Il Sistema Informativo Sanitario Provinciale di Reggio Emilia

Regolamento all'uso dei sistemi ICT

Adottato con deliberazione del Direttore Generale n. 202 del 24/05/2018

Sommario

1 Acronimi e Definizioni

Backup dei Dati: operazione di copia dei dati e archiviazione della copia a scopo di tutela della integrità e della disponibilità del dato

Credenziali: insieme di nome utente e password, costituiscono la propria identità digitale all'interno dei sistemi informativi aziendali; sono personali e non cedibili

Dato Originale: dato in copia unica, la cui perdita ne compromette la disponibilità in modo irreversibile.

HW: Hardware: l'insieme dei dispositivi fisici utilizzati per il trattamento informatico dei dati

PC, Client: computer (elaboratore) ad uso personale, normalmente collegato alla rete aziendale

Profilazione degli accessi: sistema autorizzativo per cui l'accesso a specifiche risorse informatiche (sistemi, spazi di rete, specifiche funzioni) sono limitate ad un insieme di utenti, sulla base di regole definite dall'organizzazione

Server: computer (elaboratore) collocato in locali dedicati (sale server), dedicato ad ospitare servizi software e archivi dati, resi disponibili ai client tramite rete aziendale

Share: spazio di archiviazione documentazione generica (files, documenti) reso disponibile sulla rete aziendale; normalmente visualizzato sui PC come dischi virtuali di rete (virtuali in quanto non corrispondono ad alcun dispositivi fisico collegato al PC)

SIO: Sistema Informativo Ospedaliero: insieme dei sistemi HW, SW e organizzativi che concorrono alla gestione dei dati e delle informazioni all'interno della struttura sanitaria ospedaliera

Sistema Informativo: insieme dei sistemi HW, SW e organizzativi che concorrono alla gestione dei dati

STIT: Servizio Tecnologie Informatiche e Telematiche (quello che una volta era il "CED")

SW: Software: l'insieme dei programmi che, sfruttando i dispositivi HW e le connessioni di rete, consentono l'inserimento, l'archiviazione, l'elaborazione e la consultazione dei dati (anche detti applicazioni, procedure, programmi)

2 Introduzione

Questo regolamento è rivolto al professionista che a qualsiasi titolo faccia accesso ai sistemi informatici in uso presso la AUSL-IRCCS di Reggio Emilia (di seguito "azienda").

Lo scopo del documento è quello di fornire le indicazioni operative e informazioni di base necessarie a garantire un accesso efficace e sicuro alle risorse informatiche aziendali.

Il presente documento costituisce regolamento all'uso dei sistemi informatici, ed il rispetto delle prescrizioni in esso contenute sono obbligo di ciascun dipendente, collaboratore o frequentatore che faccia accesso ai sistemi informativi.

Sono fatte salve le disposizioni relative a controlli e verifiche di sicurezza di cui al regolamento Ausl adottato con deliberazione n. 189/2009.

Il sistema informativo sanitario dell'azienda è composto da un insieme di sistemi hardware (dispositivi fisici), software (programmi, applicazioni, procedure) e organizzativi a supporto delle attività dell'azienda.

Tutti i componenti di tale sistema, più o meno direttamente collegati all'attività sanitaria, contribuiscono in modo unitario alla conduzione delle attività aziendali.

Ogni dipendente, collaboratore o frequentatore dell'azienda che ha accesso a parte di tali sistemi, sulla base del proprio profilo di autorizzazione, si assume la responsabilità di tutelare tali sistemi da usi impropri in quanto beni aziendali, e in quanto strumenti destinati alla continuità di missione della nostra azienda.

L'uso improprio di tali strumenti può causare danno all'azienda in termini economici (es. distruzione di beni, esigenza di intervenire con risorse umane per porre rimedio ad azioni non corrette), sia in termini di impossibilità di perseguire in modo ottimale gli obiettivi aziendali (es. compromissione del funzionamento di un sistema di uso clinico), o comunque di condurre le attività di supporto fondamentali per il perseguimento degli obiettivi aziendali (es. compromissione del funzionamento di sistemi amministrativi).

L'uso improprio degli strumenti può inoltre cagionare danno ai diritti e libertà fondamentali dell'individuo, in termini di riservatezza, integrità e pronta disponibilità del dato, e in termini di potenziale danno alla salute.

Le modalità di verifica e l'eventuale iter disciplinare conseguente alla individuazione di comportamenti non in linea con il presente regolamento sono oggetto di specifica delibera aziendale.

3 Struttura Generale del Sistema Informativo Sanitario

Il sistema informativo sanitario della nostra azienda è composto da **dispositivi fisici**, da **connessioni di rete**, e da **applicativi** (software, programmi, procedure) che sfruttano tali dispositivi fisici e connessioni di rete.

L'operatore a cui è concesso l'utilizzo di tali risorse per lo svolgimento della propria attività lavorativa è tenuto ad un uso corretto delle stesse.

Il sistema informativo comprende un insieme di dispositivi fisici di varia natura (es. PC, stampanti, lettori portatili, ecc.) messi a disposizione degli operatori (dipendenti, collaboratori, frequentatori ecc.) allo scopo di consultare e contribuire alla creazione del patrimonio informativo aziendale.

Uso corretto dei dispositivi fisici

È obbligo degli operatori un uso corretto di tali dispositivi fisici in quanto beni aziendali. Per "uso corretto" dei dispositivi fisici, analogamente a qualsiasi altro bene aziendale, si intende l'obbligo di un utilizzo limitato alle attività aziendali, la non sottrazione, la non distruzione e la pronta segnalazione di qualsiasi guasto o malfunzionamento.

La maggior parte dei dispositivi informatici messi a disposizione sono connessi ai sistemi di rete dati aziendale. Tale rete ha lo scopo di far accedere i nostri operatori in modo unitario al patrimonio informativo aziendale. Tale rete ha inoltre lo scopo di consentire una comunicazione verso l'esterno della nostra organizzazione, in particolare verso altre organizzazioni del sistema sanitario regionale, e verso Internet secondo protocolli di comunicazione e modalità sicure.

Uso corretto delle connessioni di rete

È obbligo degli operatori un uso corretto di tale connessione in rete. Per "uso corretto" delle connessioni di rete si intende un uso limitato alle esigenze aziendali, e rispettoso dei principi di cautela nella trasmissione di dati personali dettati dalla normativa vigente.

Ad ogni operatore, in base alle esigenze conseguenti al proprio ruolo professionale e al contesto, saranno concessi diritti di accesso a specifici applicativi aziendali.

Uso corretto degli applicativi aziendali

È obbligo degli operatori un uso corretto di tali applicativi aziendali. Per "uso corretto" si intende un uso consapevole del rischio conseguente a trattamenti dei dati impropri (es. inserimento di dati non corretti, mancato inserimento di dati, accesso a dati non pertinenti). È inoltre obbligo di ogni operatore segnalare prontamente qualsiasi malfunzionamento di tali sistemi.

Ricordiamo inoltre che ogni operatore aziendale è nominato Incaricato/Autorizzato al Trattamento Dati, e in quanto tale si assume specifici obblighi relativi alle modalità e finalità di gestione dei dati, sia con strumenti informatici, che con modalità più tradizionali (carta, verbale, ecc.).

3.1 Dispositivi Fisici

Il sistema informativo provinciale è composto da dispositivi fisici distribuiti fisicamente su tutte le strutture dell'organizzazione. Tali dispositivi fisici (PC fissi, PC portatili, stampanti, ecc.) anche se destinanti ad un uso individuale (è prevista la sessione individuale di lavoro, con autenticazione del singolo operatore), non sono assegnati alla singola persona, e possono, al bisogno, essere utilizzati da qualsiasi operatore dell'azienda (condivisione della strumentazione informatica).

A scopo di tracciabilità delle responsabilità in caso di furto, smarrimento o guasto volontario ad ogni bene è associata una struttura di competenza e, in alcuni casi, un utente di riferimento. Tali strutture ed utenti sono responsabili di garantire la non sottrazione o spostamento dei dispositivi fisici.

Allo scopo di gestire il parco dispositivi aziendale, ogni dispositivo fisico ha associata in inventario una collocazione fisica preferenziale. Qualsiasi spostamento permanente del dispositivo (es. trasloco, assegnazione ad altro reparto, assegnazione ad altro professionista) deve essere concordata con lo STIT allo scopo di tracciabilità.

In caso di furto o smarrimento di dispositivi fisici, in particolare quelli che possono contenere dati sensibili, è obbligatoria una pronta segnalazione ai canali di assistenza allo scopo sia di ripristinare il dispositivo, sia di far partire eventuali iter formali di denuncia (in particolare nei confronti dell'Autorità Garante in caso di distruzione o perdita di dati personali o sensibili).

La gestione ordinaria dei dispositivi fisici è in carico allo STIT aziendale (e altri servizi coinvolti nella gestione dei beni informatici). È però demandata alla struttura che ospita i beni la gestione dei consumabili eventualmente presenti (es. toner delle stampanti, carta, braccialetti identificativi, etichette ecc.).

Non è consentito l'utilizzo di dispositivi fisici informatici personali o comunque non di proprietà aziendale (o concessi in uso aziendale tramite atto ufficiale). Tali sistemi non possono peraltro essere collegati alla rete aziendale, e conseguentemente qualsiasi dato in essi inserito sarebbe posto all'esterno del perimetro di sicurezza aziendale, mettendolo a rischio di perdita, alterazione o accesso improprio (circostanze che, per i dati relativi alla salute, costituiscono violazione della normativa vigente).

3.2 La Rete dati aziendale

La rete aziendale, composta di cablaggi in fibra ottica di dorsale provinciale, ponti radio, cablaggi fisici nei locali e punti di accesso wifi, raggiunge oggi in modo capillare quasi ogni luogo fisico delle strutture aziendali, in particolare quelli caratterizzati da servizi sanitari.

Data la natura fortemente distribuita delle nostre strutture, le performance della rete (velocità) potrebbero differire in punti geografici diversi sulla base del tipo di collegamento disponibile. Le performance della rete sono oggetto di continuo monitoraggio, in particolare nelle aree oggetto di attività sanitaria.

I collegamenti di lunga distanza (es. ospedali periferici con le strutture centrali) sono affidati in parte a aziende terze, pertanto i tempi di risposta e l'operatività dello STIT in caso di guasto potrebbe essere vincolati a quelli degli attori terzi coinvolti.

La connessione alla rete aziendale consente un monitoraggio continuo dei sistemi di sicurezza del dato disponibili sulle postazioni di lavoro.

