restino incustoditi sul tavolo di lavoro o in cassetti non muniti di serratura o su *post-it* che vengono poi attaccati al monitor o sotto la tastiera. È altresì vietato comunicare la propria password via mail o via fax.

Le password non devono essere memorizzate per eseguire accessi automatici al sistema (per es. password memorizzate in macro, *batch* o tasti funzione).

Le password e i codici PIN sono considerati informazioni confidenziali riferibili all'A.O. Per tal motivo, salve eventuali responsabilità civili e penali, la loro comunicazione, rivelazione o divulgazione non autorizzate, all'esterno dell'ente, saranno valutabili come illeciti disciplinari per violazione dell'obbligo di fedeltà (art. 2105 del codice civile), con conseguente possibilità di irrogazione delle sanzioni previste dalle leggi, dai regolamenti, dagli statuti e dai contratti collettivi.

La password, oltre ad essere riservata, deve essere robusta e quindi complessa e nel contempo memorizzabile. In particolare deve presentare le seguenti caratteristiche (cfr. Punto 5 dell'Allegato B al Codice):

- deve essere composta da **un minimo di otto caratteri**, in quanto maggiore lunghezza è sinonimo di maggior sicurezza;
- i caratteri devono essere preferibilmente alfa-numerici (lettere e numeri alternati), così come sarebbe opportuno utilizzare caratteri *unicode* (es. £, $, &, /, §, etc.), sempre che questi ultimi siano accettati dal sistema;
- **non** deve essere **facilmente riconducibile all'incaricato** (nome e cognome, data di nascita, nomignolo del coniuge o di un figlio, attore o sportivo preferito, indirizzi etc.);
- non deve essere banale o simile a quelle già utilizzate;
- non deve consistere in parole che possono essere scritte indifferentemente nell'uno o nell'altro senso;
- può contenere al massimo due digitazioni consecutive di caratteri uguali;
- deve essere **modificata** periodicamente, e precisamente:

- almeno **ogni centottanta giorni** (sei mesi) per le utenze normali (accesso a Internet, navigazione e accesso alla mailbox);
- almeno **ogni novanta giorni** (tre mesi), per il trattamento dei dati sensibili ed eventualmente giudiziari, così come definiti dall'art. 4 del Codice.

➢ deve essere modificata quando si sospetti che terzi ne siano venuti a conoscenza.

Al fine di rendere operativa la disposizione di legge che impone il mutamento della password a cadenze prestabilite (3 o 6 mesi) il sistema informatico può essere cronologicamente configurato per il blocco automatico in caso di non modifica (per es. si potrebbe imporre all'utente di utilizzare un certo numero di password prima di riutilizzarne una già usata). Fanno eccezione a questa regola i PIN che controllano l'accesso a dispositivi sotto l'esclusivo controllo fisico dell'utente **[5]** (per es. token, budge, smart-card etc.).

Non è previsto il blocco degli accessi dopo ripetuti tentativi errati di *login*.

La sessione di collegamento al sistema deve inoltre terminare dopo tre (3) minuti di inattività. Se l'utente deve allontanarsi dalla postazione di lavoro, deve bloccare manualmente l'accesso al computer e comunque, come sopra descritto, l'accesso deve essere bloccato in automatico dopo non più di tre minuti di inattività.

La password deve essere disabilitata, anche in automatico, in caso di non uso da almeno sei mesi. Fanno eccezione quelle credenziali che, seppur scadute nel senso suddetto, siano però ancora utili per le utenze tecniche, vale a dire per scopi di gestione esclusivamente tecnica del sistema (non cioè per scopi di trattamento dei dati).

Devono altresì essere immediatamente disattivate le credenziali dell'incaricato che ha perso (per es. perché licenziato o perché trasferito ad altri incarichi) il diritto di accedere al sistema e che dunque non ne ha più la facoltà o la necessità. In questo senso va prevista una procedura di notifica al settore IT perché si attivi immediatamente per la disabilitazione dell'*account*.

3.2.4 Copie delle credenziali in caso di prolungata assenza ed impedimento dell'incaricato

In linea generale non sono custodite copie delle credenziali di accesso.

In caso di necessità di accesso ai dati, in caso di assenza o impedimento dell'incaricato (per qualsivoglia motivo si siano verificati: ferie, malattia, trasferta etc.), l'A.O. può richiedere ai responsabili IT di ri-impostare le credenziali di accesso dell'incaricato. Nel caso in cui questo si verifichi, l'A.O. provvederà ad informare *ex post* e cioè ad intervento effettuato, l'incaricato assente o impedito, stendendo apposito verbale, in cui verranno spiegate modalità, tempistica, contenuto e motivazioni dell'intervento stesso.

Solo ove non sia possibile, da parte dei responsabili IT, l'attuazione della procedura di ri-impostazione delle credenziali, allora, per iscritto, l'A.O. detta apposite istruzioni per le ipotesi di impedimento o di assenza dell'incaricato affinché le copie delle credenziali (cioè delle password o dei codici PIN) siano custodite in modo che ne sia garantita la segretezza e che siano individuati i soggetti incaricati della custodia e autorizzati a operare il trattamento di dati. Questi ultimi assumeranno la figura di delegati o fiduciari dell'incaricato.

Per la custodia delle password, si dovrà seguire allora la seguente procedura:

➢ la password viene scritta su di un foglio che poi viene collocato in busta sigillata;
➢ la busta viene consegnata al **fiduciario** (o **delegato**), che a sua volta la collocherà in cassaforte o armadietto munito di serratura.

Il fiduciario, qualora si verifichino le evenienze previste (assenze o impedimenti) dell'incaricato sarà autorizzato ad aprire la busta, utilizzare la password per l'accesso e operare i trattamenti necessari. Questi provvederà ad informare *ex post* e cioè ad intervento effettuato l'incaricato assente o impedito, stendendo apposito verbale, in cui verranno spiegate modalità, tempistica, contenuto e motivazioni dell'intervento stesso.

È ovvio che l'impedimento o l'assenza dell'incaricato rilevano come presupposti per l'attuazione della procedura di cui sopra. Tuttavia va valutata la assoluta necessità (indispensabilità) e tempestività (indifferibilità) dell'intervento in relazione ad esigenze operative e di sicurezza. Quanto alle esigenze di sicurezza, *nulla quaestio*, in quanto un intervento potrebbe essere assolutamente richiesto in caso di pericoli o minacce alla riservatezza, integrità o disponibilità dei sistemi ovvero dei dati di uno o più interessati (per necessità, dunque, di tutelarne i diritti). Quanto

[5] Tuttavia anche per i possessori di smart-card o token vale la regola per la quale è assolutamente vietato riportare per iscritto o conservare insieme col supporto hardware i codici PIN o le password necessari all'attivazione del dispositivo stesso così come ne è vietata la condivisione o rivelazione/comunicazione/diffusione.

invece alle esigenze operative, l'espressione va intesa *strictu sensu*, onde evitare di giustificare un qualsivoglia intervento, anche quando non assolutamente necessario.

Ed allora non v'è dubbio che, nell'individuare tali esigenze, bisognerà bilanciare interessi contrapposti quali:

- la necessità di assicurare la continuità dell'attività istituzionale dell'A.O., in relazione all'esercizio delle attività alle quali è preposta e all'erogazione di servizi agli utenti e ai clienti;
- il rispetto del diritto alla protezione dei dati personali, nonché dei diritti di riservatezza, dignità e identità e di tutti gli altri diritti e libertà fondamentali del personale dell'A.O..

Tale bilanciamento dovrebbe essere oggetto di un apposito accordo **sulla base del modello di concertazione previsto dall'art. 4 dello Statuto dei lavoratori** (legge 300/1970), disposizione, tra l'altro, espressamente richiamata dall'art. 114 del Codice, e la cui violazione è penalmente sanzionata ai sensi dell'art. 38 dello Statuto cit. (anche quest'ultima disposizione è richiamata dal Codice, precisamente dall'art. 171).

