Deliberazione n° _____ del _____

ESECUTIVITA'

La presente deliberazione è esecutiva a tutti gli effetti di legge a decorrere dalla data _____

Il Responsabile

_____

TRASMISSIONE

- [x] Collegio Sindacale
- [ ] UOC Segreteria Generale
- [ ] Direzione Sanitaria
- [ ] UOC Controllo di Gestione e Flussi Informativi
- [x] UOC Gestione Sistemi Informatici
- [ ] UOC Marketing Sanitario e U.R.P.
- [ ] UOC Appropriatezza ed Epidemiologia Clinica e Valutativa
- [ ] Serv. Prevenzione e Protezione e Serv. Antincendio
- [ ] UOC Affari Generali e Patrimonio
- [ ] UOC Affari Legali, Appalti e Contratti
- [ ] UOC Approvvigionamento Beni e Servizi
- [ ] UOC Gestione Risorse Economico Finanziarie
- [ ] UOC G.R.U. – Trattamento economico
- [ ] UOC Gest. Attività Tecniche e Ingegneria Clinica
- [ ] UOC Farmacia
- [ ] Comitato Etico Ospedaliero
- [ ] UOC Programmazione e Pianificazione Sanitaria

ASSESSORATO ALLA SANITA'

La presente deliberazione è stata trasmessa alla Struttura di Controllo della G.R.C. ai sensi dell'art. 35 - comma 3 - della L.R. n. 32 del 3/11/94, con nota n._____

in data _____

Il Funzionario

_____

REGIONE CAMPANIA

AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE
"A. CARDARELLI"
Via A. Cardarelli, 9 / 80131 - Napoli

Il Responsabile del Servizio, a seguito di istruttoria, dichiara la regolarità giuridico-amministrativa del provvedimento proposto.

Gaetano Adinolfo
(timbro e firma)

RELATA DI PUBBLICAZIONE

Copia della presente deliberazione è stata affissa all'Albo dell'Azienda dal giorno 26 APR 2019 e vi resterà per gg. 15 consecutivi.

Il Funzionario

DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO

N. 412 del 26 APR 2019

U.O.C. GESTIONE SISTEMI INFORMATICI

Oggetto: **Approvazione regolamento per l'utilizzo delle risorse informatiche.**

Il presente provvedimento è reso immediatamente esecutivo per l'urgenza.

Il Commissario Straordinario
(avv. Anna Iervolino)

_____

Si rende esecutivo

Napoli, _____

Il Funzionario

_____

Segreteria di Direzione

Oggetto: **Approvazione regolamento per l'utilizzo delle risorse informatiche.**

L'Ing. Gaetano Mirto, in qualità di Direttore della U.O.C. Gestione Sistemi Informativi, nominato, da ultimo, con deliberazione n. 483 del 23 Aprile 2018, nell'ambito del Regolamento delle autonomie, competenze e funzioni;

PREMESSO
- che risulta sempre più intenso l'utilizzo di risorse informatiche sia per lo svolgimento delle attività sanitarie che per lo svolgimento delle attività amministrativo contabili;
- che questo rilevante impiego richiede che l'utilizzo delle citate risorse avvenga in maniera legittima e nel rispetto della normativa che ne disciplina l'uso al fine di garantire la sicurezza dei dati gestiti e la sicurezza degli stessi sistemi di gestione;

RILEVATO
- che con l'entrata in vigore delle nuove Misure minime di sicurezza ICT per le pubbliche amministrazioni emanate da AGID e la contemporanea entrata a regime del Regolamento Generale sulla Protezione dei Dati (GDPR) l'A.O.R.N. A. Cardarelli ha avviato un percorso di aggiornamento e rafforzamento delle proprie politiche di sicurezza informatica, al fine di garantire l'integrità e la disponibilità dei dati trattati;
- che al fine di rafforzare la sicurezza è necessario che tutti i soggetti che a vario utilizzano le risorse informatiche (dipendenti, collaboratori, fornitori, etc.) si conformino a regole di comportamento ed utilizzo degli strumenti informatici che non determinino un potenziale rischio per la sicurezza dei dati trattati;
- che a tale scopo l'U.O.C. GSI ha predisposto l'allegata proposta di "Regolamento aziendale per l'utilizzo delle risorse informatiche" al fine di precisare le regole a cui i dipendenti devono ottemperare quando li utilizzano e definire le relative responsabilità;

CONSIDERATO
- che l'adozione del suddetto Regolamento potrà fornire l'opportunità di garantire la sicurezza del sistema informatico dell'Azienda e di conseguenza una gestione sicura dei dati trattati;

VISTI
- Decreto Legislativo 30 giugno 2003, n.196, "Codice in materia di protezione dei dati personali", e successive modificazioni e integrazioni (G.D.P.R., 2016/679 e D.lgs 101/2018);
- Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali";
- Legge 23 dicembre 1993 n. 547- "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica";
- Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri-Dipartimento della funzione pubblica: "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro" e Deliberazione 1 Marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet";
- Deliberazione 1 Marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet";
- Circolare AgID n° 1/2017.

Tutto ciò premesso, argomentato ed attestato, il sottoscritto Ing. Gaetano Mirto, Direttore della UOC Gestione Sistemi Informativi, dichiarata la conformità alle leggi, regolamenti e C.C.N.L. del presente provvedimento,

PROPONE AL COMMISSARIO STRAORDINARIO

Per tutti i motivi di cui in premessa che si intendono integralmente riportati di adottare il presente provvedimento, e nello specifico:

1. di approvare l'adozione del "Regolamento aziendale per l'utilizzo delle risorse informatiche" in conformità al

testo allegato alla presente deliberazione e darne massima diffusione a tutti gli utilizzatori delle postazioni informatiche e della rete informatica aziendale;
2. di stabilire che il seguente atto costituisca parte integrante della presente deliberazione:
   a. copia del "Regolamento aziendale per l'utilizzo delle risorse informatiche" (composto da n. 30 pagine);
3. Disporre la trasmissione del presente provvedimento al Collegio Sindacale;
4. Garantire le previste forme di registrazione e pubblicità dell'atto secondo legge