La rete consente di fruire di un insieme di servizi, in particolare:

- **Verifiche delle credenziali**: la rete è necessaria per consentire l'accesso agli operatori ai dispositivi aziendali; in assenza di connettività di rete non è normalmente consentito l'accesso ai dispositivi in quanto non è possibile verificare l'autenticità delle credenziali inserite.
- **Accesso ai Dischi di Rete**: la rete rende raggiungibili gli spazi di archiviazione ospitati sui server centrali; in caso di indisponibilità di rete i dischi personali, di reparto, ed altri potrebbero risultare non raggiungibili.
- **Accesso alle Stampanti di Rete**: la rete veicola le stampe provenienti da più sorgenti (es. diversi PC) verso stampanti centralizzate; in caso di indisponibilità di rete alcune stampanti, anche se fisicamente collocate in prossimità potrebbero non risultare raggiungibili.
- **Posta Elettronica (e-mail)**: la rete consente, da qualunque postazione aziendale abilitata, di accedere alla propria casella postale (tramite software Outlook o tramite posta web); in assenza di rete la posta elettronica potrebbe risultare comunque accessibile, ma non aggiornata e senza la possibilità di inviare nuove mail, oppure risultare del tutto non accessibile (es. nel caso di posta web).
- **Accesso agli applicativi aziendali**: la rete consente a ciascun dispositivo personale (PC fisso, PC portatile, dispositivo mobile) di accedere tramite appositi applicativi (es. cartelle cliniche informatizzate, sistemi di gestione di dispositivi medici) all'archivio dati memorizzato su server aziendali remoti; in casi di indisponibilità di rete questi applicativi potrebbero non funzionare correttamente, in quanto privi di possibilità di leggere e scrivere sul loro archivio dati.
- **Accesso alle risorse web interne**: la rete consente di accedere a siti web interni all'azienda (quindi non fruibili direttamente dall'esterno) utilizzati a vari scopi, sia per operatività clinica (alcuni applicativi sanitari sono realizzati come siti web interni) sia per una gestione generale dell'organizzazione (es. bollettini e notiziari disponibili sulla intranet, sistemi di gestione della documentazione qualità, sistemi di gestione delle sale riunioni, ecc.).
- **Accesso a internet**: la rete veicola l'accesso a internet per le postazioni di lavoro aziendali, limitatamente alle funzioni necessarie (navigazione generale, accesso a specifici servizi su internet, ecc.).

3.2.1 Connessione di dispositivi personali

Per motivi di sicurezza, la rete aziendale non consente al momento la connessione di dispositivi personali. Pertanto i dispositivi personali non possono essere utilizzati in ambito lavorativo. Qualsiasi utilizzo di dispositivi personali per l'inserimento, archiviazione, elaborazione o trasmissione di dati aziendali (in particolare dati sensibili) è vietato, e costituisce oltre alla violazione del presente regolamento, una violazione della normativa vigente sulla protezione dei dati personali, in quanto pone tali dati in una condizione di sicurezza non garantita dal titolare del trattamento (l'Azienda USL).

Allo scopo di consentire un utilizzo dei dispositivi personali (non a scopo lavorativo, e al di fuori dell'orario lavorativo) all'interno delle strutture, dove possibile, è resa disponibile la rete wifi denominata

"EmiliaRomagnaWiFi", ad accesso libero. Tale servizio è fornito in collaborazione con Lepida S.p.a.. Eventuali malfunzionamenti di tale rete wifi possono essere segnalati ai servizi di assistenza aziendale, ma saranno gestiti con priorità inferiore rispetto alla gestione della rete aziendale.

3.2.2 Portali Intranet

Allo scopo di consentire una efficace comunicazione tra le varie parti della organizzazione, sulla rete aziendale è reso disponibile un Portale Intranet Aziendale (sito web interno).

https://portal.ausl.re.it

Parte di questo portale è reso disponibile all'esterno dell'organizzazione.

Il portale Intranet Aziendale, seppure consenta di archiviare dati, non è deputato alla archiviazione o trasmissione di dati relativi alla salute, in quanto non garantisce i necessari livelli di confidenzialità, integrità e continuità.

Allo scopo di supportare l'operatività sanitaria è invece disponibile il Portale Clinico Aziendale (sito web interno)

https://portaleclinico.asmn.re.it

Il portale clinico è raggiungibile esclusivamente da postazioni interne all'organizzazione.

3.2.3 Le connessioni verso l'esterno (navigazione Internet)

La rete aziendale consente l'accesso alla rete Internet dalla maggior parte delle postazioni di lavoro interne alla azienda (potrebbero essere escluse postazioni che, per particolari requisiti di sicurezza e criticità, sono mantenute isolate).

L'accesso alla rete Internet è consentito nell'ambito dello svolgimento delle proprie attività professionali. Non è consentito l'uso a scopo personale. Per tale motivo l'azienda limita l'accesso alle risorse internet sulla base di sistemi di filtro automatico della navigazione verso dei siti web (es. sono esclusi siti classificati come pornografici, gioco online, trading online, ecc.) e della fruizione di specifici servizi (es. sono esclusi servizi di accesso ai social, streaming audio e video). Qualora alcuni siti web o alcuni servizi risultassero necessari per lo svolgimento dell'attività aziendale, e impropriamente resi non disponibili, è possibile contattare i servizi assistenza facendo richiesta motivata, e chiedendo l'abilitazione.

Il collegamento alla rete Internet è potenzialmente la sorgente principale di "infezione" della rete aziendale, intesa come lo scaricamento di dati e programmi (detti "malware") atti a minare l'integrità e funzionalità della rete interna o sottrarre dati. Per tale motivo è importante che ogni operatore che abbia accesso alla rete Internet eviti di accedere a servizi non noti, o comunque estranei all'attività lavorativa, e mantenga un atteggiamento cauto nell'utilizzo di servizi esterni alla rete aziendale.

È obbligatorio inoltrare pronta segnalazione attraverso i canali di assistenza nel caso in cui, a seguito di navigazione sulla rete internet o utilizzo di servizi esterni alla rete aziendale, dovessero manifestarsi comportamenti anomali della postazione di lavoro, o comunque qualora ci fosse il sospetto di tentativi di truffa/sottrazione dati/attacco informatico.

L'accesso alla rete internet è monitorato, sia a tutela della sicurezza della rete aziendale, sia per prevenire eventuali usi impropri.

3.2.4 Dischi di rete (share)

L'azienda mette a disposizione degli operatori spazio di archiviazione in rete per files/documenti generici. Tale spazio è normalmente fruibile come dischi virtuali di rete raggiungibili dal proprio PC ("virtuali" in quanto non corrispondenti a dispositivi fisici collegati al PC).

I dischi di rete sono normalmente associati al singolo operatore (disco di rete personale) e a strutture/ gruppi di operatori (es. disco di reparto, disco di struttura).

I dischi di rete sono soggetti a profilazione degli accessi: è quindi garantito che siano accessibili dai soli operatori autorizzati.

I dischi di rete non sono soggetti a strutturazione del dato, e ogni utente li gestisce in modo autonomo, organizzandoli come meglio ritiene (es. con cartelle e sotto-cartelle).

I dischi di rete sono limitati in dimensione massima dei contenuti. È possibile contattare i servizi di assistenza informatica per richiederne l'ampliamento, motivando tale richiesta.

I dischi di rete non sono deputati ad archiviare dati relativi alla salute originali, in quanto non rispettano appieno la normativa vigente in termini di integrità, continuità operativa ed il dato ivi contenuto non è riconducibile in modo univoco a posizione anagrafiche dei nostri assistiti/pazienti.

I dischi di rete non sono deputati ad una archiviazione di dati relativi alla salute anche in quanto non garantiscono una completa tracciabilità degli accessi e delle modifiche effettuate, che costituiscono obbligo di legge.

Allo scopo di consentire lo scambio di documenti tra operatori (in alternativa alla posta elettronica, in particolare quando questa risulti inutilizzabile per dimensione eccessiva dei documenti), sono resi disponibili dischi di rete di Transito, accessibili da tutti gli operatori aziendali. Tali dischi, per ovvi motivi gestionali, sono oggetto di pulizia periodica (cancellazione irreversibile dei dati ogni notte) e non sono pertanto deputate alla archiviazione a medio/lungo termine di alcun tipo di dato.

Essendo accessibili a qualunque operatore, e non tracciati negli accessi, i dischi di transito non possono essere utilizzati per la trasmissione di dati personali o sensibili.

3.3 Gli Applicativi Aziendali

Il sistema informativo aziendale comprende varie centinaia di applicativi aziendali, e copre gran parte delle diverse specifiche esigenze dell'organizzazione, dalla gestione clinica dei nostri assistiti fino alla gestione amministrativa dell'azienda.

L'abilitazione agli applicativi aziendali (permessi di accesso e uso dello strumento) può avvenire in automatico sulla base del ruolo aziendale o su richiesta esplicita del proprio responsabile di struttura (che è anche responsabile del trattamento dati aziendale). Vedi sezione dedicata.

Non è consentito l'uso di applicativi non forniti dall'azienda, in quanto non è garantita la sicurezza degli stessi, e la rispondenza alla normativa vigente. Qualora emergesse l'esigenza di nuovi applicativi/soluzioni, gli operatori devono contattare lo STIT per valutarne opportunità e modalità di adozione.

Non è consentito l'uso di applicativi aziendali per destinazioni diverse da quelle definite dall'organizzazione e dal fornitore del sistema. Per chiarimenti sulla destinazione d'uso degli applicativi aziendali, gli operatori devono rivolgersi ai canali di assistenza.

I dati gestiti nell'ambito della nostra organizzazione costituiscono patrimonio dell'azienda, e nel caso dei dati relativi alla salute costituiscono patrimonio di proprietà dell'assistito/paziente, a noi affidato per una corretta gestione nell'ambito degli scopi definiti istituzionalmente.

Usando gli applicativi aziendali ufficiali per la gestione dei dati vengono garantite la confidenzialità, l'integrità e la continuità del dato, oltre che la sua riconducibilità alla singola persona (per i dati personali e in particolare sanitari). Ogni archiviazione di dati su sistemi non aziendali o su sistemi aziendali non preposti a tale archiviazione non garantisce tali tutele, e conseguentemente mette a rischio il patrimonio aziendale, (e nel caso di dati relativi alla salute costituisce violazione della normativa vigente).