Per ogni singolo reparto è prevista la figura del custode delle password e/o fiduciario. Per es. custode delle password potrebbe essere un responsabile IT a livello locale, mentre il fiduciario potrebbe essere un primario, un dirigente, un capo-dipartimento, un capo-sezione, un capo-ufficio o un capo-reparto etc.

3.3 Corretto uso e custodia degli strumenti elettronici

L'utilizzo delle risorse informatiche e telematiche di proprietà dell'A.O. deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro. L'A.O. ribadisce la volontà di mantenere un rapporto a carattere fiduciario con i propri collaboratori, ma ritiene comunque utile adottare alcune regole interne di comportamento condivise, dirette a evitare atteggiamenti inconsapevoli e/o scorretti e/o illeciti.

Il dipendente è responsabile degli strumenti che gli vengono forniti per il regolare espletamento delle proprie funzioni ed è pertanto tenuto ad utilizzare tali strumenti correttamente e secondo la diligenza del buon padre di famiglia. Considerando che l'utilizzo degli strumenti elettronici deve essere corretto e lecito, il presente documento resta valido anche qualora il dipendente o il collaboratore utilizzi tali strumenti al di fuori del normale orario di lavoro.

Nell'ambito dei più generali obblighi di protezione e custodia diligente, l'A.O., in qualità di titolare, detta specifiche istruzioni affinché gli strumenti elettronici non siano lasciati incustoditi e accessibili a chiunque durante la sessione di trattamento dei dati (cfr. Punto 9 dell'Allegato B al Codice).

Il concetto di strumento elettronico è quanto mai ampio ed in esso vanno ricompresi:

- server
- PC, terminali, consolle e strumenti siti in una qualsivoglia *workstation* o postazione lavorativa (*modem*, *fax*, stampanti, *router*, *switch*, *hub* etc.);
- computer portatili;
- dispositivi come *memory card*, *badge*, *smart-card* o *token*;
- supporti rimuovibili utilizzati per i *"backup"* (copie di sicurezza) o per la (anche solo temporanea) memorizzazione (es. *CDR*, *floppy-disk*, nastri magnetici etc.)

Ebbene tutti questi strumenti vanno custoditi con adeguate misure di protezione in caso di allontanamento anche temporaneo o in caso di cessazione dell'attività al termine della giornata lavorativa. Siffatte misure sono:

a) logiche: screensaver con password inserita, time-out, impossibilità di memorizzazione automatica della password, etc.
b) fisiche: gli strumenti vanno posti in locali chiusi o comunque ad accesso controllato o limitato ai soli incaricati o a personale autorizzato;
c) procedurali: blocco dei *badge* in caso di smarrimento o furto, disattivazione delle password o dei codici di accesso, etc.

Tali misure hanno come punto di riferimento temporale la sessione di trattamento, cioè il periodo in cui il collegamento è ancora attivo (quando cioè l'incaricato si sia autenticato, abbia ottenuto accesso al sistema, abbia iniziato il trattamento e si sia successivamente allontanato per qualsivoglia ragione).

3.4 Regole per la sicurezza della workstation

- L'utente non deve lasciare incustodita la postazione di lavoro se non in una condizione di spegnimento o di blocco (*screensaver* con password attivata in automatico o manualmente). In alternativa, si deve chiudere a chiave la porta dell'ufficio e la chiave deve essere tenuta dall'interessato ovvero consegnata in portineria o al personale di reparto debitamente autorizzato.
- La scrivania, nell'arco di tempo in cui l'incaricato si allontana, deve essere lasciata libera da qualsiasi supporto elettronico contenente dati personali, specialmente se classificati (sensibili e/o giudiziari)
- I supporti rimuovibili (siano essi magnetici, ottici etc.), se contenenti dati personali, devono essere conservati in appositi cassetti o armadi muniti di serratura. Al termine della sessione lavorativa o nei periodi di temporaneo allontanamento (pausa caffè, pausa pranzo, convocazioni straordinarie, riunioni sindacali o programmatiche etc.), l'incaricato provvede alla chiusura dei cassetti o degli armadi in cui sono riposti i supporti rimuovibili, indi egli ha l'obbligo di portare con sé la chiave e di consegnarla in portineria o al personale di reparto debitamente autorizzato.
- La stazione di lavoro assegnata non deve essere modificata nella sua configurazione hardware e software se non dal personale preposto. È inoltre assolutamente **vietata l'installazione e/o l'utilizzo e/o l'esecuzione di qualunque software non necessario allo svolgimento della propria attività lavorativa** ovvero **non predisposto a servizio o a corredo della postazione di lavoro** o comunque **non fornito o non precedentemente controllato o autorizzato dall'A.O.** Anche i **supporti di provenienza esterna** non possono essere inseriti nel sistema per essere letti, se non previo ***screening*** effettuato dal personale competente e previa autorizzazione dell'amministratore di sistema o del responsabile. Lo screening si rende necessario per l'ovvia ragione che un file o un programma di provenienza esterna potrebbe contenere un *malware* o codice maligno. Di qui la ragione del controllo preventivo. Il mancato rispetto di tali regole comportamentali non permetterà il proseguimento della attività e di conseguenza la macchina sarà riportata agli standard interni, senza ulteriore preavviso. L'A.O. si riserva comunque di effettuare **controlli periodici a campione** su singole macchine per verificare il rispetto di tali regole. Il controllo sarà preceduto da notifica preventiva e, se necessario, l'A.O. si avvarrà di personale specializzato per la ripulitura e/o bonifica della macchina, avviando, se del caso, azione disciplinare nei confronti di colui che si sarà reso responsabile della violazione.
- Per quel che concerne in particolare i software, le banche-dati elettroniche e altri file (audio, video, audio-video, testi, immagini, fotografie), tutti gli operatori di sistema/incaricati si obbligano a rispettare la **legislazione in materia di copyright**, con specifico riferimento alla l. 633/1941 e succ. modif., c.d. "legge sul diritto d'autore". Viene dunque ribadito l'assoluto divieto di istallazione e uso e di qualsiasi altra operazione avente ad oggetto materiale informatico hardware o software illegalmente detenuto, di provenienza illecita, ricettato, contraffatto, duplicato senza autorizzazione. L'installazione di nuovi programmi può creare problemi di stabilità del sistema sul quale sono istallati, con quel che ne consegue in termini di rallentamento del funzionamento, difficoltà di elaborazione delle informazioni, fino alla perdita o cancellazione di dati. L'omessa ottemperanza a tale regola può costituire infrazione disciplinare, salve ovviamente le responsabilità civili, amministrative e penali derivanti dalle violazioni della legge sul diritto d'autore. Per garantire il rispetto della copyright-policy, l'A.O. si riserva (come nel caso precedente) di effettuare **controlli periodici a campione** su singole macchine.

  Si ricordi inoltre che l'A.O. ha adottato sistemi operativi, software applicativi, *utilities*, *tools*, *editor* (elaboratori di testo) regolarmente licenziati o *open source*.
- Nel caso in cui risulti necessaria l'installazione di software, deve essere effettuata apposita richiesta all'Help Desk.
- Non si devono introdurre nella propria stazione di lavoro documenti o files di cui non si conosce la provenienza o non strettamente legati alla propria attività.
- Non è possibile utilizzare a scopo lavorativo strumenti personali (es. portatili non forniti dalla A.O.).
- Più in generale non è consentito l'utilizzo delle infrastrutture ICT dell'A.O. (es. computer, reti, numeri verdi, etc.) per un uso non strettamente lavorativo o comunque non istituzionale.

3.5 Procedure e misure di sicurezza contro specifici rischi

3.5.1 Procedura anti-virus (AV)

L'A.O. ha un sistema anti-virus (di seguito AV) gestito in modalità centralizzata, anche per evitare l'inconveniente o comunque il pericolo che la configurazione del medesimo su ogni singola macchina sia arbitrariamente modificata.

L'AV è sempre attivo e **costantemente aggiornato** in maniera automatica (in modalità *"live update"*). In caso contrario, laddove vi sia stata notifica da parte dei responsabili del settore IT ai singoli operatori/incaricati, l'accesso a documenti provenienti dall'esterno del proprio computer (per es. floppy-disk o CDR o anche dal web) dovrà avvenire solo dopo la comunicazione ufficiale (sempre da parte dei responsabili del settore IT) dell'istallazione degli ultimi aggiornamenti dell'AV.

