SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Modena

Allegato 1 al Documento programmatico sulla sicurezza della Azienda USL di Modena_032017

# Norme per l'utilizzo degli strumenti informatici e di comunicazione aziendali e istruzioni di base per la tutela delle informazioni gestite dagli operatori

Il presente documento costituisce un disciplinare sull'utilizzo delle attrezzature informatiche e di telecomunicazioni aziendali, ai sensi di quanto previsto al punto 3.2 delle "Linee guida del Garante per posta elettronica e internet".

## Sommario



## Premessa

Il trattamento dei dati personali deve svolgersi "**nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato**, con particolare riferimento alla **riservatezza**, all'**identità personale** e al diritto alla **protezione** dei dati personali".

Da tale enunciazione del Codice Privacy (Art. 2, D. Lgs.196/2003) derivano una serie di obblighi in capo a chiunque utilizzi dati personali, non soltanto obblighi di riservatezza e segretezza, ma anche di tutela, protezione e sicurezza dei dati.

I principi contenuti nel Codice della Privacy[1] devono essere conosciuti e rispettati da chiunque tratti, nell'esercizio delle proprie funzioni, dati e informazioni personali e sensibili.
Questo documento è stato redatto tenendo conto delle indicazioni contenute provvedimento del Garante per la Protezione dei Dati Personali "Lavoro: le linee guida del Garante per posta elettronica e internet" in (G.U. n. 58 del 10 marzo 2007) e ha lo scopo di agevolare la lettura e l'interpretazione della normativa, dettando le necessarie prescrizioni e fornendo istruzioni operative.

Le istruzioni riportate si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro.

L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114, 171 e 184, co. 3, Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e comunque previa informativa ai dipendenti interessati.

Il documento opera nei confronti di ogni dipendente dell'Azienda e di tutti coloro che a vario titolo si trovino ad utilizzare il sistema informativo dell'Azienda. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore.

Il presente documento è reperibile sulla intranet aziendale all'indirizzo: **http://ts1/sio/**.
Sarà cura dell'operatore accertarsi se siano state pubblicate nuove versioni della presente linea guida e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività. Qualora l'operatore lo desideri potrà ottenere una copia a stampa del presente documento recandosi in un qualsiasi ufficio del Servizio ICT Aziendale.

È comunque indispensabile che chiunque tratti dati personali o sensibili prenda visione del vigente Documento Programmatico sulla Sicurezza (DPS); copia del DPS è reperibile presso gli uffici del Servizio ICT Aziendale o nella intranet aziendale, all'indirizzo sopra citato.

## Istruzioni

Le seguenti istruzioni sono parte del sistema di sicurezza che l'Azienda USL di Modena adotta al fine di gestire i dati trattati, nel rispetto della vigente normativa.
Si sintetizzano di seguito alcuni aspetti particolarmente rilevanti in materia.

## Accesso al sistema informatico aziendale e più in generale agli ausili tecnologici messi a disposizione dall'Azienda

- ➔ Tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale devono essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale e di un utente di posta elettronica, possono richiedere l'accesso ad Internet che sarà autorizzato o meno – in base alla mansione e a considerazioni organizzative – dal responsabile del trattamento di riferimento.
- ➔ La parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi.
- ➔ La parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato.

1 Il testo integrale del Codice Privacy è consultabile sulla intranet aziendale nella sezione speciale dedicata alla privacy (vedi in particolare il Titolo V "Trattamento di dati personali in ambito sanitario)

➔ A tutti gli utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima.

➔ Qualora si utilizzino sistemi che non siano in grado di richiedere automaticamente il cambio di password è indispensabile che l'utente – autonomamente - provveda a cambiarla ogni tre mesi.

➔ L'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

➔ L'Azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server, qualora ciò sia tecnicamente possibile. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali (personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati) la cui tutela è demandata a all'utente finale.

➔ L'effettuazione dei salvataggi con frequenza opportuna – almeno comunque settimanale - su supporti magnetici e la conservazione degli stessi in luogo idoneo - possibilmente sotto chiave e in contenitori ignifughi - è compito del singolo dipendente che usa la stazione ( nel caso di stazioni di lavoro usate da un solo utilizzatore) o da un incaricato opportunamente individuato dal responsabile del trattamento nel caso di stazioni di lavoro condivise.