Il Direttore UOC GSI
Ing. Gaetano Mirto

AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE A. CARDARELLI NAPOLI FUNZIONE TECNICA

L'anno duemiladiciannove il giorno ..... del mese di ..... nella sede dell'Azienda Ospedaliera " A. Cardarelli " di Napoli

Con il parere del Direttore Sanitario

IL COMMISSARIO STRAORDINARIO

Avv. Anna Iervolino, nominata con D.G.R.C. n. 150 del 10.04.2019, alla stregua dell'istruttoria espletata dalla U.O.C. Gestione Sistemi Informativi, e letta la su esposta proposta:

DELIBERA

Per tutti i motivi di cui in premessa, che si intendono integralmente riportati, di adottare il presente provvedimento, sulla scorta ed in conformità della proposta e, nello specifico:

1) di approvare l'adozione del "Regolamento aziendale per l'utilizzo delle risorse informatiche" in conformità al testo allegato alla presente deliberazione;
2) di stabilire che il seguente atto costituisca parte integrante della presente deliberazione:
   a. copia del "Regolamento aziendale per l'utilizzo delle risorse informatiche" (composto da n. 30 pagine);
3) Disporre la trasmissione del presente provvedimento al Collegio Sindacale;
4) Garantire le previste forme di registrazione e pubblicità dell'atto secondo legge

IL DIRETTORE SANITARIO
Dott. Franco Paradiso

IL COMMISSARIO STRAORDINARIO
avv. Anna Iervolino

REGOLAMENTO AZIENDALE
PER L'UTILIZZO DELLE RISORSE INFORMATICHE
dell'A.O.R.N. A. CARDARELLI

v.1.0

Firmato digitalmente da:Gaetano Mirto
Ruolo:Ingegnere
Organizzazione:ORDINE DEGLI INGEGNERI DI BOLOGNA/00902120377
Data:17/04/2019 10:18:47

Sommario

1. Normativa di riferimento 1
1.1. Principali riferimenti normativi 1
1.2. Violazioni della normativa 1
2. Le principali definizioni 2
3. Premessa 4
4. Oggetto e campo di applicazione 4
5. I principali indirizzi 4
6. I principali divieti 4
7 Responsabilità 5
7.1. Procedure informatizzate autorizzate 5
7.2. Procedure informatizzate non gestite dal SIA 5
8.1. Credenziali di autenticazione (coppia username e password) 5
8.2. Rilascio e rinnovo delle credenziali 6
8.3. Gestione delle credenziali 6
8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dal SIA 7
9. Norme generali per l'utilizzo delle apparecchiature informatiche 8
9.1. Computer aziendali 8
9.2. Computer portatili e aziendali 9
9.3. Utilizzo di attrezzature informatiche personali 9
9.4. Stampanti e scanner 9
9.5. Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive 10
9.6. Norme generali per l'utilizzo del software distribuito dal SIA 11
9.7. Software antivirus e di protezione dei dati 11
9.8. Dischi di rete, cartelle personali e cartelle condivise 11
9.9. Presentazioni 12
10. Collegamento di attrezzature alla rete dati 12
10.1 Rete AORN 12
10.2. Altre reti wi-fi in Azienda 13
11. Utilizzo in Azienda di dispositivi di telecomunicazione radiomobili o wireless 13
12. Uso e salvataggio dei dati aziendali 13
13. Norme generali per l'utilizzo dei servizi Internet 13
13.1. Posta elettronica e navigazione Internet 13
13.2. Pubblicazione di contenuti e realizzazione di siti personali 13
13.3. Connessione a provider diversi da quello aziendale 14

13.4.Utilizzo dell'ambiente cloud aziendale per la condivisione temporanea di documenti 14
13.5.Utilizzo di server esterni per backup/gestione/condivisione documenti aziendali 14
13.6. Assistenza da remoto (VPN e altre tipologie) 14
14. Modalità di prestazione dei servizi 15
15. Acquisto su progetti finanziati (PO) 15
16. Installazione di Microsoft Office sulle postazioni di lavoro 15
17. Disposizioni finali 15
17.1. Cessazione della disponibilità dei servizi informatici aziendali 15
17.2. Responsabilità dell'utilizzatore delle risorse informatiche 16
17.3. Informativa sul trattamento dei dati da parte del SIA 16
17.4. Disposizioni transitorie 17
Allegato A – Elenco applicativi di base e specifici autorizzati 18
Allegato B – Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente 23
Allegato C – Raccomandazioni per l'utilizzo in azienda di dispositivi di telecomunicazione radiomobili o wireless 24
1. Definizioni 24
2. Premessa 25
3. Scopo del documento 25
4. Dispositivi oggetto di regolamentazione 25
5 Classificazione 26
6. Metodologia di lavoro e documentazione 26
7. Raccomandazioni 27
Allegato D – Raccomandazioni per l'utilizzo in azienda di software medicali e per la connessione delle tecnologie biomediche alla rete dati aziendale 28
1. Definizioni 28
2. Premessa 29
3. Scopo del documento 29
4. Dispositivi oggetto di regolamentazione 29
5 Utilizzo rete dati aziendale 29
5.1 Acquisto e/o installazione di SDM e tecnologie biomediche connesse a rete 29
5.2 Installazione nuovi punti rete 30
5.3 Dispositivi e/o access point 30
5.4 Accesso da Remoto (VPN) 30
6. Conclusioni 30

1. Normativa di riferimento

1.1. Principali riferimenti normativi

- Decreto Legislativo 30 giugno 2003, n.196, "Codice in materia di protezione dei dati personali", e successive modificazioni e integrazioni (G.D.P.R., 2016/679 e D.lgs 101/2018)
- Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali"
- Legge 23 dicembre 1993 n. 547- "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".
- Direttiva n. 2/2009 della Presidenza del Consiglio dei Ministri-Dipartimento della funzione pubblica: "Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro" e Deliberazione 1 Marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet"
- Deliberazione 1 Marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet"
- Circolare AgID n° 1/2017.