Nei casi di necessità e di urgenza, laddove senza ritardo debba essere istallato un supporto o aperto ed eseguito un file o attivato un programma, uno dei responsabili del settore IT appositamente autorizzato effettuerà in locale lo *screening* del supporto o file o programma.

3.5.2 Aggiornamenti del sistema operativo

Allo scopo di prevenire *bug* o vulnerabilità del sistema operativo, è necessario aggiornare periodicamente i programmi tramite l'utilizzazione di *"patch"* o *"hotfix"*, che vengono periodicamente rilasciate dalle software-house che hanno programmato e implementato il sistema operativo stesso (cfr. il Punto 17 dell'Allegato B al Codice).

L'aggiornamento può avvenire in automatico. Laddove ciò non fosse possibile, sarà cura dell'incaricato provvedere a ciò manualmente ovvero, in difetto delle necessarie conoscenze tecniche, informare prontamente l'amministratore di sistema o il responsabile affinché provveda.

La frequenza degli aggiornamenti dovrebbe essere almeno mensile e comunque il sistema va aggiornato non appena possibile. Gli aggiornamenti devono essere approvati dai responsabili del settore IT per evitare effetti collaterali ed incompatibilità.

3.5.3 Firewall

I dati contenuti nei sistemi, soprattutto se trattasi di dati sensibili e/o giudiziari, devono essere protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale mediante l'utilizzo di idonei strumenti elettronici (cfr. Punto 20 dell'Allegato B al Codice).

A tale scopo esistono particolari programmi denominati *"firewall"*, utilizzati per il filtraggio dei dati e dei pacchetti provenienti dalla rete Internet, al fine di proteggere un qualsiasi sistema da tentativi di intrusione (es. da parte di *hacker* o *cracker*). Il firewall consente solo il passaggio di determinati tipi di dati, da determinati server, terminali o utenti. Il firewall oltre ad essere software (e in tal caso è montato su ogni singola macchina) può essere implementato anche su di una macchina dedicata (software + hardware) ed in tal senso può essere gestito in modalità centralizzata.

L'A.O. ha optato per tale ultima soluzione e precisamente si serve di un *cluster* di due macchine su piattaforma *Linux*.

3.5.4 Backup

La generazione di **copie di sicurezza** o backup può essere gestita da remoto tramite *storage* centralizzato ed in *real-time* su server appositamente predisposto dall'A.O.

Laddove ciò non fosse possibile saranno i singoli incaricati, appositamente nominati e col compito specifico in tal senso assegnato, a effettuare i backup su supporti rimuovibili (CDR, DVD, nastri magnetici etc.) con frequenza almeno settimanale. I supporti dovranno poi essere ricoverati in locali controllati e protetti e la procedura, da precisarsi nella lettera di incarico, dovrà indicare:

- chi deve effettuare i backup, su quali formati elettronici, su quali supporti e con quale frequenza;
- a quali dati va conferita priorità di copia;
- dove i backup vanno riposti;

- chi li deve custodire, chi li può prelevare e chi li può utilizzare e per quali scopi;
- come archiviarli e cioè come etichettarli ed inventariarli.

Quanto ai supporti, l'A.O. ha optato per i **nastri e hard disk rimovibili** e la frequenza delle copie di sicurezza è quotidiana.

Nell'ipotesi di backup generati attraverso trasferimento telematico di dati (c.d. *storage* da remoto), il trasferimento dovrà avvenire in forma crittografata o comunque protetta (es. in file *.zip* o *.rar* protetti da password robuste).

Tutte le risorse (hard-disk, floppy-disk, CDR, DVD, nastri etc.) che contengono o abbiano contenuto informazioni critiche (con particolare riferimento ai dati sensibili o giudiziari) devono essere controllate per garantire che tutti i dati siano stati rimossi prima di essere adibite ad altro uso (Punto 22 dell'Allegato B al Codice) con idonee procedure di *wiping* (se riutilizzabili da personale diverso da quello precedentemente incaricato) o, se non più riutilizzabili, tramite smagnetizzazione dei supporti rimuovibili o tramite distruzione (annientamento fisico) degli stessi.

3.5.5 Ulteriori misure di sicurezza per dati sensibili e giudiziari

Per tutti i dati sensibili ed eventualmente giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, è obbligatorio usare la crittografia o tecniche simili, purché sia garantita la temporanea inintelligibilità anche per chi è autorizzato all'accesso e purché l'identificabilità sia strettamente indispensabile.

In alternativa alla crittografia è possibile avvalersi il metodo c.d. di *"**disgiunzione dei dati**"* attraverso l'anonimizzazione del dato identificativo (nome e cognome dell'interessato/paziente) tramite l'uso di codici (numerici o alfanumerici) corrispondenti a quel dato, in modo che sia visibile solo la diagnosi senza alcun riferimento all'interessato, con possibilità di ricongiungere i dati (identificativi e sensibili) solo ove necessario (es. per la prognosi, per l'erogazione della cura o della terapia etc.). **Tale sistema è stato adottato dall'A.O.**

Il rispetto di tali regole è necessario in quanto i dati sulla salute e sulla vita sessuale (cd. *"dati supersensibili"*), per espressa disposizione legislativa, devono essere conservati in cartelle o archivi elettronici separati da altri dati personali trattati per finalità che non richiedono il loro utilizzo. **I dati sulla salute non possono essere diffusi**.

Oltre al rispetto per gli adempimenti in materia di protezione dei dati personali, deve essere mantenuto il più assoluto riserbo anche al fine di osservare l'obbligo del **segreto professionale** da parte del personale medico e paramedico.

3.5.6 Istallazione di misure di sicurezza da parte di soggetti esterni alla struttura

In caso di predisposizione delle misure minime di sicurezza da parte di soggetti esterni (fornitori dell'A.O.), sarà cura dei responsabili designati ovvero degli incaricati appositamente delegati dall'A.O. stessa o dai responsabili farsi rilasciare una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico in materia di misure minime di sicurezza (per l'appunto, l'Allegato B al Codice). Ottimo parametro per la valutazione dell'affidabilità delle misure minime istallate da parte di personale esterno è costituito dalle certificazioni standard di sicurezza (ITSEC, ISO etc.) dei prodotti software e hardware. Ma ciò potrebbe non bastare, poiché, se il prodotto è male istallato o non adeguatamente mantenuto, le misure si riveleranno inefficaci. A questo punto, le varianti da considerare al fine di valutare le rispettive responsabilità per danni eventualmente causati per perdita o distruzione di dati ovvero per accessi abusivi o trattamenti illeciti e/o non conformi, saranno più d'una, ed in particolare:

- **qualità del prodotto**;
- **competenza degli installatori**;
- **competenza dei manutentori**;
- **competenza dell'utente**.

3.6 Uso della posta elettronica

3.6.1 Caratteristiche di ordine generale e controlli sulla mailbox degli incaricati

Il dipendente è tenuto ad un corretto uso dei servizi informatici che l'A.O. gli mette a disposizione per svolgere la propria attività lavorativa. Tra essi v'è anche la **casella di posta elettronica** (cd. *mailbox*). Essa, seppur contraddistinta da diversi *username* di identificazione e password di accesso, è da ritenersi **equiparata ai normali strumenti di lavoro** dell'ente e viene quindi messa a disposizione dei singoli dipendenti o collaboratori per lo svolgimento dell'attività lavorativa agli stessi demandata. L'uso improprio della posta elettronica costituisce violazione dell'obblighi di diligenza e fedeltà di cui agli artt. 2104 e 2105 del codice civile con conseguente possibilità per l'A.O. di irrogare sanzioni disciplinari al lavoratore che per l'appunto la utilizzi indebitamente.

La casella di posta elettronica è dunque di proprietà dell'A.O., considerando anche che in genere l'account è così contraddistinto: nome (o semplice iniziale).cognome dell'incaricato@ente.it (es. *m.rossi@aospterni.it*).