➔ Nelle sedi aziendali dove è già presente un file server è fatto divieto di memorizzare in locale sulle stazioni di lavoro dati sensibili, che vanno salvati sui file servers. Nel caso in cui l'utente sotto la propria responsabilità memorizzi anche solo per brevi periodi dati in locale sulla stazione di lavoro, dovrà gestire i requisiti minimi di sicurezza della stessa.

➔ Tutti i pc devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi al Servizio ICT Aziendale.

➔ In caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password.

➔ Il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano il buon funzionamento delle infrastrutture aziendali e il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente.

➔ Gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc… - concessi in uso dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio. Nessun altro uso di tali strumenti è consentito se non espressamente autorizzato anche se nelle potenzialità della strumentazione concessa in uso ed eventualmente abilitata. A questo proposito è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici, o che questo, anche se tecnicamente possibile, può essere organizzativamente oneroso per l'Azienda; comunque la disponibilità di una determinata funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali.

➔ Nessun dispositivo personale potrà essere collegato alla rete dell'Azienda e/o utilizzato per trattare dati istituzionali aziendali. Qualora l'Azienda, per l'espletamento della propria attività istituzionale si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile, dovrà essere formalmente definito un

Responsabile esterno che si faccia garante degli aspetti di sicurezza e di rispondenza alla normativa vigente in tema di trattamento dei dati personali per tutti i trattamenti che avvengono su tali attrezzature.

➔ L'Azienda si riserva di verificare l'utilizzo degli strumenti aziendali concessi in uso – ad esempio il telefono, le stazioni di lavoro informatizzate, i palmari, ecc… - qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni.

➔ L'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale delle aziende che in nome e per conto dell'Azienda effettuano attività di manutenzione sugli strumenti aziendali - attrezzature di produttività personale, sistemi di comunicazione, ecc… - potranno accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto come impedimento all'accesso il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale.

## Modalità da seguire per l'accesso ai dati in caso di prolungata assenza dell'incaricato (D. Lgs. 196/2003, Allegato B, punto 10)

E' necessario distinguere due diversi casi:

**a)** I dati sono accessibili da più di un operatore,

**b)** I dati sono accessibili da parte di un unico operatore.

Per semplicità si farà riferimento al solo caso b) in quanto, nel caso in cui i dati siano accessibili da parte di più operatori (caso a) sarà necessario adottare le misure di seguito descritte solo se tutti gli operatori che hanno accesso ad un medesimo dato non sono presenti per un lungo periodo di tempo.

➔ Nel caso in cui l'operatore che ha normalmente accesso al dato non possa per lungo periodo garantire ciò, sarà cura del responsabile del trattamento vicariare tale mancanza.

➔ Nel caso in cui il responsabile del trattamento sia in grado di utilizzare le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, basterà che il responsabile del trattamento richieda al Servizio ICT Aziendale le abilitazioni necessarie ad accedere al dato. Una volta ricevute le abilitazioni opportune potrà accedere ai dati al posto dell'operatore assente; il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile.

➔ Nel caso in cui il responsabile del trattamento non sia in grado di utilizzare direttamente le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, farà richiesta al tecnico del Servizio ICT Aziendale che normalmente si occupa degli aspetti tecnici dell'applicativo, di accedere ai dati necessari in qualità di incaricato temporaneo.

➔ La misura precedente dovrà essere utilizzata solo nel caso l'urgenza lo richieda e nella misura strettamente necessaria a risolvere la situazione contingente. Se l'esigenza va oltre la singola necessità e qualora i tempi lo consentano il Responsabile del trattamento disporrà di abilitare un diverso incaricato, in aggiunta a quello assente, all'accesso dei dati. Il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile.

➔ Sarebbe opportuno che la individuazione di un diverso incaricato da abilitare all'accesso ai dati avvenisse da parte del responsabile all'interno di una rosa di fiduciari allo scopo previsti dall'incaricato; una tale gestione, se attuata, è in carico ai responsabili del trattamento.

➔ Le diverse richieste attinenti alla casistica descritta dovranno essere documentate da richieste scritte, eventualmente anche formulate via mail.

## Utilizzo dei supporti di memorizzazione

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22:

1. è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
2. nel caso non sia possibile garantire il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto.