1.2. Violazioni della normativa

La normativa di riferimento prevede in caso di violazione sanzioni penali e amministrative.

A titolo di esempio, si elencano di seguito alcune figure di reato previste dal Codice Penale:

- Attentato a impianti informatici di pubblica utilità (art. 420);
- Falsificazione di documenti informatici (art. 491bis);
- Accesso abusivo ad un sistema informativo o telematico (art. 615ter);
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615quater);
- Diffusione di programmi diretti a danneggiare o interrompere un Sistema informativo (art. 615quinquies);
- Violazione di corrispondenza telematica (artt. 616-617sexies);
- Intercettazione di e-mail (art. 617quater);
- Danneggiamento di sistemi informatici e telematici (art. 635bis);
- Frode informatica (alterazione dell'integrità di dati allo scopo di procurarsi un ingiusto profitto) (art. 640ter).

Le seguenti figure di reato sono invece previste dal Codice Privacy (Oggi G.D.P.R.):

- Trattamento illecito di dati (art. 167)
- Falsità nelle dichiarazioni e notificazioni al Garante (art. 168)
- Mancata adozione delle misure di sicurezza (art. 169)
- Inosservanza di provvedimenti del Garante (art. 170)

2. Le principali definizioni

Risorse Informatiche

Qualsiasi mezzo di comunicazione e elaborazione elettronica, hardware, software, rete, servizio e informazione in formato elettronico di proprietà dell'Azienda o in disponibilità o a essa concesso in licenza d'uso.

Le risorse informatiche includono a titolo di esempio:

- sistemi informatici a uso sanitario, amministrativo o tecnico (es. posta elettronica, accesso a Internet, applicativi aziendali quali: Cartella Clinica Informatizzata, Gestione Protocollo Easy Doc, Delibere e Determine, Elyot, GOP, etc.;
- ogni sistema di elaborazione elettronica delle informazioni: server, personal computer fissi o portatili, tablet e similari;
- software di base e di ambiente: sistemi operativi, software di rete, sistemi per il controllo degli accessi, package, utility e similari;
- software di produttività individuale (Office, LibreOffice, OpenOffice, Project, Visio ecc.);
- ogni informazione elettronica registrata o conservata in file e banche dati;
- ogni periferica: stampanti, scanner, plotter, apparecchiature per l'archiviazione elettronica dei dati, supporti di memorizzazione, video terminali;
- ogni dispositivo di rete: concentratori, ripetitori, modem, switch, router, gateway, firewall, apparati VoIP e similari, access point, chiavette Internet;
- ogni mezzo trasmissivo di cablaggio strutturato per reti locali, metropolitane e geografiche: cavi in fibra e in rame per dorsali e cablaggio orizzontale, permutazioni, attestazioni, patch e similari.

Utilizzatori

Persone fisiche dipendenti o collaboratori a vario titolo, frequentatori, universitari che hanno accesso a strumenti informatici o telematici e che sono nella potenzialità di utilizzarli.

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

L'interessato è la persona fisica cui si riferiscono i dati personali.

In merito al tipo di dati si distinguono:

- Dato personale:
  Qualunque informazione relativa a persona fisica, "interessato" identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi dato suo interesse, in particolare a quelli "sensibili", ivi compreso un numero di identificazione personale.
- Dato sensibile:
  Ogni dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
- Dato anonimo:
  I dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

In merito ai soggetti che possono effettuare operazioni di trattamento si distinguono:

- Titolare:

A.O.R.N. A. CARDARELLI, Via A. Cardarelli, n. 9 – 80131 Napoli

- Responsabile:
  La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal titolare, con atto formale di nomina, al trattamento di dati personali, sulla base di istruzioni impartite per iscritto dal titolare stesso.
  Tipicamente sono le Società esterne quando formalmente nominati dal Titolare del Trattamento attraverso contratto che disciplina i dati da trattare e le modalità di trattamento
- Delegato di funzione: Sono i dipendenti con ruoli dirigenziali che su esplicita delega del titolare del trattamento. devono garantire quanto necessario per un adeguato indirizzo e vigilanza sulle Strutture organizzative e sui soggetti che a qualsiasi titolo vi operano, anche per attività esterne, in attuazione del GDPR UE/2016/679, del D.Lgs. 101/2018 e delle norme, richiamati in premessa e delle specifiche istruzioni fornite dal " Titolare del Trattamento" attraverso le linee guida adottate in Azienda
- Incaricato:
  La persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.
  Tipicamente tutti i soggetti (dipendenti, personale esterno autorizzato (tirocinanti, allievi di Corsi di Laurea, Specializzandi, etc) che rispondono anche al Delegato di Funzione della struttura
  La persona fisica nominata dal Responsabile del Trattamento, dipendente di una Società esterna, autorizzata a compiere operazioni di trattamento per conto dell'AO Cardarelli, ad esempio gli operatori dei sistemi informatici o manutentori di software e/o di apparecchiature medico/scientifiche

Comunicazione

Il dare conoscenza dei dati personali a uno o più soggetti determinati, diversi dall'interessato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Per soggetti determinati si intendono solo i soggetti precisamente identificati e appartenenti a un elenco finito.

Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Per soggetti indeterminati si intendono soggetti non identificabili a priori.

Banca di dati

Qualsiasi complesso di dati ripartito in una o più unità dislocate in uno o più siti.

Misure minime di sicurezza

I complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, ai sensi del GDPR 679/2016 art 32 che configurano il livello minimo di protezione richiesto per la sicurezza dei dati, garantendo :la **pseudonimizzazione, la cifratura, l'adeguamento ai concetti di resilienza** e di **disaster recovery** dei sistemi e dei servizi informatici che trattano i dati personali.
Integrato dalla Circolare AgID n° 1/2017 che si riferisce alle misure di sicurezza della P.A..