L'account è pur sempre riservato, ma in tali casi **personalità dell'indirizzo non significa *"privatezza"*** del medesimo poiché l'indirizzo aziendale – al di là dell'uso di intestazioni apparentemente personali del lavoratore quale principale utilizzatore – proprio in quanto tale, per sua intrinseca natura, può sempre essere nella disponibilità di accesso e lettura da parte di soggetti diversi, sempre appartenenti alla struttura aziendale, rispetto al suo consuetudinario utilizzatore al fine, per esempio, di consentire la regolare continuità della attività dell'ente nelle frequenti ipotesi di sostituzioni di colleghi per ferie, malattia, gravidanza etc. Pertanto, **così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale**, **parimenti non appare astrattamente prospettabile un suo diritto all'utilizzo esclusivo e riservato di una casella di posta elettronica aziendale**.

Ciò implica che su richiesta dell'A.O. i responsabili dell'IT possano accedere alla mailbox, eventualmente modificando le credenziali di accesso. L'A.O. provvederà ad informare ex post (cioè ad intervento effettuato) la persona, stendendo apposito verbale, in cui verranno spiegate modalità e motivazioni dell'intervento stesso.

Sarà cura dell'A.O. mettere a disposizione dell'incaricato anche apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente in caso di assenze (per es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le *"coordinate"* (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto dell'incaricato assente o della struttura. Preferibilmente dovrebbero essere indicati account generici, es. *info@ente.it* oppure *urp@ente.it* oppure *ufficioreclami@azienda.it* (account cc.dd. condivisi), senza che sia indicato un account specifico né un numero interno. Non deve essere indicato il motivo dell'assenza. Allo stesso modo non deve essere indicata la propria mailbox privata (non aziendale) o il proprio numero di cellulare. È opportuno indicare il numero del centralino generale o di reparto, ove il mittente possa far presente le proprie esigenze.

I messaggi di posta elettronica dovranno contenere un *disclaimer* o avvertimento, rivolto ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute anche da altri membri dell'organizzazione di appartenenza del mittente, con eventuale rinvio alla policy adottata dalla stessa.

Stanti i principi di necessità, proporzionalità (pertinenza e non eccedenza), finalità, liceità, correttezza e trasparenza del trattamento dei dati personali, il controllo o il monitoraggio delle mail non potrà che essere graduale, dovendosi così escludere l'ammissibilità di controlli prolungati, costanti o indiscriminati e sono comunque vietate la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail. Trattandosi poi di controlli a distanza sarà certamente applicabile la disciplina di cui all'art. 4 della legge 300/1970, in modo che la policy sia trasparente e condivisa tra ente e lavoratori.

Ogni forma di controllo occulto è vietata e comunque l'A.O. non utilizza *"sniffer"* o altri dispositivi hardware o software finalizzati all'intercettazione e/o all'interruzione e/o all'impedimento di comunicazioni telematiche, come quelle che avvengono tramite e-mail.

3.6.2 *Best practices* per un corretto uso della posta elettronica (codice etico)

- La casella di posta interna deve essere utilizzata esclusivamente per le comunicazioni inerenti la propria funzione lavorativa e le mansioni assegnate. È generalmente vietato l'uso a carattere personale (messaggi ad amici, corrispondenza sentimentale, appuntamenti extra-lavorativi, ordinazioni via mail a imprese commerciali etc.), ma è tollerato un uso minimo e per comunicazioni urgenti a familiari o parenti. Sarà cura dell'A.O. predisporre eventuali macchine di contenimento per l'uso privato della posta elettronica da parte dei lavoratori.
- Le e-mail non provenienti dagli organi apicali o dagli organi di management dell'A.O. ovvero provenienti da mittenti sconosciuti o con oggetto in lingua straniera o allusivo o non facente riferimento all'attività dell'ente, devono essere cestinate senza essere lette e immediatamente cancellate dal cestino.
- È assolutamente vietato eseguire o estrarre gli allegati delle e-mail, del cui contenuto o della cui provenienza non si è sicuri (si pensi a messaggi con oggetto in lingua straniera o in apparenza accattivante e stimolante la curiosità): gli allegati possono, infatti, contenere virus o altri codici maligni, nascosti nell'allegato (tecnica *"troiana"*), che possono avere come scopo o effetto l'indebita appropriazione e divulgazione di password o di altri codici d'accesso ovvero il danneggiamento di dati dell'A.O. ovvero l'interruzione, anche solo temporanea o parziale, del funzionamento dei sistemi informatici o la compromissione della loro sicurezza. Tuttavia è possibile configurare il firewall per bloccare preventivamente mail con allegati infetti o per effettuare lo screening preventivo degli stessi. Nel caso comunque che mail con allegato provengano da persone note, è buona prassi chiedere prima conferma per telefono.
- È vietato cliccare sui *link* presenti nel corpo delle mail di incerto contenuto o provenienza (ut supra): anche il click su tali link potrebbe attivare virus e altri codici maliziosi, come sopra visto per gli allegati o potrebbe comunque attivare procedure di *download* (o comunque consentire l'intrusione) di codice arbitrario o malizioso (*cross site scripting* o *XSS*).
- Non è consentito utilizzare l'indirizzo di posta elettronica lavorativo per inviare o memorizzare messaggi (interni o esterni) di natura minatoria, ingiuriosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, così come più in generale è assolutamente vietato utilizzare la mail per commettere reati di ogni sorta (es. trasmissione, in HTML o in allegato, a una o più persone, di immagini o file pedopornografici ovvero archiviazione dei medesimi in cartelle di posta appositamente create; rivelazione di password o di codici d'accesso, indebitamente ottenuti, a terze persone, con o senza compenso; tentativi di estorcere danaro dietro minaccia; istigazione a delinquere o a violare le leggi dello Stato; propaganda sovversiva o a scopo terroristico; istigazione all'odio razziale…).
- Non è consentito utilizzare l'indirizzo di posta elettronica lavorativo per la partecipazione, in Internet, a dibattiti, *forum*, *newsgroup* o *mailing-list* non attinenti all'attività istituzionale dell'ente o estranei all'attività lavorativa.
- Non è consentito aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare (verso ulteriori indirizzi e-mail) contenuti o documenti oggetto delle cosiddette *"catene di S.Antonio"*, così come è vietato inoltrare falsi allarmi, false richieste di aiuto etc. (*joke*, *hoax* etc.).
- È vietato trasmettere materiale commerciale e/o pubblicitario non richiesto.
- È vietato utilizzare la posta elettronica per comunicare ad altri utenti informazioni di qualsiasi tipo relativamente ai virus. Questa misura serve ad evitare l'invio di un elevato numero di messaggi del tipo *"c'è un virus in circolazione"*. In caso di sospetta presenza di virus informatico, bisogna invece avvisare telefonicamente l'Help Desk che fornirà le indicazioni su come operare.
- È assolutamente vietato inviare messaggi di posta elettronica in caso di accertata presenza nel sistema di virus informatici o di altri *malware* (codici maligni): la posta elettronica potrà essere riutilizzata solo dopo la rimozione del virus.
- Bisogna porre particolare attenzione ai messaggi con i quali si richiedano al lavoratore la comunicazione di password o di altri codici identificativi che devono restare riservati: in genere essi non vengono richiesti via mail, ma per la comunicazione vengono utilizzati canali più sicuri e comunque ufficiali e autorizzati dall'A.O.. Potrebbe infatti trattarsi di attività fraudolente di social engineering (*ingegneria sociale* o *"arte dell'inganno"*), quali lo *scam* (truffa alla nigeriana), il *phishing* o altri tentativi di furto di identità (*"identity theft"*).
- In caso di *spamming* (comunicazioni pubblicitarie non sollecitate o pubblicità indesiderata), è consigliabile non rispondere, soprattutto a fronte di messaggi che invitano a cancellarsi con un click su una determinata area della mail contraddistinta da un link. Infatti il click non serve ad altro che a far sapere allo *spammer* che l'account è attivo.
- Non è consentito effettuare comunicazioni di tipo finanziario, ivi comprese le operazioni di *remote banking*, né possono essere poste in essere attività di *e-commerce*, acquisti on-line e simili, salvo diversa ed esplicita autorizzazione e sempre per finalità istituzionali.
- Non è consentito simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi (c.d. *mailspoofing*).