In generale i supporti di memorizzazione, anche non removibili, che contengono dati personali o sensibili, nel caso in cui non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dismessi (per es. per obsolescenza o per guasto) dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

## Buon uso della rete di comunicazione e delle attrezzature aziendali di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Servizio ICT Aziendale. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- ➔ divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password) se non espressamente autorizzate dal Servizio ICT Aziendale;
- ➔ divieto di alterare la configurazione di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…);
- ➔ è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia.

È vietata l'installazione non autorizzata di modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda.
È vietata l'installazione non autorizzata di apparati di rete di qualsiasi tipo – hub, switch, router, access point WI-FI, access server, ecc… -.
È vietata l'installazione di qualsiasi attrezzatura informatica o di comunicazione non espressamente autorizzata dal Servizio ICT Aziendale.
È vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il *by pass* delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati.

L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o danneggiamento degli stessi sarà sanzionata.
I responsabili delle varie macro articolazioni organizzative, di concerto con i responsabili del trattamento e con il Servizio ICT, sono responsabili della adozione degli atti e delle misure organizzative necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'Azienda.

## Virus

Si invitano gli utenti:

- ➔ alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione removibile sia stato utilizzato su un computer diverso dal proprio (supponendo che il proprio PC sia immune da infezioni) occorrerà

verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione, in quanto potenzialmente infetto;

- ➔ in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
  - ➔ è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure. Nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato, avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'ufficio reti del Servizio ICT Aziendale (reti@ausl.mo.it ) e non inviare indiscriminati messaggi a tutti i propri conoscenti: questo evita l'ingenerarsi di falsi allarmi e di inutili catene di Sant'Antonio.

## Internet

E' vietato l'utilizzo personale e non istituzionale della connessione a internet aziendale.
Tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log; tali log tengono traccia dei seguenti dati per ogni accesso:

- ➔ identificativo dell'utente che ha navigato in internet;
- ➔ identificazione della stazione di lavoro;
- ➔ data e ora
- ➔ riferimento al sito visitato (URL)

Tali log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema, entrambi su base anonima. I log saranno trattati in maniera tale da fornire informazioni in maniera aggregata in modo da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo.

l'Azienda si riserva di filtrare l'accesso a siti che risultino non in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento del sito in una cosiddetta "Black list" ovvero nell'inserimento del sito in una categorizzazione, eventualmente predisposta anche da fornitori esterni specializzati; la lista dei siti inaccessibili o delle categorie potrà essere chiesta alla direzione del Servizio ICT Aziendale da chiunque e, in caso di motivate ragioni, potrà essere autorizzata la navigazione sul sito mediante rimozione dalla lista di esclusione; l'esclusione dei siti verrà operata periodicamente in base all'analisi di dati aggregati. A tal proposito, nel corso del 2015 è stata effettuata una modifica delle impostazioni del server proxy, al fine di limitare il numero dei siti a cui gli operatori possono accedere liberamente e prevenire così casi di navigazione indebita: rimane salva la possibilità di richiedere alla direzione del Servizio ICT Aziendale, di accedere ad uno o più siti bloccati, motivandone la necessità.

A titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:

- ➔ servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- ➔ scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste al Servizio ICT Aziendale che provvederà a eseguire fisicamente lo scarico da stazione protetta, applicare le misure antivirus relative e consegnare il software al richiedente;

➔ utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem) da quello centralizzato;

➔ usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;

➔ produrre e pubblicare propri siti web sulla infrastruttura tecnologica dell'Azienda; ogni eventuale necessità di realizzare siti web personali o di struttura dovrà essere espressamente autorizzata dal Responsabile del trattamento dei dati.

## Posta elettronica

E' vietato l'utilizzo personale e non istituzionale della posta elettronica aziendale.
**E' vietato l'utilizzo della posta elettronica per l'invio di dati sensibili**. In particolare è vietato un uso di tale strumento dal quale possa derivare la possibilità, anche indiretta o preterintenzionale, di rilevare le opinioni politiche, religiose o sindacali dell'operatore, le sue inclinazioni sessuali, il suo stato di salute.
Il sistema di posta elettronica tiene traccia, per tutte le e-mail inviate e ricevute, di:

- data e ora;
- identificativo della stazione di lavoro che ha inviato il messaggio;
- indirizzo di posta del mittente;
- indirizzo del destinatario.