Credenziali di autenticazione

I dati e i dispositivi, in possesso di una persona, da questa conosciuti o a essa univocamente correlati, utilizzati per l'autenticazione informatica, ovvero il processo che garantisce l'accesso a un sistema informatico.
La parola chiave (password) è la componente di una credenziale di autenticazione associata a una persona e solo a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica, da mantenere riservata.

3. Premessa

Il presente documento, redatto a cura del servizio Sistema Informativo Aziendale (di seguito SIA), regolamenta l'accesso e l'uso delle risorse informatiche dell'A.O.R.N. A. Cardarelli (nel seguito AORN), secondo i principi e le disposizioni della normativa citata in premessa e le indicazioni in materia di corretto uso delle risorse informatiche secondo le politiche e disposizioni aziendali definite in accordo con la direzione aziendale.

I servizi informatici aziendali sono regolamentati, oltre che dal presente documento, dal Regolamento per l'utilizzo della Posta Elettronica e Internet. Per le misure in materia di protezione dei dati personali, ma non esclusivamente relative al trattamento di dati con supporto informatico, si rinvia ad altra documentazione aziendale specifica.

Il SIA si impegna ad adeguare questo regolamento in funzione di eventuali mutamenti legislativi o in ragione di particolari necessità tecniche. L'ultima versione del regolamento sarà sempre consultabile sul sito intranet aziendale.

4. Oggetto e campo di applicazione

Le regole stabilite si riferiscono a tutte le risorse informatiche dell'Azienda, devono essere applicate da tutti i soggetti che le utilizzano e hanno valenza per tutte le tipologie di dati.

Gli utenti, dipendenti dell'AORN e i collaboratori esterni autorizzati, sono individuati, ai sensi del Dlgs 101/2018, quali "incaricati del trattamento dei dati personali, conservati in formato elettronico", se, autorizzati all'accesso previo registrazione ai servizi informativo/informatici aziendali.

Pertanto i dati possono essere trattati limitatamente alle operazioni indispensabili per l'esercizio delle funzioni degli incaricati.

Gli utenti a vario titolo autorizzati devono attenersi alle disposizioni del presente regolamento.

Oltre a quanto definito in questo documento si precisa che:

- per le risorse informatiche messe a disposizione o date in uso all'azienda da altre organizzazioni valgono gli accordi e le condizioni contrattuali stipulate fra le parti;
- per l'utilizzo di dati, programmi e materiali valgono sempre le condizioni di copyright, ove previsto;
- l'utilizzo delle risorse informatiche dell'azienda deve essere comunque conforme a quanto previsto dalla normativa vigente.

5. I principali indirizzi

Le risorse informatiche:

- sono parte integrante del patrimonio dell'AORN;
- devono essere utilizzate per gestire le attività aziendali, secondo le finalità autorizzate e definite dalla direzione aziendale e inerenti alla propria mansione, nel rispetto dei principi di necessità, indispensabilità, non eccedenza;
- devono essere rese disponibili solo alle persone autorizzate;
- devono essere protette da danneggiamenti, furti e cause diverse che possano compromettere le attività aziendali.

6. I principali divieti

- Introdursi abusivamente nei sistemi informatici aziendali.
- Procurare a sé, o ad altri, profitto, o arrecare danni all'azienda, procurandosi, riproducendo, diffondendo, o consegnando codici, parole chiave o altri mezzi idonei all'accesso ai sistemi informatici.

- Riprodurre, duplicare e/o asportare, comunicare a terzi, diffondere i dati di cui l'azienda è titolare del trattamento.
- Riprodurre e asportare documentazione di qualsiasi tipo classificata riservata, compresi progetti, schede, prospetti se non dietro esplicita autorizzazione del titolare dei relativi diritti (o di persona delegata).
- Intercettare, impedire, interrompere le comunicazioni inerenti ai sistemi informatici.
- Distruggere, deteriorare, rendere inservibili, del tutto o in parte, i sistemi informatici ovvero i programmi e le informazioni o i dati esistenti nei sistemi.
- Riprodurre, duplicare e/o asportare programmi installati di cui l'azienda è licenziataria o proprietaria.
- Introdurre, installare, utilizzare programmi e/o apparati (Firefox, Masterizzazione, Access Point, Hub, Switch, ecc...) che non siano stati regolarmente acquistati, distribuiti e installati dalle preposte funzioni aziendali.
- Adottare comportamenti che mettano a rischio la sicurezza del sistema informatico/informativo, inclusi i dati contenuti, o che pregiudichino o ostacolino le attività della collettività degli utilizzatori.

7 Responsabilità

7.1. Procedure informatizzate autorizzate

Le procedure informatiche distribuite e gestite dal SIA sono tutte e sole quelle individuate nell'allegato A - Elenco dei trattamenti di dati personali.

Tale allegato sarà costantemente aggiornato dal SIA e sempre disponibile in Intranet.

Relativamente a tali procedure, sono a carico del SIA le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, per quanto riguarda i server, i software di base, le procedure applicative, le infrastrutture, i dispositivi della rete aziendale, ovvero tutto quanto riguarda la sicurezza e protezione dei dati trattati.

Sono invece a carico degli utilizzatori (responsabili del trattamento e incaricati, ciascuno per i rispettivi ambiti di competenza e responsabilità) le misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, per quanto riguarda le postazioni di lavoro (Personal Computer) e le attività svolte con esse.

7.2. Procedure informatizzate non gestite dal SIA

Fermo restando il divieto di utilizzare programmi non autorizzati, se per qualsiasi ragione, in particolare la necessità di garantire la continuità operativa, dovessero essere in uso presso le Unità Operative procedure informatizzate NON distribuite dal SIA, fintanto che esse rimangono operative l'organizzazione e la gestione delle misure di sicurezza, e più in generale il rispetto della normativa e delle disposizioni aziendali, sono a carico del singolo responsabile del trattamento, se non richiede l'intervento del SIA per verificarne la corretta applicazione.