Il tentativo di installare applicativi non aziendali su qualunque dispositivo aziendale ne può compromettere la stabilità, e quindi la sicurezza. È quindi opportuno specificare, che, pur essendo già indicato che l'uso di applicativi non aziendale non è ammesso, costituisce elemento di particolare gravità il tentativo di installarli sui dispositivi aziendali.

Gli applicativi aziendali potrebbero, per motivi di sicurezza e di organizzazione, non essere disponibili su tutti i dispositivi. In caso di necessità, per estendere la disponibilità di applicativi aziendali a specifici contesti occorre contattare i canali di assistenza.

3.4 L'Autenticazione sui Sistemi Informativi

Ad ogni operatore dell'azienda, all'atto dell'iscrizione nei registri informatizzati preposti al censimento delle persone fisiche che hanno accesso alle strutture dell'azienda (a qualsiasi titolo), viene assegnata una identità digitale aziendale (anche dette "credenziali di accesso").

Tali credenziali, costituite da un Nome Utente ed una Password (inizialmente impostata provvisoriamente, e da cambiare obbligatoriamente al primo accesso) sono strettamente personali e l'operatore si assume la responsabilità di conservarle in modo sicuro, non comunicarle a terzi ed utilizzarle prontamente in ogni contesto di accesso ai sistemi informativi aziendali.

La password è soggetta, da normativa, a vincoli specifici in termini di lunghezza, complessità, e scadenza. Tali vincoli non sono derogabili. È quindi in particolare obbligatorio per gli operatori assicurarsi una sostituzione della password prima della scadenza (che i sistemi notificano all'approssimarsi).

Qualsiasi operazione sui sistemi informativi aziendali prevede l'inserimento di tali credenziali, a conferma della identità dell'operatore. L'inserimento e le verifica delle credenziali su qualsiasi sistema informativo aziendale apre una "sessione dell'utente" (intervallo temporale in cui ogni operazione è attribuita all'operatore che ha inserito le credenziali). Ogni azione svolta in tale sessione (accesso ai dati, modifica dei dati, uso di risorse informatiche aziendali locali o remote) è tracciata e ricondotta alla persona fisica corrispondente alle credenziali associate. L'azienda si riserva, sia a tutela dei dati che per obbligo normativo, di tenere traccia ("log di sistema") delle operazioni svolte dagli operatori all'interno delle loro sessioni.

Le informazioni relative alle operazioni svolte dagli operatori sui sistemi informativi aziendali possono essere utilizzate sia per individuare e perseguire usi impropri degli strumenti aziendali, sia a supporto di approfondimenti in merito a specifici episodi di operatività aziendale non strettamente informatica (es. ricostruzione di iter clinici, ricostruzione di iter amministrativi).

Nota: è possibile che alcuni sistemi, per loro caratteristiche tecniche a volte legate a elementi di sicurezza, richiedano l'inserimento di un secondo insieme di credenziali, anche differente da quello principale aziendale. A queste credenziali secondarie si applicano le stesse considerazioni e vincoli normativi sopra esposti.

3.5 Gestione dei permessi di accesso ai servizi e applicativi aziendali

L'accesso alle risorse informatiche aziendali (accesso a dispositivi fisici, accesso alla rete, accesso agli applicativi) è concesso ai soli operatori registrati presso l'azienda (dipendenti ed ogni altra figura che a vario titolo collabori con l'organizzazione) secondo due logiche:

- In automatico sulla base del ruolo (es. ad ogni operatore è automaticamente creato un account (username + password), una casella postale e-mail, e dato accesso a internet).
- Su richiesta del responsabile del trattamento dati (responsabile di struttura) o suo delegato, o su richiesta diretta della Direzione (in rappresentanza del titolare del trattamento dati).

Analogamente, ogni limitazione di accesso rispetto ai permessi automatici, o revoca di permesso precedentemente concesso può avvenire unicamente su richiesta del responsabile del trattamento dati (responsabile di struttura) o suo delegato, o su richiesta diretta della Direzione (in rappresentanza del titolare del trattamento dati).

È compito del delegato/responsabile del trattamento dati assicurarsi che i collaboratori e ogni operatore da lui coordinato che a vario titolo necessiti di accedere a sistemi informatici aziendali abbia le necessarie autorizzazioni, nei limiti dei principi di pertinenza e non eccedenza. Nel contempo, è sua responsabilità assicurarsi che, qualora vengano meno le condizioni che hanno reso necessaria l'abilitazione degli operatori, tale abilitazione sia prontamente revocata.

Le richieste di abilitazione e disabilitazione alle varie componenti dei sistemi informativi aziendali devono essere inoltrate allo STIT tramite gli appositi canali di assistenza.

3.6 Canali di Assistenza Informatica

Per ogni segnalazione, richiesta di informazioni, richiesta operativa relativa all'uso dei sistemi informatici gli operatori possono accedere al punto unico di accesso intranet (Portale Clinico Aziendale):

https://portaleclinico.asmn.re.it

Su tale portale è possibile trovare la principale modulistica on line per richiedere supporto e informazioni, ed i riferimenti telefonici da contattare per ulteriori informazioni.

4 Trattamento Informatico di Dati relativi alla Salute

4.1 Principi Generali

La gestione (informatica o cartacea) dei dati relativi alla salute è un elemento fondamentale dell'attività sanitaria per una migliore continuità assistenziale, per tutela medico-legale, e per attività di ricerca.

I dati personali relativi a nostri assistiti e pazienti, in quanto "relativi allo stato di salute", devono essere trattati in base ad un insieme di principi e indicazioni tecniche.

Attenzione: la normativa vigente e i vincoli normativi relativi al trattamento di tali dati si applicano a dati personali, quindi **dati riconducibili alla persona** (dato nominale o associato a codici riconducibili all'individuo). Ogni dato non nominale può essere trattato con le sole cautele relative alla tutela del patrimonio aziendale.

Attenzione: la normativa impone vincoli particolari per i **dati originali**, cioè ai dati in copia singola la cui perdita o alterazione comporta un danno per la persona a cui fanno riferimento; il trattamento di copie di

dati (es. per attività di ricerca, per audit clinico, ecc.) pur essendo vincolata ad alcuni vincoli di normativa, risulta meno complesso.

Attenzione: altro elemento fondamentale relativo alla classificazione dei tipi di dato è relativo al **ruolo svolto dal dato nella continuità di cura**. Per i dati (originali o non) vincolanti per la continuità di cura (la cui indisponibilità comprometterebbe la cura del paziente) sussistono vincoli maggiori in termini di modalità di gestione.

La normativa impone che il dato personale sia tutelato in termini di:

- **Riservatezza**: evitare accessi impropri, garantire la tracciabilità degli accessi, evitare che la trasmissione del dato possa renderlo visibile a terze parti non autorizzate.
- **Protezione dalla perdita e distruzione**: le aziende sanitarie devono garantire di poter "restituire" il dato all'assistito nel caso questi ne facesse richiesta, garantendone la riconducibilità anagrafica esatta.
- **Pronta disponibilità in caso di necessità**: il paziente deve poter accedere ai suoi dati (direttamente o tramite operatori sanitari da lui autorizzati), compatibilmente con le sue esigenze; es. se il paziente chiede i suoi dati per un consulto presso altra struttura è dovere dell'azienda fornire il dato prontamente.

4.2 Trattamento Informatico – Archiviazione Informatica di Dati relativi alla Salute

Dal punto di vista del trattamento informatico del dato, è obbligatorio per l'azienda garantire che i sistemi informatici adottati tutelino i tre principi generali sopra esposti. È quindi compito dello STIT, nonché responsabilità del Titolare del trattamento, assicurare l'adozione di misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alla normativa vigente, orientata alla sicurezza e alla protezione dei dati.

Oltre agli aspetti normativi, è inoltre mandato dello STIT quello di garantire uno **sviluppo organico e strategico dei sistemi informativi aziendali**. È infatti evidente che una adozione non coordinata e non omogenea di sistemi informativi sanitari porta, su scala più ampia, ad una frammentazione del dato, vanificando i potenziali benefici in termini sia assistenziali che di ricerca. Per garantirne una crescita coordinata, integrata e omogenea dei sistemi informativi, lo STIT ha il compito di assicurare che i sistemi adottati rispettino la normativa e le **linee guida aziendali**.

Non tutti i sistemi informativi aziendali rispondono ai requisiti normativi e linee guida aziendali, e non sono quindi tutti destinati all'archiviazione di dati relativi alla salute. **Non è pertanto consentita l'archiviazione di dati relativi alla salute su sistemi non destinati esplicitamente a tale scopo.**

In particolare NON SONO ADEGUATI al trattamento sicuro di dati relativi alla salute i seguenti sistemi:

- **Spazio disco sul PC** (o altri dispositivi singoli): i dati personali archiviati sui singoli PC possono essere oggetto di accesso da parte di terze parti (es. in caso di furto), possono essere persi in caso di guasto.
- **Disco di rete personale (o di struttura)**: i dati personali archiviati sui dischi di rete, anche se protetti da accessi non consentiti, non sono garantiti in termini di tracciabilità degli accessi, integrità e pronta disponibilità.
- **Portale Intranet:** i dati personali archiviati sul portale Intranet aziendale. In quanto esposto anche potenzialmente su internet, non è adeguatamente protetto da accessi non consentiti; inoltre il portale intranet non garantisce integrità e continuità del dato (in caso di guasto i dati potrebbero non essere del tutto recuperabili, e rimanere inoltre indisponibili per un tempo non determinabile).

- **Posta Elettronica**: i sistemi di posta elettronica, oltre a non essere adeguati per la trasmissione di dati personali (vedi sezione successiva), non costituiscono un sistema a norma per archiviazione di dati relativi alla salute (es. consulenze, appuntamenti, comunicazioni con pazienti, ecc.), in quanto non garantiscono integrità, continuità, tracciabilità di accesso e riconducibilità anagrafica dei dati.

  Esempio: l'archiviazione di dati nominali su file Excel sul disco locale o disco di rete (personale o di reparto) non sono consentiti.

  Esempio: l'archiviazione di dati non nominali e non originali su file Excel su disco locale o disco di rete è consentita in quanto non soggetta ai vincoli relativi ai dati relativi allo stato di salute.

Sono invece ADEGUATI per il trattamento di dati relativi alla salute NON ORIGINALI e NON COINVOLTI IN PROCESSI CHE PREVEDANO CONTINUITA' CLINICA i seguenti sistemi:

- **Portale Clinico**: il portale destinato all'attività clinica aziendale consente l'archiviazione del dato sanitario garantendo accessi riservati, tracciabilità di accessi e modifiche e riconducibilità alla posizione anagrafica. Non è garantita la completa integrità dei dati e la continuità di servizio.