Anche in questo caso i log vengono mantenuti per lo stesso periodo e le stesse finalità indicate per gli accessi Internet.

Tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con virus, effettua i seguenti controlli:

- blocco delle e-mail con allegati potenzialmente pericolosi (file con estensioni EXE, .COM, VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)
- blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 7 Mb
- blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari
- in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il Servizio ICT Aziendale si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducili alla violazione di sicurezza o a codice pericoloso.

Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare:

- il passaggio di SPAM qualora non sufficientemente selettive;
- il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.

Per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.

Dal mese di APRILE 2015 è stata inoltre attivata una nuova funzione sul sistema di posta elettronica aziendale che permette la gestione personalizzata delle mail che il sistema di AntiSPAM aziendale ha individuato come potenziali SPAM.

**Il sistema di posta elettronica in uso, e concesso in utilizzo, non è un sistema di posta certificata, non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di riservatezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio.**
L'Azienda favorisce la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "maling list", cioè di gruppi di indirizzi.
L'Azienda non fornirà indirizzi di posta elettronica aziendali per usi di tipo personale, ma non vieta la consultazione del contenuto di indirizzi di tipo personale, anche dall'interno dell'Azienda, qualora la modalità di consultazione di tali informazioni sia compatibile con i vincoli di sicurezza del sistema aziendale e ciò avvenga in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda.
L'Azienda mette a disposizione funzionalità di avviso in caso di assenza prolungata dell'operatore, che sfruttano le peculiarità del sistema di posta elettronica e possono fornire coordinate di altri riferimenti all'interno dell'Azienda tali da garantire il corretto funzionamento dei servizi. L'attivazione di tali misure sarà a cura dell'operatore che dovrà avvisare le locali sedi del Servizio ICT Aziendale di attuare la misura o attuarla in autonomia se tecnicamente non in grado; qualora l'operatore non abbia adottato tale misura e l'assenza si protragga per più di una settimana, il responsabile del trattamento potrà richiedere al Servizio ICT Aziendale l'adozione di tale misura.
Ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, dirottare la propria posta elettronica su un diverso indirizzo di posta elettronica personale o di un fiduciario; nel caso non sia in grado di attuare detta misura in autonomia, potrà chiedere alla locale sede del Servizio ICT Aziendale la messa in atto della misura; della attuazione di tale misura verrà tenuta traccia e verrà data notizia al lavoratore interessato alla prima occasione utile.
Qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario.
Fatte salve le limitazioni di cui ai punti precedenti l'Azienda favorisce l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra pubbliche amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore. Fatte salve le limitazioni precedentemente esposte, alla trasmissione telematica di atti e documenti all'interno dell'Azienda per posta elettronica è riconosciuta la stessa validità della trasmissione per via cartacea; in particolare potranno essere trasmessi atti deliberativi, disposizioni dirigenziali e documenti in genere che non contengano dati sensibili e il cui mancato recapito non ingeneri danni per l'azienda, per i dipendenti o per altri. L'utilizzo della posta elettronica, in questi casi, potrà sostituire completamente l'invio di carta. Atti o documenti aventi valenza generale possono essere comunicati a tutti o a grande parte dei dipendenti dell'Azienda; ciò può avvenire tramite l'utilizzo di apposite liste di distribuzione che sono messe a disposizione in posta elettronica; esigenze particolari od occasionali di comunicazione ad un numero di utenti il cui volume o la cui qualità non sia già stata prevista dovranno essere inoltrate dal Servizio ICT Aziendale.

A titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:

- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni non istituzionali o azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, giochi, scherzi, barzellette e altre e-mail avulse dal contesto lavorativo;
- usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete.

## Data breach

Dal mese di agosto 2015, in ottemperanza ad un obbligo sancito dal Garante Privacy è stata introdotta e diffusa tra tutti i dipendenti una procedura per la comunicazione obbligatoria e tempestiva al Garante (entro le 48 ore dalla conoscenza del fatto) di eventuali violazioni dei dati o incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle banche dati dell'Azienda – c.d. data breach[2].
Pertanto chiunque in Azienda sospetti sia avvenuto un data breach deve immediatamente comunicarlo al Servizio ICT, utilizzando l'indirizzo email: ict_privacy@ausl.mo.it.