8. Sistemi di autenticazione e di autorizzazione

Il responsabile del trattamento, individuati gli incaricati, dovrà richiedere l'attivazione della credenziale di autenticazione informatica, specificando a quali dati e tipi di operazioni può accedere in relazione ai compiti impartiti.
Il trattamento di dati personali, con strumenti elettronici, è consentito infatti ai soli incaricati dotati di credenziali di autenticazione, in genere costituite da Nome Utente (username) e password.

8.1. Credenziali di autenticazione (coppia username e password)

Le credenziali di autenticazione sono il presupposto necessario per l'utilizzo dei sistemi informatici messi a disposizione dall'AORN.

Le credenziali consentono il superamento di una procedura d'autenticazione che permette l'accesso a uno specifico trattamento o a un insieme di trattamenti.

8.2. Rilascio e rinnovo delle credenziali

Tutte le informazioni relative alle modalità di rilascio e di rinnovo delle credenziali sono riportante nell'Allegato B - Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente.

8.3. Gestione delle credenziali

Le credenziali possono consistere:

- in un codice per l'identificazione dell'incaricato, associato ad una parola chiave riservata conosciuta solamente dal medesimo (**username e password**),

Lo ***username,*** o nome utente, è di norma costituito dalla matricola dell'utilizzatore

Lo stesso username non potrà, neppure in tempi diversi, essere assegnato a incaricati diversi.

La ***password*** (o parola chiave) è una parola segreta, conosciuta solo dall'incaricato che, in coppia con lo username, permette di accedere alla procedura informatizzata scelta dal dipendente e deve essere cambiata, per motivi di sicurezza, ogni sessanta giorni (con altra diversa da quella precedente).

La password è strettamente personale e per nessun motivo deve essere resa nota a altri. La sua conoscenza da parte di estranei consentirebbe il trattamento dei dati per nome e per conto del possessore delle credenziali. Infatti, l'eventuale uso improprio di apparecchiature, strumenti o servizi sarà imputato al titolare della password con la quale è avvenuto l'accesso.

A ogni incaricato sono assegnate individualmente una o più credenziali per l'autenticazione.

L'assegnatario dovrà farne un uso strettamente personale (quindi non condivisibile con altri), operare nell'ambito delle autorizzazioni ricevute e utilizzare le risorse solo per scopi aziendali.

Ogni incaricato è tenuto ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (password), e la diligente custodia dei dispositivi in suo possesso o a suo uso esclusivo.

Le credenziali potranno essere disattivate nel caso di non utilizzo per oltre 6 mesi.

Le credenziali vengono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Sono esplicitamente vietate credenziali di accesso anonime, ovvero non corrispondenti a una persona fisica.

La scelta sicura della password si realizza attraverso le seguenti regole di buon senso:

- Deve essere facilmente memorizzabile in modo tale che si possa evitare di scriverla (per es. sulla postazione di lavoro o in prossimità), ma non banale e di facile individuazione (per es. con riferimenti chiari all'incaricato).
- La sua lunghezza deve essere di almeno otto caratteri e deve contenere almeno un numero e una lettera maiuscola (il sistema non consentirà di agire diversamente)[1].
- Non deve contenere nome o cognome della persona.
- Deve essere modificata al primo utilizzo e successivamente ogni due mesi (per dati sensibili e/o giudiziari) o sei mesi secondo i casi (le regole saranno preimpostate nei sistemi gestionali).

[1] Solo nel caso in cui, per es. per obsolescenza, lo strumento elettronico non consenta una password lunga 8 caratteri, questa deve avere lunghezza pari al numero di caratteri massimo consentito

- Deve essere modificata ogni volta che si abbia la sensazione che possa essere conosciuta, intenzionalmente o accidentalmente, da altri.
- In caso di modifica, la nuova password non deve essere uguale a una password già usata in precedenza.

8.4. Sistema d'autorizzazione per le procedure informatizzate distribuite dal SIA

L'assegnazione di credenziali di autenticazione del tipo "nome.cognome" abilita l'assegnatario a una serie di "servizi informatici di base" quali:

- accesso a una casella di posta elettronica;

L'assegnazione di credenziali di autenticazione del tipo "matricola" abilita l'assegnatario a una serie di "servizi informatici di base" quali a esempio:

- visualizzazione del GOP;
- accesso a Internet;
- accesso a una cartella di rete personale (se richiesta);
- accesso potenziale a gran parte degli applicatici aziendali (richiede separata autorizzazione).

L'abilitazione all'uso dei servizi informatici di base può essere richiesta al SIA direttamente dall'interessato.

Per l'abilitazione all'accesso a servizi informatici e procedure non comprese nei servizi di base, la relativa autorizzazione dovrà essere richiesta dal responsabile della struttura organizzativa di appartenenza.

È dovere del responsabile di una struttura organizzativa, firmatario della suddetta modulistica, dare immediata comunicazione al SIA circa la modifica o revoca di funzioni che avevano giustificato l'accesso da parte di un proprio collaboratore a procedure/banche dati/servizi.

La richiesta di una nuova attivazione deve pervenire con almeno **15 giorni** d'anticipo rispetto alla data di attivazione del codice identificativo.

La richiesta di modifica o disattivazione di un profilo deve pervenire con almeno **10 giorni** d'anticipo rispetto alla data di variazione.

La maggior parte dei servizi e procedure informatiche distribuite dal SIA prevedono differenti profili di autorizzazione: tali profili, definibili per ciascun incaricato o per classi omogenee d'incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, il responsabile del trattamento deve verificare la sussistenza delle condizioni per la conservazione dei profili d'autorizzazione attribuiti ai singoli incaricati.

Dopo un limitato numero di tentativi d'accesso falliti, alcuni sistemi di sicurezza disattivano lo username, che sarà riattivabile solo a seguito di richiesta scritta del singolo incaricato del trattamento.