  Esempio: archiviazione di dati per audit clinici (quindi copie di dati originali presenti su altri sistemi o su carta) possono essere archiviati su sezioni dedicate del Portale Clinico.

  Esempio: consulenze informatizzate NON possono essere archiviate su Portale Clinico in quanto dati originali, la cui integrità non potrebbe essere garantita.

Sono invece ADEGUATI per il trattamento di dati relativi alla salute i seguenti sistemi:

- Sistemi di Cartella Clinica Informatizzata.
- Sistemi di gestione della Refertazione Ambulatoriale.
- Sistemi di gestione Specialistica (cosiddetti "Verticali Dipartimentali").

Per valutare l'adeguatezza di un sistema all'archiviazione di dati personali e sanitari, contattare lo STIT.

Sono descritti in appendice i requisiti minimi e le linee guida aziendali, allo scopo di consentire ai professionisti che leggono il presente regolamento di comprendere le caratteristiche dei sistemi deputati all'archiviazione dati relativi alla salute.

4.3 Trasmissione Informatica di Dati relativi alla Salute

La trasmissione di tali dati è a tutti gli effetti un tipo di "trattamento", pertanto è soggetta ai requisiti normativi precedentemente descritti. In particolare, i vincoli di riservatezza e tracciabilità diventano fondamentali in quanto si applicano al mezzo usato per trasmettere i dati.

È opportuno ricordare che tali vincoli sussistono solo nel caso in cui la trasmissione sia relativa a dati nominali. Questo implica che qualsiasi trasmissione che riporti riferimenti non espliciti a pazienti (es. link a documenti su applicativi aziendali, riferimenti anonimizzati, ecc.) non rientrano nei vincoli di riservatezza e tracciabilità e conseguentemente possono sfruttare i normali canali di comunicazione "generalisti". In particolare, il DataWareHouse clinico (Dossier Sanitario) consente di trasmettere via posta elettronica link a specifici referti o alla storia clinica di specifici pazienti.

Lo STIT ha il compito di verificare i canali di trasmissione dei dati relativi alla salute, garantendone la rispondenza alla normativa in termini di riservatezza.

Va ricordato che la trasmissione di dati originali (ad esempio consulenze) implica anche una esigenza di archiviazione a norma del dato. Molti strumenti di trasmissione dei dati seppure rispondenti ai requisiti minimi per una trasmissione sicura, possono non essere adeguati per l'archiviazione. Ad esempio, la posta elettronica certificata può essere ritenuta rispondente ai requisiti di sicurezza per una trasmissione dati ma

non risponde ai requisiti minimi alla conservazione del dato, pertanto non può essere usata per conservare dati in versione originale, quali ad esempio consulenze o esiti di accertamenti diagnostici.

È fondamentale ricordare che la trasmissione dei dati deve avvenire tra operatori sanitari autorizzati/incaricati al trattamento degli stessi. Ogni trasmissione verso altri destinatari (es. case farmaceutiche, colleghi di altre strutture, enti di ricerca, colleghi aziendali non autorizzati alla visione dei dati specifici) prevede esplicite autorizzazioni ed informativa per l'interessato (es. protocollo di ricerca autorizzato dal Comitato Etico, trasmissione dati verso enti in virtù di convenzioni, ecc.). Tali autorizzazioni ed informativa sono relative sia al destinatario della trasmissione che alle modalità di trasmissione (informatizzate o non).

4.3.1 La Posta Elettronica

La posta elettronica tradizionale (e-mail) non è uno strumento sicuro poiché la trasmissione avviene "in chiaro" quindi senza garanzia di confidenzialità dei contenuti e potenzialmente intercettabile sia nelle comunicazioni verso destinatari interni all'azienda che esterni.

Va inoltre ricordato che le caselle postali "gratuite" rese disponibili da varie aziende del mercato ICT (es. Google, Microsoft, ecc.) sono tali in quanto l'utente cede ai fornitori alcuni diritti di accesso e consultazione dei dati. Tali fornitori si riservano di utilizzare tali dati a scopo commerciale ivi compresa la possibilità di cedere parte delle informazioni a terze parti. La trasmissione di dati che si appoggi su tali servizi non è quindi riservata tra mittente e destinatario, ma coinvolge istituzionalmente il fornitore del servizio gratuito.

Anche la posta elettronica aziendale, seppure la probabilità di accesso fraudolento sia sicuramente minore, non ha garanzie di sicurezza tali da renderla formalmente adeguata per la trasmissione di dati relativi allo stato di salute (anche perché accessibile dall'esterno della struttura tramite qualsiasi PC, tablet o smartphone collegati a Internet).

Soluzione simile, ma alternativa alla e-mail tradizione, è la Posta Elettronica Certificata (PEC). Tale strumento di comunicazione, di fatto molto simile alla posta elettronica, oltre a garantire tracciabilità e certezza di recapito, garantisce anche una comunicazione sicura del messaggio tra i server coinvolti nelle comunicazioni, e conseguentemente è uno strumento adeguato per la trasmissione di dati relativi allo stato di salute. Essendo però una tipologia di servizio non comune (e in molti casi a pagamento), è meno diffusa della posta elettronica tradizionale, e di solito limitata ad un uso professionale.

L'azienda può predisporre caselle PEC di equipe per le strutture aziendali che nell'ambito di convenzioni specifiche necessitino di comunicare via PEC con istituzioni terze.

4.3.2 Portale Caricamento Documentazione Sanitaria

Allo scopo di consentire una facile soluzione di comunicazione dal paziente verso la nostra organizzazione, lo STIT rende disponibile un Portale Web su cui i professionisti dell'azienda possono predisporre aree di deposito di documentazione e comunicazioni da parte dei nostri pazienti (definite "Cartelle Condivise con il Paziente"). Ad ogni caricamento da parte del paziente viene inviata automaticamente una e-mail di notifica di presenza di nuova documentazione verso tutti i professionisti dell'equipe associata a quella cartella, consentendo loro di accedere in modo tracciato e sicuro al portale per lo scaricamento della documentazione inviata.

Tali cartelle condivise, in quanto disponibili in sola trasmissione (dall'esterno non è possibile consultare o scaricare il materiale caricato), rispettano i vincoli normativi di riservatezza e tracciabilità.

Lo strumento può essere configurato per la trasmissione di documentazione dalla nostra azienda verso il paziente. Questa configurazione è possibile solo in deroga alla normativa per situazioni in cui il FSE (vedi sezione seguente) non sia ancora disponibile o utilizzabile.

Per attivare una cartella condivisa con i pazienti in carico ad una equipe, occorre contattare i canali di assistenza STIT.

4.3.3 Fascicolo Sanitario Elettronico (FSE)

La normativa nazionale indica nel Fascicolo Sanitario Elettronico (FSE) il canale di comunicazione informatizzato unico e ufficiale da parte delle strutture sanitarie pubbliche verso il paziente.

Conseguentemente, su indicazione regionale, non è consentita la creazione di strumenti informatici diversi dal FSE per la trasmissione di documentazione sanitaria verso li paziente.

Al FSE vengono ad oggi inviate regolarmente:

- Tutti i referti ambulatoriali (laboratorio, radiologia ed ogni specialistica) generati all'interno dell'organizzazione.
- Tutti i referti finali di Pronto Soccorso.
- Tutte le notifiche di Accettazione di Ricovero Ordinario/Day Hospital/Day Service.
- Tutte le lettere di dimissione relative a episodi di Ricovero Ordinario/Day Hospital/Day Service.
- (altri documenti specifici quali inviti allo screening, buoni celiachia, certificati vaccinali, certificati di idoneità sportiva, ecc.).

Qualora fosse necessario veicolare altre tipologie di documenti (già gestiti in modalità informatizzata internamente all'azienda) è possibile predisporre i necessari canali verso FSE. Qualora vi sia interesse a valutare questa modalità di comunicazione occorre contattare i canali di assistenza STIT per maggiori informazioni.

Attenzione: il FSE è uno strumento regionale tecnicamente consolidato e in corso di diffusione in Emilia Romagna e altre regioni italiane. Potrebbero però non essere ancora attivo per molte aree del nostro paese. Per la trasmissione di documentazione sanitaria verso pazienti di zone non servite dal FSE, la Regione Emilia Romagna e l'Azienda si stanno dotando di strumenti informatici temporanei.

4.3.4 Notifiche e-mail da Applicazioni Sanitarie

Qualora fosse necessario trasmettere routinariamente dati relativi alla salute contenuti in applicazioni sanitarie (es. cartelle cliniche, referti ambulatoriali o altri sistemi specialistici) ad altri operatori aziendali è possibile chiedere allo STIT di predisporre sistemi automatici che, al verificarsi di specifiche condizioni, trasmettano via posta elettronica un link o altre informazioni sintetiche (non nominali).

4.3.5 Portale Clinico per la comunicazione di Dati relativi allo Stato Salute

Qualora fosse necessario trasmettere dati internamente all'azienda, e non fosse possibile trasmettere link al DataWareHouse Clinico o generare notifiche automatiche da parte di applicativi sanitari, è possibile sfruttare aree dedicate sul Portale Clinico predisposte dallo STIT in cui depositare i dati di interesse (come documenti allegati), e trasmettere (automaticamente o manualmente) via posta elettronica il link al portale clinico ai destinatari.

Questa strumento è particolarmente indicato per la trasmissione di grandi quantità di dati.

4.3.6 Comunicazione con i MMG/PLS

Va ricordato che MMG e PLS sono titolari terzi rispetto all'azienda, seppure convenzionati. Questo implica che non sia automaticamente lecita la comunicazione di dati relativi alla salute verso di loro da parte dell'azienda sanitaria.

La Regione ha individuato nella rete SOLE il canale unico e capillare per la comunicazione da parte delle strutture sanitarie verso i MMG/PLS. Ogni documento inviato dalle aziende sanitarie alla rete SOLE viene

trasmesso, previa verifica del consenso del paziente (espresso una tantum e revocabile in qualsiasi momento), al suo MMG/PLS.

Ogni trasmissione diretta da parte di operatori aziendali di dati da e verso MMG/PLS che non avvenga nell'ambito di specifiche convenzioni (e di cui conseguentemente i pazienti sono stati adeguatamente informati ed hanno espresso consenso, qualora previsto), non è autorizzata.