- L'utente non può esprimere via mail posizioni che facciano ritenere che egli stia parlando in nome e per conto dell'A.O., a meno che non sia stato appositamente delegato o autorizzato per farlo.
- Non è consentito prendere visione della posta altrui, se non a fronte di apposita delega da parte del proprietario della casella postale (vedi la procedura di cui al paragrafo precedente).
- Il lavoratore non utilizzerà sistemi *client* di posta elettronica che non siano stati previamente testati e autorizzati dai responsabili IT dell'A.O.: infatti in seguito alla semplice visualizzazione della posta scaricata nell'anteprima di molti client, quando il formato utilizzato è quello *"HTML"*, è possibile contrarre virus o altri codici maliziosi. Onde evitare inutili rischi, sempre che si voglia utilizzare un client di posta elettronica, risulterà molto utile disattivare la cd. *"anteprima"*, come per es. quella di *"Outlook Express"*.
- Non è consentito l'utilizzo di programmi di crittografia e steganografia non previsti esplicitamente dal *security management* dell'A.O..
- Per quanto possibile, non dovrebbe consentirsi la comunicazione di dati delicati come quelli sensibili o giudiziari attraverso la mail, salve eventuali cautele stabilite dall'A.O. (per es. posta elettronica certificata, protocollo *S/Mime*, utilizzo di allegati compressi e protetti con password robuste o cifrati tramite l'uso di crittografia simmetrica DES, 3DES o meglio AES, etc.). E in tal senso va incentivato e favorito l'uso della **posta elettronica certificata** o **P.E.C.** (v. D.P.R. 68/2005 e art. 48 del D.Lgs. 82/2005 e succ. modif.), almeno per le comunicazioni di carattere ufficiale (per es. contatti con enti pubblici o con aziende fornitrici) e per la trasmissione di dati particolarmente delicati (es. dati sensibili, soprattutto quelli sulla salute e sulla vita sessuale) in modo che possa esserne garantita l'inalterabilità, l'integrità e l'autenticità per tutto il corso della trasmissione del file da una mailbox all'altra, dal momento dell'invio/inoltro a quello di arrivo (momenti entrambi che la tecnologia della P.E.C. è in grado di certificare e di rendere certo e opponibile a terzi).
- La mail deve essere firmata (basta la semplice indicazione del nome e cognome del mittente), ma non va assolutamente usato lo *specimen*, ossia l'immagine scannerizzata della propria firma fisica. Semmai si possono utilizzare software per la generazione di firme digitali o comunque, per le comunicazioni ufficiali (v. punto precedente) è sempre preferibile l'uso della posta elettronica certificata.

Qualsiasi utilizzo non conforme alla presente policy e/o alle leggi vigenti resterà esclusivamente a carico dell'utilizzatore, che se ne accollerà le rispettive responsabilità e conseguenze sul piano civile, penale, disciplinare. A tal proposito l'A.O. si riserva il diritto di verificare l'attuazione della policy e di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato, mentre si riserva di agire comunque sotto il profilo civilistico e disciplinare in caso di ogni tipo di violazione o di illecito, anche se non rivesta rilevanza penale.

3.6.3 Disclaimer

Tutti i messaggi di posta elettronica, relativi alle attività lavorative, dovrebbero contenere la seguente avvertenza o *disclaimer*:

> *"Le informazioni trasmesse attraverso la presente comunicazione via mail, ivi inclusi gli allegati, sono da ritenersi strettamente confidenziali ed esclusivamente spettani all'effettivo destinatario indicato come tale. Qualora il messaggio Vi/Le fosse pervenuto per errore, Vi/La invitiamo ad eliminarlo senza copiarlo e a non inoltrarlo a terzi, dandone gentilmente comunicazione al mittente. Eventuali violazioni saranno perseguibili ai sensi del D.Lgs. 196/2003 ("Codice in materia di protezione dei dati personali") e dell'art. 616 e ssgg. del codice penale). Grazie"*

Nel caso invece di comunicazioni strettamente riservate, in quanto coperte anche da segreto professionale, il disclaimer dovrebbe essere più stringente e avere il seguente tenore:

> *"Il presente messaggio di posta elettronica ed i suoi allegati sono strettamente confidenziali, in quanto rivolti esclusivamente al/ai destinatario/i identificato/i e sono inoltre tutelati dal segreto professionale. Ne sono dunque proibiti l'intercettazione, la lettura, la consultazione, la duplicazione, la modificazione, l'alterazione, la falsificazione, il blocco, la comunicazione, la rivelazione, la divulgazione, la diffusione e ogni altra forma d'uso da parte di chiunque non sia stato espressamente autorizzato. Se non siete il/i destinatario/i oppure avete ricevuto questo messaggio per errore, siete esplicitamente diffidati da ogni e qualsivoglia utilizzazione non consentita, sia ai sensi del D.Lgs. 196/2003 ("Codice in materia di protezione di dati personali", altrimenti detto "Codice della Privacy"), sia ai sensi dell'art. 616 e seguenti del codice penale (che puniscono i delitti contro l'inviolabilità dei segreti). Pertanto La/Vi invitiamo a eliminare immediatamente il messaggio e gli allegati dal Suo/Vostro account di posta elettronica, dandone prontamente comunicazione via mail al mittente. Grazie"*

NOTA

La medesima tipologia di disclaimer potrebbe essere utilizzata anche per le comunicazioni via fax, salvo vietare che quelle contenenti dati sensibili e/o giudiziari o notizie coperte da segreto professionale o scientifico possano avvenire tramite tale forma di trasmissione. Ad ogni modo, prima dell'invio di fax, è opportuno assicurarsi telefonicamente che il destinatario effettivo sia davanti alla macchina.

3.7 Navigazione in Internet

3.7.1 Controlli legittimi

Tutte le risorse informatiche e di rete di proprietà dell'A.O. devono essere protette.

L'accesso ad Internet, tramite risorse informatiche e di rete dell'A.O., deve avvenire in modalità sicura, per garantire la protezione degli asset e delle informazioni dell'A.O. stessa. Gli utenti dovranno essere identificabili individualmente prima di poter avere accesso ad Internet. L'A.O. si riserva il diritto di filtrare la navigazione su Internet, a cui è possibile accedere tramite connessione aziendale.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, l'A.O. può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un **controllo preliminare su dati aggregati**, **riferiti all'intera struttura lavorativa o a sue aree**.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o al settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

L'A.O. utilizza, attraverso personale tecnicamente competente, preventivamente reso noto agli utilizzatori e agli operatori di sistema, strumenti elettronici sia per esigenze produttive e/o organizzative (per es. per rilevare anomalie o per ordinaria e/o straordinaria manutenzione), sia per esigenze di sicurezza sul lavoro. Nelle suddette ipotesi l'A.O. si avvarrà legittimamente, nel rispetto dell'art. 4, comma 2, dello Statuto dei Lavoratori di sistemi informatici ed elettronici che consentono **solo indirettamente un controllo a distanza** e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò sarà possibile anche in presenza di attività di controllo discontinue. In tal senso strumenti leciti si rivelano i firewall, gli IPS, gli IDS e i registri dei *log*.

Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori (come per es. in caso di introduzione di controlli degli accessi in taluni locali o aree *"sensibili"* o ad alto rischio attraverso credenziali biometriche o dispositivi RFID).

L'A.O., nell'esercizio delle sue prerogative datoriali di direzione e organizzazione del lavoro (v. art. 2086 del codice civile), si riserva periodicamente, e almeno su base annuale, di porre in essere le seguenti attività:

- selezione del personale autorizzato alla navigazione online;
- valutazione dell'impatto dei controlli sui lavoratori;
- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni – reputate inconferenti con l'attività lavorativa – quali l'accesso a determinati siti (inseriti in una sorta di black list) e/o l'*upload* e/o il *download* di file o software aventi particolari caratteristiche (per dimensioni o per contenuto);
- trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (per es., con riguardo ai file di log riferiti al traffico web, il trattamento deve avvenire su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati attraverso i registri di *log* e comunque almeno per 18 mesi, estensibili a 24 in caso di illeciti particolarmente gravi, sempre salva diversa disposizione dell'Autorità giudiziaria; la conservazione deve essere strettamente limitata al perseguimento di finalità organizzative, produttive, di sicurezza nonché di prevenzione e/o accertamento di reati ovvero alla possibilità di svolgere attività di investigazioni difensive oppure di esercitare o far valere un diritto in giudizio.