Nel caso di prolungata assenza o impedimento di un incaricato le cui credenziali consentano in modo esclusivo l'accesso ad alcuni dati o strumenti elettronici, tale da rendere indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'incaricato potrà individuare per iscritto un altro lavoratore (fiduciario) a cui affidare il compito dell'accesso in sua vece, o, alternativamente, il Responsabile del trattamento potrà richiedere per iscritto al SIA di autorizzare un altro incaricato all'accesso ai dati o strumenti interessati. Tale attività dovrà essere riportata in apposito verbale dal Responsabile che deve informare l'incaricato del trattamento alla prima occasione utile.

9. Norme generali per l'utilizzo delle apparecchiature informatiche

L'utente deve utilizzare in modo corretto e lecito le risorse che gli sono state messe a disposizione.

Si riportano di seguito alcune tra le principali indicazioni a cui gli utilizzatori sono tenuti ad attenersi; il personale del SIA è a disposizione per fornire chiarimenti e ulteriori precisazioni in merito ad aspetti che possano risultare complessi o troppo tecnici.

9.1. Computer aziendali

Il personal computer aziendale in dotazione è uno strumento di lavoro. L'utilizzo personale o improprio dello stesso può comportare inefficienze, problemi di sicurezza e costi di manutenzione imprevedibili ed è pertanto non consentito, salvo casi particolari espliciti.

L'utilizzatore di attrezzature informatiche, quali ad esempio lap top, pc, tablet, etc., ovvero Consegnatario per debito di vigilanza, che riceve in consegna beni mobili inventariabili dell'Azienda è tenuto:

1. Ad utilizzare il bene che ha in uso secondo le regole del buon senso comune;
2. Rispettare le regole per l'utilizzo del bene;
3. Restituire al consegnatario per debito di custodia i beni divenuti inutili;
4. Comunicare al proprio dirigente ogni variazione che intervenga sulla consistenza dei beni affidati e alla loro dislocazione;
5. È personalmente responsabile, sotto il profilo patrimoniale, della presa in carico dei beni assegnati, della loro vigilanza e del loro spostamento.

Possono essere utilizzati unicamente programmi/applicazioni installati o autorizzati dal SIA e per i quali siano stati regolarmente assolti gli oneri relativi alla concessione delle licenze d'uso, ove richieste. In caso di necessità di ulteriori applicazioni il dipendente dovrà farne richiesta al SIA.

È vietato disinstallare o disattivare i software presenti sul PC, in particolare i sistemi di protezione e sicurezza aziendali (tra cui l'antivirus), e i prodotti software di inventariazione e controllo remoto (OCS Inventory, Ultra VNC ecc.). Eventuali eccezioni devono essere concordate con il SIA ed esplicitamente autorizzate.

Il personale tecnico potrà effettuare verifiche automatizzate o puntuali sui software presenti nelle postazioni, rimuovendo o bloccando l'esecuzione dei software non autorizzati, richiedendo eventualmente giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

L'utilizzatore è personalmente responsabile del computer assegnatogli; egli ha pertanto l'obbligo, per quanto nelle sue possibilità, di impedire ad altri indebiti utilizzi dell'apparecchiatura informatica.

Si sottolinea che il furto o l'indebito utilizzo di un computer rilevano, oltre che sotto il profilo patrimoniale, anche in relazione a un possibile improprio utilizzo dei dati in esso contenuti e/o alla perdita degli stessi.

È obbligatorio segnalare tempestivamente casi di furti o incidenti relativi alla sicurezza.

Per finalità di sicurezza e risparmio energetico, computer e monitor devono sempre essere spenti al termine del loro utilizzo. Le apparecchiature devono essere disattivate anche nel caso di prolungate assenze dal servizio, pur nell'ambito dell'orario di lavoro.

In caso di assenze brevi (es. pausa mensa, riunione ecc.) durante le quali l'apparecchiatura rimane incustodita è obbligatoria l'attivazione dello screen saver (salvaschermo) protetto da password.

Al computer possono essere connesse solamente periferiche o dispositivi forniti o autorizzati dall'Azienda, da utilizzarsi esclusivamente se necessari per le attività aziendali.

Nessuna periferica o dispositivo componente la stazione di lavoro può essere rimossa, salvo specifica autorizzazione.

Il personale tecnico dell'ente gestore potrà effettuare verifiche automatizzate o puntuali sulle periferiche presenti nelle postazioni, disabilitando o rimuovendo le periferiche non autorizzate, eventualmente chiedendo motivazioni e giustificazioni agli utenti utilizzatori relativamente alle anomalie riscontrate.

9.2. Computer portatili e aziendali

Oltre a quanto indicato nel paragrafo precedente, gli utilizzatori dei computer portatili aziendali (includendo anche tablet, mini PC ecc.) devono seguire le seguenti istruzioni.

Il computer portatile deve essere conservato con cura sia durante gli spostamenti sia sul luogo di utilizzo aziendale o extraaziendale, adottando idonee precauzioni per preservarlo da furti e custodendolo in luogo sicuro in caso di allontanamento, anche temporaneo.

Inoltre, in luoghi pubblici non devono essere inserite o lette informazioni di carattere riservato o critico.

Il SIA provvederà a dotare i portatili di ulteriori sistemi di sicurezza (es. crittografia dei contenuti, sistemi antifurto ecc.).

9.3. Utilizzo di attrezzature informatiche personali

Le attrezzature personali di qualsiasi tipologia (PC, tablet, smartphone ecc.) non possono essere collegate alla rete aziendale, salvo diversa esplicita autorizzazione in forma scritta rilasciata dal SIA.

In alcuni casi i dispositivi personali potranno collegarsi, previa richiesta al SIA, a sotto reti appositamente predisposte nel rispetto della sicurezza della rete aziendale e pertanto destinate a funzioni limitate (es. rete ospiti per accesso a Internet).

9.4. Stampanti e scanner

Salvo eccezioni particolari e giustificate (es. ambulatori, guardiole, sportelli), saranno sempre installate stampanti di rete o fotocopiatrici multifunzione (con funzione stampante e scanner) in modo da consentirne l'uso condiviso tra più uffici, settori, strutture, anche al fine di un razionale utilizzo delle risorse assegnate.