Lo STIT rende disponibile lo strumento denominato OFI per la comunicazione sicura di dati verso i MMG/PLS (singolarmente o massivamente). Tale strumento è utilizzabile per la comunicazione di dati non veicolati tramite SOLE, ma previsti nell'ambito di altre specifiche convenzioni.

4.3.7 Interlocutori e Strumenti Utilizzabili

La trasmissione di dati relativi allo stato di salute da parte degli operatori dell'azienda può avvenire da e verso i seguenti interlocutori:

- Altri operatori dell'azienda (autorizzati a trattare i dati inviati).
- Enti terzi, autorizzati da apposita convenzione a ricevere e trattare dati di pazienti in carico.
- MMG/PLS, nell'ambito della rete SOLE o di convenzioni specifiche
- Pazienti.

Gli strumenti informatici deputati alla comunicazione da e per gli interlocutori di cui sopra sono riassunti nel seguente diagramma:

Da \ Per	Operatori AUSL	Enti Terzi	MMG/PLS	Pazienti
Operatori AUSL	Trasmissione e-mail non nominale Trasmissione e-mail di link al DWH Trasmissione e-mail di notifiche da Applicazioni Sanitarie Appoggio di dati su Portale Clinico	Posta Elettronica Certificata	OFI	Fascicolo Sanitario Elettronico Portale Caricamento Documentazione Sanitaria (*) Portale Regionale Scaricamento Referti(*)
Enti Terzi	Posta Elettronica Certificata	-	.	.
MMG/PLS	OFI	-	-	-

Pazienti	Portale Caricamento Documentazione Sanitaria			

(*) soluzione provvisoria (in attesa di diffusione nazionale del FSE)

5 Acquisizione di Beni Informatici

5.1 Acquisizione di Nuovo Software

Dovendo garantire la conformità ai requisiti tecnici minimi e alle linee guida aziendali, **non è consentita l'adozione autonoma, da parte di strutture o singoli operatori sanitari, di sistemi informativi destinati al trattamento di dati relativi alla salute senza una preventiva verifica da parte dello STIT**.

Lo STIT quindi si pone come interlocutore fondamentale per la fase di valutazione preliminare all'adozione di nuovi sistemi, e successivamente rende disponibili i servizi necessari per l'attivazione e la gestione dei sistemi (la cui gestione può poi operativamente essere affidata anche a strutture diverse dallo STIT).

La richiesta di acquisizione di nuovi strumenti software deve, per ovvie ragioni di strategia ed economicità, passare il vaglio dello STIT affinché verifichi se esistono già sistemi informativi aziendali dedicati allo scopo.

Nel caso non esistano, lo STIT verifica se sussistono condizioni per una acquisizione diretta del software richiesto dal professionista. Un software è acquisibile direttamente qualora le sue caratteristiche lo individuino come "unico" e fornito da un solo fornitore/distributore, oppure qualora la sua acquisizione comporti immediate ed evidenti economie per l'azienda (ad esempio in caso di rinnovo di software preesistente, condizione in cui vengono meno gli oneri di installazione e formazione).

Dovendo l'azienda attenersi alla normativa vigente per gli acquisti della Pubblica Amministrazione, qualora non sussistano le condizioni per una acquisizione diretta, diviene necessario procedere tramite gara.

Un sistema informativo, qualora archivi dati relativi allo stato di salute o sia comunque parte dell'iter diagnostico-terapeutico, deve prevedere garanzie di integrità del dato (vedi sezione precedente sulla archiviazione) e garanzie di continuità operativa (intervento in assistenza in tempi rapidi). Ogni acquisizione di software pertanto **prevede sempre l'acquisizione dei relativi servizi di assistenza da parte del fornitore**.

Qualora per un sistema software non sia disponibile un servizio di assistenza (ad esempio per software forniti in omaggio da aziende farmaceutiche, software sviluppati da aziende di piccolissime dimensioni o da singoli professionisti o software artigianali sviluppati da operatori sanitari o da soggetti esterni) lo STIT potrebbe negare l'autorizzazione all'acquisto o all'installazione.

L'iter di acquisizione di software, in quanto materiale inventariabile (seppure "immateriale") richiede un passaggio di autorizzazione di budget. È pertanto necessario pianificare per tempo l'acquisizione, confrontandosi con lo STIT per stimare l'importo necessario sia per l'acquisizione che per i relativi servizi di installazione e successiva assistenza. La proposta di acquisto, se autorizzata dallo STIT, deve essere presentata con gli importi stimati alle direzioni in fase di discussione di budget.

5.2 Acquisizione di Nuovo Hardware

L'acquisizione di hardware di qualsiasi tipo (computer, stampanti, periferiche, ecc.) da parte della Pubblica Amministrazione è sempre più soggetta a vincoli normativi che impongono verifiche di economicità e sostenibilità.

L'iter di acquisto prevede quindi la trasmissione allo STIT della richiesta, espressa come "esigenze" (e non come marca e modello). Tali esigenze saranno analizzate per trovare lo strumento più adeguato ed economico disponibile tramite i canali di acquisto della pubblica amministrazione. La richiesta sarà poi portata dallo STIT all'attenzione delle direzioni per valutazioni di budget.

È importante sottolineare che i costi di un sistema hardware (ad esempio un computer) non si limitano al solo acquisto, ma comprendono anche la sua gestione (ad esempio gli interventi di assistenza da parte degli operatori STIT). Allo scopo di ridurre tali costi indotti, lo STIT cerca di rendere quanto più omogeneo possibile il parco hardware installato. È quindi possibile che sia rifiutato l'acquisto di dispositivi "esotici" richiesti in sostituzione di un prodotto standard aziendale. Questo, ovviamente, solo qualora non sussistano reali esigenze per discostarsi da tale standard.

Attenzione: il sistema informativo dell'azienda sanitaria è di tipo "enterprise". Questo termine identifica realtà in cui ogni stazione di lavoro è potenzialmente utilizzabile da qualsiasi operatore. Non esiste infatti il concetto di "dispositivo per uso personale". Conseguentemente ogni acquisizione hardware sarà valutata in un'ottica di potenziale riutilizzo da parte di altri operatori, e non sono normalmente autorizzate personalizzazioni non giustificate da specifiche esigenze.

6 Accesso ai dati per uso non legato all'attività di cura

Riassumendo i principi di base della normativa sul trattamento dati:

> I dati sono di proprietà del paziente, che li affida all'azienda al solo scopo di curarlo e per altri scopi definiti nell'informativa a lui consegnata o resa disponibile (e autorizzazioni esplicite per attività di ricerca o altre destinazioni). È dovere dell'azienda conservare tali dati e consentirne la consultazione limitatamente agli scopi dichiarati.

Da questo principio di base nascono una serie di linee guida aziendali che lo STIT applica nel consentire accessi ai dati per scopi diversi, riassunte di seguito:

- L'accesso ai dati attraverso i sistemi informativi sanitari è consentito nei limiti imposti dai permessi configurati sui sistemi informativi stessi, e limitatamente alle destinazioni d'uso dei sistemi stessi. L'uso di sistemi informativi sanitari per accesso di dati per scopi diversi non è consentito.
- Ogni accesso ai dati per altri scopi, in particolare per estrazioni massive (anche dette "estrazioni dati"), in quanto non legato direttamente alle destinazioni d'uso del sistema informativo, deve essere richiesto allo STIT previa:
    - (se legato ad attività di progetti di ricerca) autorizzazione dal Comitato Etico e dei direttori delle unità operative di pertinenza del dato.
    - (se non legato ad attività di progetti di ricerca, es. valutazioni gestionali, audit clinici interni, valutazioni epidemiologiche interne) autorizzazione dei direttori delle unità operative di pertinenza dei dati.

Per richiedere accessi ai dati per scopi diversi da quelli di destinazione d'uso dei sistemi informativi, fare riferimento ai canali di assistenza STIT.

Lo STIT ha il compito di tracciare tali accessi, come previsto da normativa.

Attenzione: l'estrazione dei dati dai sistemi sanitari DEVE essere svolta dagli operatori dello STIT, in quanto agisce su sistemi la cui funzionalità non può essere compromessa o rallentata. In alcuni casi le operazioni di estrazione vengono eseguite di notte o nei fine-settimana per evitare di interferire con la normale operatività dei sistemi.

7 Riferimenti dello STIT

Sede Presidio Ospedaliero - Arcispedale Santa Maria Nuova, viale Risorgimento, 80: 0522.296966

Sede Legale Ausl - via Amendola, 2: 0522.335370

8 Appendice: Requisiti Minimi e Linee Guida Aziendali per Software Ad uso Sanitario

8.1 Requisiti Tecnici Minimi (da normativa)

8.1.1 Riservatezza dei dati

Il sistema adottato deve archiviare i dati relativi personali o allo stato di salute su server centrali, e non sui dispositivi locali.

Il requisito nasce dall'esigenza di tutela della riservatezza in caso di furto del computer locale. In azienda sono presenti oltre seimila elaboratori, sparsi su tutto il territorio provinciale. È fisiologico che ci sia un certo numero di furti o smarrimenti. È fondamentale che a seguito di questi furti o smarrimenti non siano conseguenti anche la sottrazione di dati. Tale sottrazione costituirebbe infatti violazione della riservatezza, oltre che potenziale perdita degli stessi (violazione di integrità dei dati) qualora fossero archiviati solo sul computer in versione unica.

Il sistema deve consentire l'accesso ai dati solo a seguito di autenticazione (verifica dell'identità dell'utente). L'autenticazione deve avvenire come da normativa vigente (es. lunghezza della password, obbligo di cambio password periodico, ecc.).

Il sistema deve prevedere un tracciamento di tutti gli accessi ai dati

L'esigenza legale di potere in qualsiasi momento documentare eventuali accessi impropri al dato (in lettura o modifica), impone che ogni operazione sui sistemi sia associabile ad un utente specifico.

Su alcuni sistemi particolarmente critici è previsto anche un monitoraggio pro-attivo degli accessi potenzialmente impropri, allo scopo di intercettare eventuali non conformità nell'utilizzo.

Il sistema deve consentire la profilazione degli utenti: deve essere possibile la limitazione di accesso a porzioni di dati a specifici gruppi di utenti.

Il sistema sanitario è oggi composto da molte figure professionali, che vanno oltre la tradizionale organizzazione in "medici e infermieri". È quindi importante che sui sistemi informativi sia possibile definire i "permessi" di accesso ai dati in modo differenziato per ciascun ruolo, sia per garantire la riservatezza (permesso di lettura), che l'integrità (permesso di modifica). Queste limitazioni dei permessi sono anche a tutela del professionista sanitario, a cui è impedito di eseguire involontariamente accessi ed operazioni a lui non consentite. La normativa prevede

il principio di "pertinenza e non eccedenza" degli accessi, imponendo che ogni profilazione dei permessi sia mantenuta al minimo livello di estensione possibile.