I sistemi software devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione come, per es., la cd. *rotazione dei log file*) i dati personali

relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria (principi di necessità e proporzionalità ai sensi degli artt. 3 e 11 del Codice).

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario – e predeterminato – a raggiungerla (v. art. 11, comma 1, lett. e), del Codice).

Un eventuale **prolungamento dei tempi di conservazione** va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari (incidente informatico di particolare rilevanza, come un attacco *DoS* o *DDoS* o la diffusione di un *worm* distruttivo o compimento di un reato grave di cui non si sia potuta accertare la responsabilità etc.);
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

Altrimenti, scaduti i termini senza che siano stati ottenuti risultati o senza che si siano prese iniziative o senza che si siano attivate le autorità competenti, i log devono essere cancellati o in alternativa possono essere copiati su supporti rimuovibili e chiusi in cassaforte per un periodo corrispondente a quelli sopra indicati

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

I dati raccolti sono adeguatamente protetti contro rischi di indebita visualizzazione, manipolazione, alterazione, falsificazione, cancellazione, distruzione o perdita.

3.7.2 Limiti all'attività di controllo

Nell'esercizio delle sue prerogative datoriali in relazione per l'appunto ai controlli sull'attività dei dipendenti, in modo da assicurare il corretto svolgimento delle mansioni e il lecito, diligente e leale uso degli strumenti elettronici per l'espletamento delle mansioni lavorative, l'A.O. rispetterà nella maniera più assoluta la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (art. 4, primo comma, legge 300/1970), tra le quali sono certamente comprese strumentazioni hardware e software mirate al controllo dell'utente di un sistema di comunicazione elettronica. Con ciò volendosi altresì dire che i controlli sono legittimi solo se non sono occulti ovvero, a prescindere addirittura dalla consapevolezza o meno dell'esistenza degli stessi, se non sono diretti, prolungati, costanti, indiscriminati o mirati su determinati lavoratori o comunque eccessivi, pervasivi e *"mobbizzanti"*.

In tal senso l'A.O. non pone in essere controlli volti alle seguenti finalità:

- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore, anche per ottemperare al precetto di cui all'art. 8 dello Statuto dei lavoratori;
- lettura e registrazione dei caratteri digitati tramite la tastiera (*keylogging*);
- intercettazione di comunicazioni telematiche (es. di telefonate effettuate con tecnologia VOIP) o comunque monitoraggio mirato dei siti visitati da un determinato utente.
- analisi occulta di computer portatili affidati in uso.

Più in generale l'A.O. non utilizza, in quanto vietati, strumenti e dispositivi hardware o software come gli *sniffer* (v. anche il paragrafo dedicato ai controlli sulla mailbox aziendale), *keylogger* (tracciatori di chiavi attraverso la digitazione della tastiera) o *trojan-spy* (software che occultamente spiano o monitorizzano l'attività su protocollo TCP/IP dell'utente).

In tutti i casi predetti, salve resta sempre (anche in caso di controlli leciti) impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice), salve ulteriori azioni nelle competenti sedi giudiziarie, laddove si ravvisino gli estremi di illeciti compiuti dalla struttura datoriale e apicale.

3.7.3 Regole per una sicura e legittima navigazione in Internet (codice etico)

- L'accesso a Internet deve essere autorizzato dal proprio direttore o dal responsabile di reparto, tramite un apposito modulo cartaceo (es. lettera di incarico) e la navigazione deve avvenire esclusivamente a fini lavorativi.
- È vietato svolgere attività di *e-commerce*, *shopping* virtuale o *trading online*.
- È vietato scaricare software da siti web; dove ciò sia assolutamente necessario a fini lavorativi, gli utenti devono accertarsi che siano state adottate le opportune precauzioni per proteggere le risorse di A.O., informatiche e di rete, quando si scaricano programmi, file o dati da Internet. È richiesta la conformità totale alle regole della policy AV (cfr. il paragrafo dedicato alla procedura AV a pag. 14 del presente documento), con particolare riferimento al divieto di *download* di immagini (*.jpg*, *.gif* etc.) o di file di testo cc.dd. a rischio (es. i formati *word* con estensione *.doc* o altri formati come *excel*, che potrebbero contenere *macro*) o file audio o video o audio-video (quale che ne sia l'estensione: *.mp3*, *.avi*, *.mpg*, *.wmv* etc.), salvo autorizzazione e salvo lo screening preventivo. Gli utenti non devono intenzionalmente sviluppare, scaricare o in qualche modo installare programmi o altri software che possano insidiare risorse informatiche o di rete dell'A.O. e/o danneggiare o modificare il software, l'hardware o le informazioni in tali risorse contenute. I file cc.dd. ***eseguibili*** (con estensioni *.exe*) e in genere i file con estensioni a rischio (*.cab*, *.com*, *.pif* etc.) non devono mai essere aperti, salvo *screening* preventivo e autorizzazione dei responsabili del settore IT.
- In generale è proibito svolgere sulla rete ogni attività vietata dalla legge dello Stato, dalle normative vigenti nei Paesi ospitanti i servizi di rete che vengono acceduti e dalla normativa internazionale, nonché dai regolamenti e dalle consuetudini di utilizzo delle reti e dei servizi di rete acceduti (*netiquette*). Sono dunque consentite solo le attività che non arrechino danno ad altri utenti o all'A.O. e che comunque non siano in contrasto con il presente documento e con le norme legislative vigenti.
- È assolutamente vietato accedere abusivamente a sistemi informatici altrui o intrattenervisi senza il consenso dell'avente diritto, ovvero diffondere *virus*, *worm*, *trojan*, *bot* o altri programmi la cui presenza danneggia la rete e/o le risorse ad essa collegate, così come è vietato intercettare abusivamente comunicazioni telematiche altrui, pubblicare su siti web password o altri codici d'accesso (atti di criminalità informatica - legge 547/1993).
- È assolutamente vietato compromettere l'integrità dei sistemi o dei servizi o delle risorse di rete attraverso attacchi *DoS* o *DDoS* (diniego di servizio, *syn-flooding*, *net-straking*, *mail-bombing*), avvalendosi o meno di programmi maliziosi, come *worm* o *bot* o *backdoor* o *rootkit*.
- È assolutamente vietato violare la privacy di altri utenti e più in generale l'integrità e la riservatezza di dati personali altrui, così come è vietato utilizzare servizi o risorse di rete in modo da danneggiare o molestare altre persone o da attentare alla dignità umana (es. realizzazione di servizi di *internet relay chat* o *blog* o *forum* o *newsgroup* o siti a sfondo terroristico, razzista, diffamatorio, pedopornografico o inneggianti all'odio religioso etc.).
- È assolutamente vietato creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno o indecente, specialmente se riguardante il sesso, la razza o il credo.
- È vietato creare o trasmettere materiale finalizzato allo scopo di arrecare disturbi o produrre ingiustificate preoccupazioni (es. falsi allarmi, *catene di Sant'Antonio*, *joke*, *hoax* etc.).
- È assolutamente vietato il consumo di risorse in misura tale da compromettere l'efficienza di altri servizi di rete, per es. occupando indebitamente la banda di trasmissione tramite servizi di *peer-to-peer* o di *file-sharing*, sia in *upload*, sia in *download*, sia in condivisione, condotte tra l'altro sanzionate, a seconda dei casi, in via civile, amministrativa e penale dalla legge sul diritto d'autore (legge 633/1941 e successive modifiche; v. anche pag. 14 del presente documento).
- È vietato usare sistemi cc.dd. *"rogue"*, quali *notebook*, cellulari non aziendali, *laptop*, *I-Pod*, lettori *mp3* in particolare per effettuare il *download* dalla rete, se non sono stati preventivamente autorizzati.
- È assolutamente vietato impedire l'uso della rete ad altri utenti legittimi, per esempio sovraccaricando le linee di accesso o gli apparati di commutazione, ovvero accedere alla rete con apparecchiature o software che interferiscono con il corretto funzionamento della rete stessa o di altre reti ad essa collegate.
- È assolutamente vietato permettere il transito di dati e/o informazioni sulla rete tra due soggetti entrambi non ammessi all'accesso sulla rete intranet (*third party routing*).
- Possono essere visitati solo siti a carattere istituzionale e per scopi strettamente legati all'espletamento delle proprie mansioni lavorative o comunque per necessità professionali, di aggiornamento professionale, normativo etc. È assolutamente vietato visitare siti illegali (es. siti di cracking o diffamatori o pedopornografici etc.) e a rischio (siti commerciali, siti pornografici, *BBS* clandestini etc.). Per la navigazione non istituzionale l'A.O. si riserva di mettere a disposizione dei lavoratori macchine di contenimento per gli orari di pausa, sempre che la navigazione non avvenga per scopi illeciti o comunque su siti illegali e a rischio. In alternativa l'A.O. si riserva di istallare strumenti necessari al filtraggio dei contenuti (*URL filtering* o *content filtering*), per mezzo dei quali in via preventiva è inibito l'accesso a determinati siti che presentino un determinato indirizzo IP o URL o particolari stringhe di testo, *tag*, *directory* etc. Attualmente l'A.O. ha in essere un accordo con l'ISP *Telecom* in base al quale l'uscita sulla rete