Sono distribuite esclusivamente stampanti bianco/nero, generalmente laser. Nel caso si ritenga indispensabile, per uso clinico, l'acquisto di una stampante a colori, la richiesta dovrà essere motivata e autorizzata dal Responsabile dell'UO richiedente.

È consentita la stampa solo di documenti strettamente necessari, mentre dovrà essere privilegiato l'utilizzo di documenti informatici. In caso di stampa è importante ritirarla prontamente dai vassoi delle stampanti comuni per evitare accesso indesiderato a dati personali. Si raccomanda in particolare di indirizzare verso una stampante dedicata, collocata in un'area controllata, le stampe di dati sensibili.

È buona regola, inoltre, privilegiare la stampa di documenti in modalità fronte/retro e bianco/nero in *modalità risparmio*.

In caso di necessità di stampe di documenti particolarmente lunghi o di un numero significativo di copie, si consiglia di rivolgersi al Centro Stampa.

Nell'utilizzo dello scanner accertarsi di utilizzare sempre una bassa risoluzione di scansione, in particolare prima di inviare, per es. via mail, un documento scansionato.

Si ricorda che nel caso di utilizzo di scanner deve essere rispettata la normativa sul diritto d'autore, analogamente a quanto avviene per la riproduzione di documenti attraverso fotocopiatrici. Inoltre non possono essere scansionati documenti aventi contenuto oltraggioso e/o discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9.5. Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive

L'utilizzo di hard disk esterni e supporti di memorizzazione rimovibili deve essere effettuato con molta cautela, utilizzando solo dispositivi necessari per le attività aziendali, seguendo le seguenti istruzioni: Scaricare da help desk il programma che permette di criptare i dati contenuti nel dispositivo portatile e installarlo.

Nel caso fosse strettamente necessario, per es. se il dispositivo è utilizzato per le copie di sicurezza, è obbligatorio criptare i dati con programmi adeguati, in genere già contenuti negli stessi supporti. Per eventuali istruzioni rivolgersi al personale tecnico dell'help desk.

In caso di perdita dei dati contenuti in un dispositivo non protetto con crittografia dei dati, il proprietario del dispositivo sarà ritenuto responsabile della perdita dei dati di proprietà dell'Azienda

Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antimalware, che non può essere interrotta dall'utente per permettere al sistema di sicurezza di completare la verifica. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, manovra che rischia di danneggiare e rendere non più leggibili i dati presenti sul dispositivo.

È da evitare il salvataggio su tali supporti di dati sensibili. L'eventuale perdita accidentale del supporto consentirebbe a chiunque di accedere ai medesimi dati, senza che peraltro si conosca la sua identità.

Nel caso fosse strettamente necessario, per es. se il dispositivo è utilizzato per le copie di sicurezza, è obbligatorio criptare i dati con programmi adeguati, in genere già contenuti negli stessi supporti. Per eventuali istruzioni rivolgersi al personale tecnico dell'help desk.

L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto l'esclusiva responsabilità dell'utilizzatore e deve essere effettuato avendo cura di cifrare i dati aziendali riservati e i dati personali o sensibili con l'utilizzo di password sicure.

Alcune raccomandazioni di buon senso:

- I supporti rimovibili (CD, DVD, pen drive, memorie flash per macchine fotografiche digitali e palmari, hard disk rimovibili ecc.) devono essere custoditi con la massima riservatezza e con la massima diligenza e non devono essere lasciati incustoditi o facilmente accessibili da parte di altri incaricati non autorizzati al trattamento dei dati contenuti.
- In particolare, durante il loro utilizzo devono essere presidiati dagli incaricati e quando non temporaneamente utilizzati devono essere riposti in contenitori sicuri.
- I supporti rimovibili possono essere utilizzati e ceduti solamente tra gli incaricati autorizzati al trattamento dei dati in essi contenuti.
- I supporti rimovibili non riscrivibili, per i quali i dati presenti non possono essere eliminati attraverso procedure di formattazione del supporto (ad esempio: CD-R, DVD-R, DVD+R ecc.), devono essere distrutti fisicamente nel momento in cui si ritiene non debbano essere più utilizzati per il trattamento.
- I supporti rimovibili riscrivibili (ad esempio: CD-RW, DVD-RW, DVD+RW, pen drive, memorie flash per macchine fotografiche digitali e palmari, hard disk rimovibili ecc.) non più utilizzati per il trattamento di dati devono essere formattati completamente e a basso livello da parte degli utilizzatori, in modo che i dati precedentemente in essi contenuti non siano intelligibili e non siano tecnicamente in alcun modo ricostruibili.

È vietato consegnare a terzi supporti in precedenza utilizzati per la memorizzazione di dati personali o sensibili, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo la cancellazione.

L'utente è tenuto a comunicare immediatamente al proprio Responsabile o a denunciare all'autorità giudiziaria l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi dei supporti rimovibili. Copia della denuncia deve essere inviata al SIA.

È infine obbligatorio verificare sempre l'assenza di virus prima dell'utilizzo dei supporti rimovibili.

9.6. Norme generali per l'utilizzo del software distribuito dal SIA

L'incaricato del trattamento:

- deve utilizzare il software solo per attività aziendali;
- deve custodire il software ricevuto in dotazione;
- non deve cedere il software a colleghi o a terzi;
- deve utilizzare solo il software aziendale assegnato.

Inoltre si ribadisce che:

- è vietata qualsiasi riproduzione (permanente, temporanea, parziale o totale), traduzione, distribuzione di software di terzi, che non sia autorizzata in base alla licenza a esso applicabile,
- salvo specifiche autorizzazioni, non è consentito l'uso in azienda di software acquisito privatamente o disponibile gratuitamente, né l'uso all'esterno dell'azienda di software aziendale.

9.7. Software antivirus e di protezione dei dati

Il SIA, mediante l'utilizzo di firewall e prodotti antivirus gestiti e aggiornati centralmente, assicura la protezione dell'infrastruttura, dei sistemi informatici e delle postazioni di cui effettua la manutenzione.