8.1.2 Integrità dei dati

Il sistema adottato deve garantire una protezione da virus informatici

Frequentemente i sistemi informatici aziendali, per quanto protetti dalla rete, sono oggetto di "infezioni" informatiche. Queste infezioni sono spesso causate da singoli elaboratori non coperti dai sistemi antivirus, quindi non a norma. Proprio come per i virus "biologici", è fondamentale prevenire, garantendo che tutti i sistemi aziendali siano coperti da software antivirus. È inoltre necessario che organizzativamente non sia consentito l'uso di vettori di infezione (strumenti di archiviazione esterni, es. chiavette USB, CD, DVD).

Il sistema adottato deve garantire un backup dei dati

Gli elaboratori si guastano… è normale. È necessario garantire che tutti i dati abbiano una copia di emergenza (backup) per assicurarci di non perderli. Tale copia di backup deve essere eseguita con una frequenza tale da garantire che, in caso di necessità, sia possibile recuperare una versione dei dati relativi ai nostri pazienti sufficientemente aggiornata. È inoltre necessario che organizzativamente non siano archiviati dati al di fuori dei sistemi oggetto di backup.

Il fornitore del sistema deve garantire che, in caso di completa distruzione dell'archivio dati, sia possibile ricostruirlo a partire dal backup dei dati nei tempi massimi indicati dalla normativa vigente

I fornitori dei nostri sistemi devono garantire di essere in grado, in caso di necessità, di recuperare i dati dalla copia di emergenza (backup) in tempi compatibili con l'operatività sanitaria.

Il fornitore del sistema deve garantire un continuo aggiornamento delle componenti del sistema allo scopo di prevenire possibili problematiche di sicurezza (es. aggiornamenti del sistema operativo)

Tutti i sistemi informativi, di qualsiasi tipo e produttore, hanno piccole falle di sicurezza che potrebbero portare a distruzione di dati o accessi abusivi. Queste falle emergono col tempo, e i fornitori dei sistemi distribuiscono, a titolo gratuito, aggiornamenti che aggiustano questi malfunzionamenti. I fornitori dei nostri sistemi sanitari devono garantire questi servizi di aggiornamento.

Il sistema deve prevedere il collegamento ai sistemi anagrafici aziendali per i dati dei pazienti/assistiti a livello centralizzato

L'iter clinico di un paziente prevede la raccolta dei dati su sistemi diversi. È obbligo dell'azienda garantire al paziente la completa riconducibilità di qualsiasi dato alla posizione anagrafica corretta. A tale scopo è necessario che tutti i sistemi informativi ad uso sanitario siano collegati all'anagrafe aziendale.

8.1.3 Pronta Disponibilità del Dato

Il sistema deve garantire, tramite soluzioni tecniche e/o organizzative, che il dato sia sempre disponibile (inteso come indisponibile al massimo entro una tolleranza dichiarata).

Lo STIT adotta soluzioni tecniche per garantire che i dati relativi alla salute non siano mai in singola copia, e che in caso di indisponibilità del sistema principale (per attività manutentive o guasti), i dati siano resi disponibili tramite sistemi secondari raggiungibili automaticamente o tramite procedure organizzative specifiche. I fornitori di sistemi informativi sanitari devono predisporre i loro sistemi affinché tale garanzia di continuità sia possibile.

8.2 Linee Guida (Aziendali)

8.2.1 Integrità dei Dati e Continuità

Il sistema deve prevedere un monitoraggio delle sue performance allo scopo di individuare preventivamente l'eventuale emergere di malfunzionamenti.

Pur essendo previsti, da requisiti di normativa, sistemi di garanzia di integrità (backup) e continuità (replica del dato), allo scopo di prevenire l'attivazione di tali rimedi di emergenza in caso di guasto, l'azienda chiede ai fornitori di monitorare attivamente i sistemi allo scopo di individuare l'emergere di problemi prima che questi generino una potenziale perdita di dati.

8.2.2 Riservatezza e Tracciabilità

Il sistema deve potersi collegare alla infrastruttura di autenticazione aziendale, garantendo quindi agli utenti di poter utilizzare le stesse credenziali (nome utente e password) su tutti i sistemi informativi.

Avere credenziali (nome utente e password) diverse per ogni sistema, seppure formalmente a norma, rende difficile l'operatività. Quando possibile, l'azienda impone ai fornitori l'utilizzo dei sistemi di autenticazione aziendale centralizzata, consentendo quindi l'utilizzo di un solo insieme di credenziali aziendali.

Il sistema deve prevedere una storicizzazione di tutti i dati modificati, garantendo il recupero di versioni precedenti del dato e indicazione sugli utenti che hanno eseguito le modifiche.

A scopo di tutela medico-legale dell'azienda e dei singoli operatori, in aggiunta ai requisiti da normativa di tracciabilità degli accessi in lettura e modifica, l'azienda chiede, quando possibile, ai sistemi informativi sanitari la completa tracciabilità delle versioni del dato. Tale tracciabilità consente di rispondere non solo dell'identità degli utenti che hanno eseguito modifiche, ma anche la ricostruzione esatta delle modifiche apportate.

8.2.3 Strutturazione e Integrazione dei Dati

Il sistema deve prevedere, in tutti i casi in cui sia possibile, una strutturazione del dato (suddivisione della informazione in campi, evitando quindi i testi liberi) e una sua codifica, adottando preferibilmente codifiche consolidate (nazionali o internazionali).

I dati archiviati sono spesso oggetto di indagini epidemiologiche, ricerca, o semplici valutazioni statistiche sull'attività sanitaria. Sebbene dal punto di vista clinico i dati testuali possono essere più che adeguati, è sempre auspicabile, in prospettiva, organizzare i dati in modo che possano essere analizzati statisticamente. È pertanto preferibile organizzare il dato in porzioni di informazione omogenee (campi) e rappresentarlo usando codifiche standard (e non solo descrizioni testuali).

Il sistema deve prevedere l'esportazione di una sintesi dei propri dati relativi allo stato di salute verso il DataWareHouse Clinico.

La continuità clinica, se supportata da sistemi informativi, imporrebbe che ogni operatore possa accedere a tutti i sistemi informativi coinvolti nell'iter diagnostico-terapeutico. Essendo questo difficilmente sostenibile, è necessario disporre di un sistema centrale, detto "Clinical Data Repository (CDR)" (o Dossier Sanitario) che collezioni e renda fruibile in modo unitario copie di tutti i documenti e dati generati nell'iter di cura. Nella nostra azienda tale sistema prende il nome di DataWareHouse Clinico. Viene chiesto a tutti i sistemi informativi di nuova acquisizione di riversare una sintesi dei propri dati sul DataWareHouse Clinico.

Il sistema deve evitare il reinserimento manuale di dati che siano già disponibili nei sistemi informativi sanitari aziendali (es. esiti di accertamenti diagnostici). Deve pertanto essere prevista l'importazione automatica o semi-automatica di tali esiti dal DataWareHouse Clinico.

Il re-inserimento di dati disincentiva significativamente la rilevazione delle informazioni in formato elettronico. È quindi necessario che, attraverso sistemi centrali di condivisione dell'informazione (es. il DataWareHouse clinico in uso presso la nostra azienda), sia possibile importare automaticamente le informazioni già presenti su altri sistemi. Viene chiesto a tutti i sistemi, quando possibile, di consentire il recupero dati da DataWareHouse Clinico.

Qualora il sistema preveda l'inserimento di richieste di accertamento diagnostico o di altra attività clinica da inoltrare verso terzi, il sistema deve prevedere l'invio automatico di tali richieste tramite i sistemi di Order Entry interaziendali, evitando quindi di obbligare gli operatori sanitari al re-inserimento manuale delle richieste su altri sistemi.

L'attività degli operatori sanitari non si conclude con la rilevazione dei dati e con la consultazione degli accertamenti diagnostici. Affinché un sistema informativo sia effettivamente utile agli operatori sanitari è necessario che consenta anche di gestire le attività prescrittive di farmaci e accertamenti. È pertanto necessario che, qualora il sistema preveda tali operazioni, queste non siano una semplice rilevazione della prescrizione/richiesta, ma siano collegati anche con i sistemi informativi che erogano tali prestazioni (es. sistema di laboratorio, radiologia, CUP, somministrazione farmaci, ecc.).

8.2.4 Sostenibilità del sistema

Il sistema deve essere dotato di modalità di accesso riservate ad amministratori di sistema, e tali accessi devono essere resi disponibili allo STIT o ad altri utenti dell'azienda sanitaria incaricati della gestione ordinaria del sistema. Tale attività non deve rimanere in carico esclusivo al fornitore del sistema.

Un rischio che c'è sempre con qualsiasi prodotto, ma in particolare con i sistemi informativi, è quello di dipendere dal fornitore per la gestione ordinaria. Questa situazione, seppur comoda in alcune circostanze, può rendere il sistema economicamente non sostenibile. È pertanto fondamentale che i sistemi informativi acquisiti siano gestibili, nella loro quotidianità, da amministratori di sistema della nostra azienda.

9 Appendice: Creazione di Password

La definizione della propria password deve avere come obiettivo primario l'impossibilità da parte di terze parti di indovinarla o ricostruirla sulla base di informazioni sulla vostra persona.

Di seguito alcuni elementi che costituiscono aspetti normativi e linee guida/suggerimenti per la composizione di una buona password:

- (da normativa) La password deve essere di almeno 8 caratteri.
- La sequenza delle lettere deve sembrare casuale e priva di logica per un estraneo.
- Usare contemporaneamente lettere MAIUSCOLE e minuscole .
- Inserire almeno un numero.
- Inserire simboli non alfanumerici come "@", "#", "%", "!", "$", …
- Evitare invece l'utilizzo di:
    - parole del vocabolario, nomi di paesi o animali
    - il proprio nome, cognome, soprannome o quello di familiari
    - la data di nascita personale o riferimenti personali come il codice fiscale
    - non ripetere la stessa parola di seguito.

    Esempi di password da evitare: giuseppe85, miaomiao, fidobello, 13012009, RSSMRA88C01H627B

- Non usare la stessa identica password per più sistemi (es. evitare di impostare la stessa password per e-mail personale e accesso ai sistemi aziendali).