Internet è possibile solo passando per il *router* dell'A.O. stessa, senza possibilità di avvalersi di provider esterni. È dunque inibito l'accesso a Internet tramite *modem* e tal proposito, in base all'accordo, i numeri telefonici dei principali provider (es. Libero, Tiscali etc.) sono stati bloccati. Sono previsti **aggiornamenti periodici** della black-list.

- È assolutamente vietato collegarsi, con computer dell'A.O., alla rete Internet utilizzando chiavette USB e/o interfacce PCMCIA che sfruttano la connessione via cellulare (GSM, UMTS, GPRS).

In caso di mancato rispetto o violazione delle suddette regole o comunque nel caso di comportamenti non consentiti o non conformi al presente regolamento, l'amministratore di rete ovvero il responsabile del trattamento dei dati personali può sospendere temporaneamente l'accesso ai servizi informando gli organi di management.

Ogni unità operativa, congiuntamente all'ufficio Risorse Umane e all'ufficio Legale, deve sviluppare ed implementare una pratica disciplinare formale per i casi di non conformità alle policy e alle pratiche interne.

Restano salve le eventuali responsabilità civili, amministrative e penali di chiunque abbia commesso illeciti e la cui responsabilità sia stata accertata.

3.8 Protezione dei PC portatili

Ogni reparto dell'A.O. ha in dotazione un PC portatile che viene utilizzato dal personale medico preposto per l'archiviazione delle cartelle cliniche elettroniche dei pazienti e per l'erogazione di cure (farmaci monodose). I PC sono 5 (tanti appunto quanti sono i reparti) e sono abilitati per la connessione *wireless*. Per ovviare ai rischi di *wardriving* e di altre forme di intercettazione o navigazione o comunque utilizzo abusivi, la connessione è protetta dall'algoritmo di cifratura ***WEP*** (*Wired Equivalent Privacy*), ma si sta valutando l'ipotesi di utilizzare una crittografia più robusta, quale quella dello standard **WPA** (*Wi-Fi Protected Access*) o **WPA2**, di più recente rilascio (ove sia possbile). Al termine della sessione lavorativa, ogni PC viene collocato in un armadio del reparto munito di serratura. La chiave è a disponibilità del primario o, in sua assenza, del vice-primario o del medico di guardia. In alternativa viene consegnata al personale della portineria, che a tal proposito tiene un registro delle consegne delle chiavi, in cui vengono annotate generalità, orari di prelievo e di riconsegna del personale autorizzato a usare i PC**.**

4 CAPO III – Auditing

L'A.O. si riserva di attuare politiche di ***auditing*** **[6]**. L'auditing viene implementato attraverso diverse attività:

- test periodici relativi al funzionamento del sistema operativo e delle altre risorse software, hardware e di rete;
- test periodici di ripartenza, per valutare l'efficacia e la rapidità del ripristino degli accessi ai sistemi e ai dati;
- verifica delle procedure di backup (con particolare riferimento all'integrità, resistenza nel tempo e disponibilità dei dati salvati), di quelle di *"**disaster recovery**"*, anche attraverso simulazioni di incidente;
- verifica del funzionamento di eventuali sistemi *"R.A.I.D."* **[7]** o di altri sistemi di *mirroring* e di duplicazione da remoto in real time (server e CED ridondanti);
- controlli a campione sulle macchine;
- eventuale simulazione annuale di disastro;
- *compliance* o verifica del rispetto delle normative statali, comunitarie e internazionali in materia di privacy, tutela della riservatezza e della dignità dei lavoratori, *computer-crimes* e sicurezza informatica, *digital copyright* (tutela giuridica del software e delle banche-dati elettroniche e online), segreto industriale e scientifico, concorrenza.

[6] Viene considerato il terzo cardine della sicurezza logica dopo *autenticazione* e *autorizzazione*, secondo quello che a oggi è conosciuto come il sistema delle tre *"A"*: A/A/A.

[7] R.A.I.D. è l'acronimo di *"Reduntant Array of Indipendent Disks"*, un insieme di hard-disk che, connessi tra loro, appaiono come un unica memoria di massa.
In caso di malfunzionamento o di rottura dell'hard-disk principale costituisce un ottimo metodo di ripristino. Il sistema *"R.A.I.D. level one"*, che consente una duplicazione di dati in tempo reale su un altro disco (*"mirroring hard-disk"*). È necessaria dunque l'utilizzazione di due dischi, in modo che, in caso di guasto ad un'unità, il sistema è in grado di leggere i dati sull'unità gemella immediatamente ed automaticamente.

5 CAPO IV – Reportistica degli incidenti

5.1 Premessa

Tutti gli incidenti, confermati o sospetti, devono essere documentati, riportati in apposito registro e comunicati al security management.

Gli utenti devono riportare, ai loro responsabili locali, ogni sospetta violazione delle previste politiche sulla sicurezza dei dati.

5.2 Definizioni

A titolo esemplificativo, rientrano negli *"incidenti di sicurezza"*:

- la diffusione di *virus* o di altri codici maliziosi, come *trojan*, *spyware*, *worm*, *bot* etc.;
- gli accessi abusivi (fisici o logici) consumati o tentati;
- le intercettazioni telematiche abusive;
- tentativi o consumazioni di attività truffaldine volte alla captazione di password o altri codici d'accesso (*phishing*, furti d'identità, attività di *social engineering* etc.);
- il rilevamento di *backdoor* o punti d'ingresso occulti nei software (non solo nel sistema operativo); in genere tali *"porte"* vengono lasciate aperte dai programmatori per scopi leciti (aggiornamenti di sicurezza o del sistema operativo, manutenzione delle risorse software etc.), talora però possono essere sfruttate per finalità del tutto illecite (inserire software maligni come *rootkit* o *spyware* etc.);
- la modifica, la cancellazione o la soppressione non autorizzate di file;
- la falsificazione di file o di indirizzi IP da cui provengono messaggi o comunicazioni (*webspoofing*);
- la manipolazione o l'alterazione fraudolenta dei dati o del funzionamento dei sistemi o dei programmi o altri interventi non autorizzati sui medesimi (*pharming*, frodi telematiche…);
- violazione o rivelazione non autorizzata di corrispondenza telematica;
- la rivelazione all'esterno di notizie riservate, soprattutto se relative al segreto professionale o scientifico;
- il blocco dei sistemi o della rete (attacchi *DoS* o *DDos*, *mail-bombing*, *botnet* etc.);
- trattamenti illeciti o non conformi di dati personali.