## Utilizzo dei sistemi di comunicazione in fonia: telefoni fissi, telefoni mobili, ecc…

E' vietato l'utilizzo personale e non istituzionale del telefono.
L'azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri: ad esempio numeri a pagamento per servizi particolari che si giudicano non interessanti dal punto di vista istituzionale, ecc….
Ogni operatore che abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione.

Per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate, qualora queste inducano un onere economico per l'Azienda; non sono ad esempio tracciate le telefonate in ingresso che sono tipicamente non onerose in termini economici. Viene registrato:

- ➔ il numero del chiamante;
- ➔ il numero chiamato;
- ➔ la data e ora di inizio della telefonata e la data e ora di fine della stessa

Tutti i log sopra citati vengono conservati dall'Azienda un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti. I dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi. I controlli verranno effettuati in maniera non nominativa e aggregata – ad esempio aggregando i dati per edificio o per unità erogante; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi. Normalmente sarà necessario adottare una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati. Qualora l'integrità del sistema tecnologico dell'azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione.
In generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative.

## Tutela del diritto d'autore

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore:

---

2 Fra gli eventi che possono essere ascritti ad un data breach, pur essendo l'elenco non esaustivo, vi sono:l'accesso abusivo a dati personali, sensibili o giudiziari contenuti nelle banche dati aziendali; la copia abusiva per immagine su supporto informatico di documenti analogici contenenti dati personali, sensibili o giudiziari; la perdita o il furto di attrezzature aziendali – PC portatili, PC fissi, dispositivi di memorizzazione, ecc… che contengano dati personali, sensibili o giudiziari; attacchi condotti da persone o software – malware - che ottengano l'accesso alle banche dati aziendali o più in generale eventi che possano portare ad accessi indebiti o alla cattura di dati di accesso e di identificazione - user name e password.

- E' vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi;
- è fatto divieto ad ogni utilizzatore del sistema informativo aziendale scaricare, gestire in qualsiasi modo e trattare dati o informazioni che violino la normativa sulla tutela del diritto d'autore;
- qualora l'operatore nonostante tale divieto infranga tale normativa sarà penalmente e civilmente responsabile del proprio operato sollevando l'azienda da ogni responsabilità.

## Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

### Documentazione cartacea

- L'operatore, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi.
- L'operatore deve controllare che i documenti siano sempre completi ed integri.
- In caso di abbandono, anche temporaneo, dell'ufficio, l'operatore non deve mai lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto); è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.); ove si utilizzi un contenitore/locale chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di operatori autorizzati.
- Occorre in particolare accertarsi che nessun visitatore o terzo estraneo possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti.
- Al momento della consegna di documenti contenenti dati personali o sensibili ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate.
- La distruzione dei documenti contenenti dati personali o sensibili deve avvenire con modalità che rendano impossibile l'individuazione dell'interessato da parte di terzi non autorizzati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi).

### Comunicazioni telefoniche e via fax

- Nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chi risponda all'apparecchio. In caso di risposta negativa l'operatore deve chiedere in alternativa un numero riservato.
- Occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati.
- In caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza; qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata.
- L'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.

### Utilizzo della fotocopiatrice e della stampante

- In caso di stampa o duplicazione non riuscite di documentazione contenente dati personali/sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati.
- Qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili.

➔ Occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso.

**Utilizzo dei supporti di memorizzazione**

E' vietato l'utilizzo di supporti rimovibili, come ad esempio chiavetta usb o cd rom, per lo scambio di dati sensibili; qualora vi fosse assoluta necessità di utilizzarli è indispensabile assicurarsi che essi non vengano riutilizzati e siano distrutti dopo il loro utilizzo; qualora, viceversa, vengano riutilizzati occorre verificare che il precedente contenuto sia stato reso assolutamente irrecuperabile, con procedure di cancellazione sicure da concordare con il Servizio ICT, in quanto le normali procedure di cancellazione di un dato informatico non sono normalmente sufficienti a garantire ciò, potendosi in molti casi recuperare anche dati cancellati con procedure e strumenti particolari.

**Rapporti di front office**

➔ **Rispetto della distanza di cortesia**: l'operatore di sportello deve prestare attenzione al rispetto dello spazio di cortesia e, se del caso, invitare gli utenti a sostare dietro le apposite linee/barriere delimitanti lo spazio di riservatezza.