Esistono sistemi su internet che "verificano" l'appropriatezza di una password. Ad esempio, suggeriamo il seguente: http://www.passwordmeter.com/ (Lo score dovrebbe superare almeno il 60%).

10 Appendice: Domande Frequenti

10.1 Domande Frequenti - Autenticazione (Username e Password)

10.1.1 Posso dare le mie credenziali ad un collega che le ha dimenticate?

Le credenziali sono strettamente personali. Prestare le credenziali ad un collega è una violazione del regolamento aziendale, oltre che degli obblighi conseguenti alla nomina a Incaricato al Trattamento Dati.

Inoltre, ogni operazione svolta dal collega sarà imputata a te, e anche qualora tu riuscissi a dimostrare l'estraneità, ti verrebbe comunque imputata la responsabilità di un uso improprio dei mezzi aziendali.

Il collega che ha perso le credenziali può utilizzare i canali di assistenza informatica aziendali (anche in reperibilità notturna e festiva) per recuperare le proprie credenziali di accesso.

10.1.2 Ho involontariamente eseguito operazioni e redatto documentazione sanitaria con la sessione di un collega, e conseguentemente tutto è stato tracciato a suo nome, come posso sistemare?

In questi casi è necessario segnalare prontamente l'accaduto ai canali di assistenza informatica. Insieme a loro valuterete se è opportuno e possibile annullare le operazioni svolte e ri-eseguirle con le credenziali corrette, o tracciare informaticamente tramite dichiarazione dell'operatore reale la reale identità di chi ha svolto le operazioni (es. dichiarazione nel referto che "Il testo del referto, redatto dal Dr. XXXXX XXXXX, risulta erroneamente attribuito al Dr. YYYYY YYYYYY per problemi di natura informatica".

10.1.3 Cambiare continuamente credenziali su PC condivisi è scomodo… Non c'è altro modo?

Purtroppo la normativa impone una disconnessione ad ogni attivazione di altra sessione.

Alcuni applicativi consentono, per migliorare l'operatività, di aprire sessioni secondarie, all'interno di quella principale, relative ad altri utenti (il cosiddetto "cambio utente al volo"). Tale modalità, seppure molto comoda, va usata con accortezza in quanto chi ha aperto la sessione "ospitante" (quella principale, che rimane attiva) ha l'obbligo di continuare a sorvegliarla e assicurarsi che nessuno la utilizzi direttamente.

10.2 Domande Frequenti – Archiviazione Dati Relativi allo Stato di Salute

10.2.1 Posso archiviare dati di pazienti sui dischi di rete?

I dischi di rete garantiscono la confidenzialità del dato (possono accedervi solo gli utenti abilitati), ma non garantiscono la completa tracciabilità al singolo dato (chi ha aperto uno specifico file, e cosa ha eventualmente modificato). Pertanto l'uso dei dischi di rete per l'archiviazione di dati (nominali) dovrebbe essere limitata a operazioni temporanee di elaborazione degli stessi.

I dischi di rete non garantiscono integrità e continuità operativa con standard compatibili con l'attività sanitaria. Conseguentemente stante il rischio di perdita di dati e potenziale indisponibilità temporanea, i dischi di rete non possono essere utilizzati per archiviare dati relativi allo stato di salute originali (la cui distruzione sarebbe permanente) o necessari per l'operatività clinica (che sarebbe interrotta in caso di indisponibilità temporanea del dato).

10.2.2 Vorrei condividere alcuni documenti solo con specifici colleghi (e non tutto il reparto), è possibile?

Sì, previa richiesta motivata da parte del delegato/responsabile al trattamento dati o suo autorizzato/incaricato è possibile creare nuovi dischi di rete dedicati a scopi specifici (team specifici). Tali dischi possono anche avere la funzione di scambio documenti, in alternativa alla posta elettronica e allo spazio di Transito. Rimangono valide le considerazioni generali sulla inadeguatezza alla archiviazione a lungo termine di dati relativi allo stato di salute.

10.2.3 Posso archiviare i dati personali e relativi allo stato di salute dei miei pazienti su Excel (o Access, o Word)?

Purtroppo no. Questi sistemi, come anche gli equivalenti di Open Office, seppure utilissimi in ambito di "produttività individuale" non rispettano molti dei requisiti minimi e delle linee guida.

Ad esempio:

- non garantiscono l'integrità del dato (capita abbastanza frequentemente che documenti Word, Access o Excel si "corrompano" perdendo i dati contenuti).
- non garantiscono un accesso limitato (chiunque può aprire questi documenti).
- non tracciano chi fa accesso al dato, e che modifiche ha fatto.
- il fornitore di questi sistemi (Microsoft, o altro fornitore nel caso di prodotti analoghi) non si assume alcun onere di garanzia di integrità del dato o di recupero dello stesso in caso di malfunzionamento.
- consentono, anzi incentivano il salvataggio dei dati in locale invece che su server.
- non sono integrabili con il resto dei sistemi del SIO (es. anagrafe, DataWareHouse).

10.2.4 Posso archiviare i dati personali e relativi allo stato di salute dei miei pazienti sul web (es. Google Documents, Dropbox, Skydrive, ecc.)?

Purtroppo no. Questi sistemi di archiviazione non sono un servizio acquisito o gestito dalla nostra azienda, la quale non ha pertanto modo di garantirne la rispondenza ai requisiti minimi. Inoltre, questi servizi, specialmente nella loro versione gratuita, prevedono una parziale cessione di diritti sul dato archiviato (ad esempio non sono vincolati alla riservatezza, quindi potenzialmente possono farne quello che vogliono, oltre che perderlo senza risponderne). Tale cessione di diritti sul dato a terzi non è consentita dalla normativa vigente.

10.2.5 Posso archiviare i dati personali dei miei pazienti su una chiavetta USB, CD, DVD?

Purtroppo no (anche se la chiavetta fosse aziendale). Il motivo principale è che, essendo dispositivi facilmente "perdibili" e comunque non sottoposti a limitazioni di accesso per chi dovesse per caso entrarne in possesso, non sono strumenti idonei alla archiviazione di dati personali.

10.2.6 Ho dei dati archiviati storicamente su formati ora non più a norma, come posso fare?

Contatta lo STIT. Imposteremo assieme un percorso di selezione dello strumento più idoneo e il recupero dei dati storici.

10.2.7 Devo iniziare una raccolta di dati relativi allo stato di salute, come posso fare?

Contatta lo STIT. Assieme verificheremo se esiste già un sistema informativo adeguato, e se non è disponibile valuteremo assieme l'acquisizione di un sistema specifico.

10.2.8 Voglio acquistare un sistema informativo per l'archiviazione… perché mi obbligate ad acquistare anche i servizi di assistenza del fornitore?

I requisiti minimi, come anche le linee guida, prevedono un coinvolgimento attivo del fornitore del sistema nella gestione del dato. Il suo ruolo è parte attiva specialmente nella garanzia di integrità del dato e continuità operativa del sistema. Lo STIT rende quindi obbligatoria la definizione di un contratto di assistenza per tutti i sistemi informativi dedicata all'archiviazione di dati relativi alla salute.

10.3 Domande Frequenti – Trasmissione Dati Personali e Relativi allo Stato di Salute

10.3.1 Posso inviare dati relativi allo stato di salute dei miei pazienti via posta elettronica?

Lo strumento "posta elettronica" che tutti conosciamo non risponde ai requisiti di sicurezza e riservatezza in quanto la trasmissione è "in chiaro" (non criptata), e pertanto potenzialmente intercettabile da malintenzionati.

È quindi tassativamente vietata la trasmissione di dati relativi allo stato di salute via posta elettronica verso indirizzi esterni all'azienda sanitaria, in quanto i dati, transitando su Internet, sono potenzialmente a rischio di intercettazione.

In nessun caso è consentito trasmettere dati relativi allo stato di salute originali (referti, consulenze, esiti di accertamenti strumentali in versione unica) via posta elettronica, in quanto la posta elettronica aziendale non è destinata ad una archiviazione a norma (ad esempio, in caso di contenzioso potrebbe non essere possibile recuperare l'email oggetto della trasmissione da verificare).

10.3.2 Posso condividere dati relativi allo stato di salute con colleghi attraverso piattaforme “social” web (es. facebook, twitter, google+, slideshare, ecc.)?

Purtroppo no. Questi sistemi di condivisione non sono un servizio acquisito o gestito dalla nostra azienda sanitaria, la quale non ha pertanto modo di garantire i requisiti minimi sulle modalità di trattamento del dato. Questi servizi, in quanto gratuiti, prevedono una parziale cessione di diritti sul dato e non offrono alcuna garanzia sulla sicurezza e riservatezza, riservandosi inoltre di variare arbitrariamente le politiche di condivisione, anche senza preavviso. La condivisione di dati su queste piattaforme, anche in forma anonima, non è consentita per due motivi: prevede la cessione di diritti sul dato, che non è nelle nostre facoltà, e può essere oggetto in futuro a variazioni improvvise e non controllabili delle politiche di condivisione.

È importante ricordare che il dato, anche in forma anonima, rimane di proprietà del paziente che ce lo ha “affidato” per l’archiviazione, pertanto non è nostro diritto trattarlo in modo non conforme, anche in forma anonima.

È importante inoltre prestare attenzione al fatto che molti dati in formato elettronico possono apparentemente sembrare “anonimizzati” in quanto non presentano esplicitamente dati anagrafici visibili, ma mantengono riferimenti nascosti all’identità anagrafica del paziente (es. le immagini radiologiche in formato DICOM).

Infine, segnaliamo che la trasmissione da e verso le piattaforme digitali “social” non è garantito che avvenga in forma criptata, quindi protetta da intercettazioni malevole o intercettazioni ad uso commerciale. Ad esempio, la piattaforma Facebook autorizza applicazioni di terze parti ad intercettare ed analizzare i dati caricati sul proprio profilo a scopo commerciale.

10.3.3 Se devo inviare dei dati personali e relativi allo stato di salute in formato elettronico ad un collega, come posso fare?

Normalmente se il collega fa parte della nostra azienda sanitaria ed ha diritto ad accedere a quel dato, lui stesso può consultare il dato per via elettronica senza che gli sia trasmesso. In questo caso è sufficiente trasmettere al collega le informazioni necessarie al recupero del dato di interesse. Ad esempio, se si vuole segnalare un particolare referto, è possibile navigare sul referto sul DataWareHouse clinico, e spedire al collega il collegamento ipertestuale (indirizzo della pagina).