Ovviamente sarà da ritenersi incidente di sicurezza ogni anomalia che faccia sospettare la presenza di una violazione della sicurezza esistente.

5.3 Report degli incidenti

Gli amministratori locali sono responsabili del monitoraggio sull'andamento dei sistemi e dei server di loro competenza. Questi devono:

- riportare qualsiasi perdita inaspettata o modifica verificatasi nei dati;
- individuare quali file e quali directory sono stati attaccati;
- valutare se il sistema attaccato costituisca il *target* (obbiettivo) dell'attacco o se invece era un semplice "ponte" per effettuare altri attacchi;
- identificare ogni comportamento sospetto, per es. richieste di accesso o di informazioni su password o su altri dati critici e confidenziali, avanzate da persone sconosciute, non identificate o non autorizzate;
- riportare tutti i tentativi di intrusione, non autorizzati, verso la rete o l'*host* nonché tutti gli altri attacchi ed eventi negativi, allo scopo di effettuare una prima stima dei danni e per valutare le criticità e il tempo impiegato per il ripristino.
- adottare le opportune procedure di *"Panic Room"* **[8]** in caso di incidenti di particolare gravità.

---

[8] Particolare misura di emergenza che blocca l'utilizzo della Rete, salvo che per porte particolari o particolari domini. In genere la panic room va attivata nel giro di una decina di minuti massimo oppure salvata come impostazione alternativa al firewall. Si può valutare la possibilità di istituire un *C.I.R.T.* (*"Computer incident response team"*), al fine di porre in essere le procedure di emergenza per il ripristino della normalità, per assicurare la continuità nel business, per ridurre e contenere le perdite e soprattutto per attivare per l'appunto la panic room.

Al fine di ottenere un report adeguato e completo degli incidenti è però necessario aver previamente posto in essere le ssgg. operazioni:

- precisa regolazione degli **orologi**.
- dettagliato disegno dell'**architettura di rete**, in modo da aver sempre presente la collocazione del sistema attaccato e la sua posizione rispetto a tutti gli altri, cosicché si possa valutare se possa verificarsi l' *"effetto domino"* o meno.
- stesura dell'**elenco dei sistemi operativi e degli applicativi**.
- redazione della **lista dei responsabili del settore IT**, **degli incaricati/operatori di sistema** e di chiunque abbia diritti di accesso e controllo rispetto alle macchine;
- **associazione univoca dell'ID degli incaricati/operatori si sistema all'IP della macchina**.

5.4 Scala gerarchica

Gli incidenti di sicurezza devono essere riportati, secondo le opportune modalità, via mail, seguendo la seguente scala gerarchica:

- Utente locale (livello <*user*>);
- Amministratore di sistema - Security Manager locale (livello <*admin*>);
- Responsabile dei sistemi informativi (<*root*>)
- Responsabile della sicurezza.

5.5 Informazione e collaborazione con autorità istituzionalmente riconosciute

Il responsabile della sicurezza, in caso di incidenti gravi, ha il compito di allertare le autorità competenti e di tenere i contatti con esse in merito alle eventuali azioni da intraprendere soprattutto allo scopo di preservare eventuali indizi o prove in relazione al verificarsi di un illecito (soprattutto se penale) per agevolare le attività di rilievo, accertamento, localizzazione e repressione dell'illecito stesso, nonché tutte le altre attività di *computer forensic* necessarie per l'acquisizione e la conservazione della prova digitale. Potrebbe all'uopo rivelarsi utile effettuare i ***backup*** dei file e delle directory attaccati.

6 CAPO V – Accordi di riservatezza ("Non Disclosure Agreements")

Tutto il personale dell'A.O. (dirigenti, dipendenti, collaboratori etc.), avente accesso alle informazioni critiche e quindi non pubbliche o non comuni o comunque non destinate alla divulgazione, deve sottoscrivere un **accordo di riservatezza** o di non diffusione (o documento equivalente) che per l'appunto vieta la comunicazione, rivelazione, diffusione o divulgazione delle suddette informazioni alle parti interne od esterne alla realtà di A.O., che non hanno effettivo motivo di conoscerle.

Allo stesso modo i contractors, i fornitori, i consulenti e tutte le terze parti, che abbiano rapporti con l'A.O. devono sottoscrivere, senza eccezioni, un accordo di riservatezza o di non diffusione, prima e allo scopo di ottenere accesso alle informazioni critiche e quindi non pubbliche o non comuni o comunque non destinate alla divulgazione.

Gli accordi di riservatezza o non diffusione saranno oggetto di revisione e/o aggiornamento nei casi in cui intervengano cambiamenti in termini di risorse umane, organizzative, strutturali e patrimoniali ovvero in termini di tipologia di attività effettuate e/o di dati trattati e comunque su base annuale.

Un programma di sicurezza e sensibilizzazione, incluse le politiche e pratiche di sicurezza dei dati, deve essere parte integrante degli orientamenti di tutte le nuove risorse.

Come contenuto minimo, gli accordi di riservatezza dovranno tener presenti le seguenti criticità:

- precisazione delle informazioni da considerarsi confidenziali;
- indicazione di limiti alla confidenzialità: notizie e informazioni suscettibili di comunicazione ed eventualmente di diffusione, in quanto già di pubblico dominio, ovvero provenienti da fonti esterne o già ricevute e acquisite, purché in maniera legittima;
- fissazione del periodo temporale durante il quale mantenere il riserbo (per es. facendo riferimento in via di interpretazione sistematica o analogica all'art. 2125 del codice civile);
- fissazione di penali per la violazione del riserbo, sulla base di quanto dispone per es. l'art. 1382 e ss. del codice civile.

7 CAPO VI - Formazione

Tutto il personale dell'A.O. deve ricevere una formazione sulla sicurezza ed un aggiornamento delle conoscenze **almeno una volta l'anno**. Ciò è necessario anche in relazione all'obbligo di formazione in materia di protezione dei dati personali ai sensi della regola 19.6 dell'Allegato B al Codice (parte integrante tra l'altro del contenuto del documento programmatico sulla sicurezza, cd. *"DPS"*), in virtù della quale gli incaricati del trattamento dovranno essere adeguatamente formati, informati e sensibilizzati sulle seguenti criticità:

- rischi incombenti sui dati e impatto sugli stessi;
- contromisure a fronte dei rischi valutati e considerati;
- aggiornamenti a carattere tecnico e normativo;
- responsabilità;
- aspetti più rilevanti della disciplina in materia di protezione dei dati personali, soprattutto in riferimento alla tutela dei dati sensibili e giudiziari.

Della partecipazione ai corsi di formazione ed ai relativi aggiornamenti sulla sicurezza deve essere redatta e regolarmente tenuta documentazione comprovante per tutto il personale di A.O., così come se ne dovrà dare atto nel DPS ai sensi della regola 19.6 dell'Allegato B al Codice.

8 CAPO VII – Norme transitorie e finali

1. Il presente regolamento, salve eventuali modifiche concordate col personale, entra in vigore a decorrere dal _____, per dar modo agli Amministratori di Sistema incaricati dell'A.O., ai responsabili e agli incaricati del trattamento dei dati personali di prenderne accurata visione.

2. Il presente regolamento sarà pubblicato nelle forme che la Direzione Aziendale dell'A.O. riterrà più opportune per consentirne la più ampia diffusione tra il personale interessato, ivi inclusi i canali ufficiali di comunicazione dell'A.O., tra i quali anche il sito istituzionale dell'ente.

3. Il presente regolamento sarà suscettibile, se necessario, di revisione e/o aggiornamento almeno una volta all'anno in corrispondenza dell'aggiornamento del DPS (regola 19 dell'Allegato B al Codice) ovvero qualora intervengano novità di tipo normativo sul piano della disciplina dei dati personali e delle norme tecniche emanande ai sensi dell'art. 71 del D.Lgs. 82/2005 e succ. modif.

Terni, li _____

per l'Azienda Ospedaliera "Santa Maria" di Terni

Il Refernte Aziendale per la Pivacy

(Dott.ssa Giuseppina Ferraro)

_____