➔ **Controllo dell'identità del richiedente**: nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente (ad esempio formulando una serie di quesiti al fine di un accertamento sommario) e la sua legittimazione a ricevere le informazioni su quanto richiesto.

➔ **Identificazione dell'interessato e controllo dell'esattezza dei dati**: nel momento della raccolta di dati anagrafici (in particolar modo nel caso di cittadini stranieri) occorre fare attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato.

➔ **E' vietata la chiamata nominativa dell'utente**: nelle sale e negli spazi di attesa i nomi dei pazienti non devono essere divulgati ad alta voce; occorre utilizzare un sistema che prescinda dai dati anagrafici (es. codice alfanumerico, orario della prenotazione, ecc.). Eventuali deroghe ed eccezioni devono essere discusse con l'Ufficio Privacy.

**Corretta comunicazione dei dati**

➔ La richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge (in casi dubbi rivolgere sempre richiesta di chiarimenti al responsabile del trattamento). In tal senso assoluta attenzione deve essere in particolare prestata nelle operazioni di consegna di referti diagnostici, cartelle cliniche, risultati di analisi e certificati.

➔ Devono comunque essere rispettate le modalità del controllo dell'identità del richiedente (vd. paragrafo "rapporti di front office").

➔ La comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato (art. 84 D.Lgs. 196/03).

➔ L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi nonché essere contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

**Rispetto della privacy in corsia**

➔ Devono essere adottate soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza, da parte di terzi, di informazioni idonee a rivelare lo stato di salute (ad es. utilizzo, laddove possibile, di spazi riservati).

➔ Devono altresì essere adottate soluzioni tali da garantire il rispetto della dignità dell'interessato, in occasione di prestazione mediche particolarmente delicate (ad es. utilizzo di paraventi).

- ➔ L'interessato ricoverato, se cosciente e capace, deve essere preventivamente informato e poter decidere a chi possa essere data comunicazione della propria presenza in ospedale. Qualora l'interessato non possa essere interpellato in proposito, potranno essere fornite informazioni, anche telefoniche, sul passaggio o sulla presenza dello stesso al Pronto Soccorso o in altri reparti solo ai terzi legittimati come familiari e congiunti, previo accertamento sommario dell'identità del richiedente (es. mamma che contatti il Pronto Soccorso per avere notizie circa l'eventuale presenza del figlio nella struttura).
- ➔ Occorre porre in essere procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparto o strutture indicativa dell'esistenza di un particolare stato di salute (sono vietate ad es. le carrozzine che riportano per esteso il nome dell'unità operativa di appartenenza).
- ➔ E' vietata, in locali aperti al pubblico o di passaggio, l'affissione di liste di pazienti in attesa di intervento; in tali luoghi è vietata altresì l'affissione della turnistica degli operatori riportante la causa di assenza (es. malattia).
- ➔ Non devono essere visibili ad estranei documenti sulle condizioni cliniche del malato (es. cartelle cliniche/infermieristiche poste vicino al letto di degenza). Qualora fosse necessario mantenere la grafica ai piedi del letto, essa dovrà essere girata o comunque posizionata in modo tale da non poter essere immediatamente visibile da terzi estranei.

## Servizio deputato ai controlli

L'Azienda delega al Servizio ICT i controlli tecnici sui sistemi informatici previsti dalla presente linea guida e alle macro articolazioni gestionali la responsabilità complessiva del controllo del personale afferente alle unità organizzative di competenza.

## Facoltà dell'Azienda

Qualora l'Azienda:

- abbia ad accertare manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso;
- riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema informatico, telematico, telefonico aziendale o il suo buon funzionamento e/o a garantire ad altri accessi o altri privilegi non dovuti;
- abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata

si riserva il diritto di:

- effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali;
- disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature aziendali;
- segnalare al responsabile organizzativo situazioni e comportamenti anomali degli operatori.

In caso di problemi inerenti la sicurezza della infrastruttura tecnologica l'Azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware, ecc… Tutte le azioni messe in atto dovranno essere valutate in una logica di costo/beneficio e dovranno essere improntate ad un criterio di minimizzazione del disservizio.

L'Azienda si riserva la facoltà di sospendere l'accesso ai servizi qualora, anche a seguito di segnalazioni rappresentate dal Responsabile Organizzativo, sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

L’Azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.