È anche possibile richiedere spazi intranet tracciati e sicuri condivisi tra colleghi per la trasmissione e condivisione di documentazione non originale.

È inoltre possibile attivare sistemi di notifica automatica che, all’inserimento di dati sui sistemi informativi aziendali, notifichino ad un insieme di colleghi tale inserimento, consentendo loro di accedere per consultare il dato.

Per approfondimenti su questi strumenti di comunicazione, contattate lo STIT.

10.3.4 Come posso far arrivare i dati relativi allo stato di salute in formato elettronico al MMG/PLS?

La trasmissione delle informazioni cliniche dalle strutture sanitarie verso il MMG o PLS è stata oggetto di profonde innovazioni e regolamentazioni nell’ultimo decennio. La regione Emilia Romagna ha infatti istituito il circuito SOLE (Sanità On Line Emilia Romagna) che prevede la trasmissione automatica per via informatizzata al MMG di tutti i referti ambulatoriali, delle informazioni di accesso al PS, delle informazioni di ricovero e dimissione. Questa trasmissione di dati è regolata da complessi sistemi di verifica del consenso del paziente. È pertanto fondamentale non aggirare tali sistemi inviando autonomamente (spesso con strumenti impropri) dati in formato elettronico.

L'azienda rende disponibile strumenti di comunicazione a scopo puramente organizzativo e a copertura delle esigenze di condivisione con il MMG/PLS di documentazione sanitaria non compresa nella rete SOLE (quando regolamentata da precisa convenzione/progetto). Contattate lo STIT per approfondire l'uso di tali strumenti.

10.3.5 Come posso far arrivare i dati personali e relativi allo stato di salute in formato elettronico al paziente?

I referti trasmessi alla rete SOLE sono anche automaticamente resi disponibili per l'assistito sul Fascicolo Sanitario Elettronico. Tale strumento è in corso di estensione a livello nazionale, e sarà quindi possibile raggiungere anche gli assistiti fuori regione.

L'azienda rende disponibile strumenti di comunicazione a scopo puramente organizzativo e a copertura delle esigenze di condivisione con il paziente di documentazione sanitaria non compresa nella rete SOLE (quando regolamentata da precisa convenzione/progetto). Contattate lo STIT per approfondire l'uso di tali strumenti.

10.3.6 Come può un paziente trasmettermi documentazione sanitaria elettronica?

L'azienda rende disponibile un sistema denominato "Portale Caricamento Documentazione Sanitaria" che consente ai nostri professionisti di predisporre degli spazi condivisi con i nostri pazienti, su cui possono caricare la loro documentazione sanitaria in modo sicuro. Tale caricamento viene notificato all'equipe sanitaria che lo ha in carico, consentendo una rapida consultazione della documentazione caricata.

In specifici contesti (assenza di accesso al Fascicolo Sanitario Elettronico) questo canale di comunicazione può essere reso bidirezionale, consentendo al nostro professionista di trasmettere documentazione in modo sicuro al paziente.

Per approfondimenti su questi strumenti di comunicazione, contattate lo STIT.

10.3.7 Posso archiviare e inviare i dati relativi alla salute ad un ente terzo a scopo di ricerca o valutazione epidemiologica?

L'archiviazione e invio di dati esternamente all'azienda sanitaria può essere autorizzato solo da specifico consenso del paziente, relativo a specifici progetti e a seguito di approvazione da parte del Comitato Etico. In alcuni casi l'invio può essere previsto nell'ambito progetti regionali che traggono la loro autorizzazione a livello istituzionale (es. flussi epidemiologici regionali).

In tutti i casi è fondamentale che gli strumenti di trasmissione del dato siano preventivamente verificati ed autorizzati dallo STIT, che ne determina la conformità ai requisiti adeguati, in particolare quelli di sicurezza e riservatezza.

10.4 Domande Frequenti – Acquisizione di Nuovi Software

10.4.1 Ho bisogno di un nuovo software… cosa devo fare?

Contatta per tempo lo STIT. Insieme a loro analizzerai i tuoi requisiti, e valuterete se esiste già in azienda un software adeguato. Se non esiste, valuterete assieme cosa è disponibile sul mercato, se è necessario fare una gara, e gli importi coinvolti per l'acquisto e servizi di assistenza. Con queste informazioni potrete poi richiedere l'autorizzazione all'acquisto alle direzioni in sede di discussione di budget.

10.4.2 Conosco già produttore, modello e versione del software che voglio acquistare… come fare?

Purtroppo non è così facile… se il software è "unico" per sue caratteristiche, allora è possibile un acquisto diretto. Se invece sul mercato esistono altri software con caratteristiche simili è probabilmente necessario procedere con una gara. Contatta lo STIT per valutare assieme il caso specifico.

10.4.3 Ma perché lo devo comprare, non possiamo farcelo noi internamente?

Lo STIT gestisce un parco di oltre 290 sistemi informativi diversi. È pertanto impensabile gestire una complessità simile con sole risorse interne. È quindi rarissimo che lo STIT si occupi di sviluppare internamente software. Normalmente ci si orienta verso l'acquisto di software commerciali già esistenti. Qualora le esigenze fossero così particolari da non trovare risposte sul mercato (o da avere solo risposte in sistemi eccessivamente costosi), lo STIT può coordinare attività di sviluppo di software ad-hoc da parte di fornitori esterni. Anche in tal caso si applicano gli iter di acquisizione sopra descritti.

10.4.4 Ho un amico/parente che mi fa il software gratuitamente… come fare?

Anche se l'amico/parente volesse donare il software, è comunque necessario che siano disponibili (donati anch'essi) servizi di assistenza. Tali servizi devono essere regolati da un contratto che preveda vincoli per il fornitore (livelli di servizio). Questo rende di fatto difficile accettare donazioni di questo tipo in quanto raramente alla donazione si accompagna una formalizzazione dei servizi di assistenza. Non è consentita l'installazione o l'uso di sistemi software non coperti da servizio di assistenza.

10.4.5 Una Azienda Farmaceutica o Associazione mi vuole donare il software… come fare?

Di solito questi "omaggi" non prevedono servizi di assistenza. Qualora fossero previsti, raramente sono offerti gratuitamente. Diventa pertanto necessario acquisire, con lo stesso iter sopra descritto, i servizi di assistenza e manutenzione necessari. Non è consentita l'installazione o l'uso di sistemi software non coperti da servizio di assistenza.

10.5 Domande Frequenti – Acquisizione di Hardware

10.5.1 Ho bisogno di hardware, e in discussione di budget non era ancora previsto… devo aspettare il budget del prossimo anno (o biennio)?

Non necessariamente. Se l'esigenza è conseguenza di variazioni non prevedibili della vostra attività (es. attivazione di un nuovo ambulatorio, arrivo di nuovi borsisti o tirocinanti, ecc.), potete fare richiesta di nuovo hardware, e il caso sarà portato all'attenzione della direzione senza attendere la discussione di budget.

10.5.2 Una Azienda Farmaceutica o Associazione mi vuole donare dell'hardware… come fare?

Non ci sono problemi. Contattate lo STIT e fornite i riferimenti del donatore. Saremo noi a contattarlo per seguire l'iter. Se la donazione prevede un acquisto di hardware da noi indicato, indirizzeremo il donatore verso gli standard aziendali (vedi discorso sui costi indotti fatto in sezione precedente). Se invece il donatore ha già acquistato l'hardware, i nostri tecnici provvederanno a valutarne la compatibilità con i sistemi aziendali, e qualora non emergessero problemi, provvederanno a seguire l'iter di donazione, e conseguentemente configurarlo per un inserimento nella rete aziendale.

10.5.3 Non c'è bisogno di comprare nuovo hardware, posso usare il mio portatile personale! È OK?

Le garanzie di sicurezza da virus informatici e da accessi impropri che per normativa l'azienda deve garantire rendono attualmente difficile l'autorizzazione alla connessione di dispositivi personali alla rete aziendale. Questi, infatti, non essendo controllati dallo STIT, potrebbero potenzialmente essere vettori di infezione o di accessi abusivi. Conseguentemente non è al momento consentito l'uso di dispositivi personali per l'accesso alla rete aziendale (e conseguentemente ai dati aziendali).

10.6 Domande Frequenti – Accesso al Dato

10.6.1 Ho bisogno di estrarre dei dati da alcuni sistemi informativi, come posso fare?

1. Chiedi l'autorizzazione a tutti i direttori delle unità operative di pertinenza del dato (es. laboratorio, anatomia patologica, oncologia, ecc.).
2. Se intendi pubblicare i risultati delle elaborazioni che farai sui dati, contatta il Comitato Etico. Saranno loro a dirti se è necessaria la presentazione di un progetto formale, o se le elaborazioni sono in forma sufficientemente aggregata ed anonima da non richiedere un progetto formale.
3. Dopo aver avuto l'OK del Comitato Etico (su un progetto formale o sulla non necessità di tale progetto), contatta lo STIT per fissare un appuntamento. Valuteremo assieme come impostare l'estrazione. Ti sarà fornita una data programmata per l'estrazione e per tale data, se non ci sono problemi, ti saranno trasmessi i dati.

10.6.2 Voglio estrarre dei dati dal sistema informativo del mio reparto, che uso tutti i giorni… devo avere una autorizzazione?

Se si richiede una estrazione massiva, sì. La destinazione d'uso del sistema è relativa al solo scopo di cura del paziente. Le estrazioni massive esulano normalmente da tale scopo. Comunque, se l'estrazione non ha scopo di ricerca, è sufficiente l'autorizzazione del direttore.

10.6.3 Io non ho la minima idea di dove e come siano archiviati i dati che mi servono… come posso fare?

Contattate lo STIT. Saremo felici di guidarvi tra le possibili sorgenti per i dati di vostro interesse, e aiutarvi nell'impostare l'iter corretto di autorizzare all'accesso a tali dati.

10.6.4 Posso chiedere i dati direttamente al fornitore del sistema informativo?

No, l'accesso ai dati deve essere autorizzato e tracciato dalla nostra azienda, e non dal fornitore del sistema. Il fornitore non dovrebbe prestarsi a operazioni di questo tipo. Se lo fa (per mancata conoscenza delle procedure) siete comunque voi a dover seguire preventivamente tutto l'iter di richiesta allo STIT.

10.6.5 Devo fare una estrazione periodica… devo fare richiesta tutte le volte?

No, se lo segnali allo STIT la prima volta, ti renderemo disponibile uno strumento con cui potrai autonomamente eseguire la stessa estrazione le volte successive, in modo tracciato e sicuro.