L'aggiornamento dell'antivirus avviene giornalmente, quello delle patch critiche e di sicurezza di Windows avviene mensilmente, previa verifica in ambienti di test.

È comunque responsabilità di ogni incaricato controllare che il PC sia dotato del prodotto antivirus aziendale e che sia configurato per l'aggiornamento automatico. In caso contrario l'incaricato è tenuto a farne immediata richiesta al SIA.

È vietato il collegamento alla rete aziendale di qualsiasi personal computer non adeguatamente protetto mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).

9.8. Dischi di rete, cartelle personali e cartelle condivise

L'Azienda mette a disposizione degli utilizzatori che ne fanno richiesta, dischi di rete, anche in Cloud (cartelle che possono essere personali o condivise tra più utilizzatori) per l'archiviazione di informazioni di carattere professionale. Non possono essere collocati sulle unità di rete - nemmeno per periodi brevi - file personali o comunque aventi contenuto diverso da quello strettamente connesso all'attività lavorativa.

La richiesta di attivazione di tale servizio va fatta tramite il Modulo per l'utilizzo dei Servizi Informatici Aziendali (vedi anche Allegato B).

Il servizio SIA deve svolgere periodici controlli a campione sulle unità di rete e può procedere autonomamente alla rimozione di dati non connessi alle attività proprie dell'azienda. Nel caso in cui la natura o il contenuto di informazioni/dati da collocare in rete per un utilizzo professionale potesse risultare dubbia/ambigua il titolare degli stessi dovrà informare preventivamente il SIA affinché non proceda alla rimozione.

Il SIA provvede al backup dei dati collocati su unità di rete. Nel caso di perdita di dati in rete, pertanto, sarà possibile richiedere il recupero del file così come salvato nell'ultima versione di backup. Per questi motivi è fortemente consigliato l'utilizzo delle unità di rete per il salvataggio di dati/file di particolare importanza e rilevanza.

Le unità di rete devono essere mantenute con diligenza a cura degli utilizzatori; agli stessi è richiesta la periodica – almeno semestrale – revisione dei dati salvati e l'eliminazione di quelli obsoleti o, comunque, non più utilizzati o necessari. È opportuno evitare la duplicazione di dati onde consentire uno sfruttamento razionale delle unità di rete.

I server aziendali centralizzati sono le uniche entità predisposte alla condivisione di risorse. È vietato condividere localmente e direttamente dischi, cartelle o risorse (es. cartelle di scambio) a eccezione delle stampanti comuni.

Solo in situazioni di particolari problematiche tecniche, su autorizzazione del SIA, potranno essere attivate condivisioni fra personal computer che dovranno inderogabilmente essere protette da password di accesso.

Per ogni cartella condivisa è individuato un referente, avente la responsabilità di definire l'elenco degli utilizzatori e dei profili di abilitazione, nonché di verificare il corretto utilizzo della cartella da parte degli utilizzatori stessi.

Al referente spetta verificare periodicamente e comunque almeno annualmente, le abilitazioni assegnate agli utilizzatori, segnalando tempestivamente al SIA la necessità di assegnare, modificare o cancellare l'accesso alla cartella da parte degli utilizzatori.

Il referente della cartella più individuare fino a 2 collaboratori per affiancarlo nella gestione delle abilitazioni all'uso della cartella.

Lo spazio assegnato può essere concordato di volta in volta secondo le reali necessità.

9.9. Presentazioni

È fatto divieto di inserire dati personali nelle presentazioni (es. powerpoint): si devono utilizzare dati privi di qualsiasi riferimento ai soggetti interessati. Va precisato che anche codifiche, quali il codice fiscale o altro codice, non sono ammesse in quanto possono ricondurre indirettamente ai dati identificativi del soggetto interessato.

10. Collegamento di attrezzature alla rete dati

La rete dati aziendale su cavo o wireless (wi-fi) è gestita dal SIA.

L'accesso di computer o altre attrezzature (biomedicali e non) alla rete aziendale deve essere autorizzato dal SIA, che definisce la connettività da assegnare in base alle caratteristiche dell'attrezzatura e alle esigenze dell'utilizzatore (Allegato D).

10.1 Rete AORN

La rete interna permette l'accesso a tutti i principali applicativi aziendali e pertanto è destinata all'uso da parte dell'utente aziendale esclusivamente mediante dispositivi dell'azienda.

Il collegamento alla rete di attrezzature informatiche personali, se ammesso, è regolato mediante accesso a sotto reti predisposte ad-hoc (per es. la rete ospiti per l'eccesso a internet).

Pertanto sono vietati:

- Il collegamento alla rete Aziendale di computer e server se non forniti o autorizzati dal SIA.
- Il collegamento alla rete aziendale di personal computer non adeguatamente protetti mediante software antivirus (aggiornamento almeno settimanale) e patch di sicurezza del sistema operativo (aggiornamento almeno mensile).
- Il collegamento alla rete, non autorizzato dal SIA, di apparati di rete quali switch, router (anche USB o wifi) e attrezzature per reti wireless (es. access point).
- Qualsivoglia forma di collegamento ad altre reti laddove la stazione di lavoro sia connessa alla rete dell'A.O.R.N. A. Cardarelli di Napoli; sono pertanto vietate, per le stazioni di lavoro connesse alla rete aziendale, le connessioni tramite modem o chiavette Internet e l'utilizzo di una doppia scheda di rete; per i PC portatili dotati sia di scheda di rete tradizionale che di

scheda di rete wireless, entrambe le schede possono essere abilitate al collegamento alla rete aziendale purché non vengano utilizzate contemporaneamente.

Le regole valgono anche per le attrezzature collegate o ospitanti strumentazioni medicali e analitiche.

10.2. Altre reti wi-fi in Azienda

Oltre alla rete dati aziendale, sia cablata che wi-fi, sono disponibili anche le seguenti reti wi-fi:

- *Guest_Cardarelli, senza accesso alla rete aziendale;*
- *Ospiti: rete a disposizione degli ospiti dell'azienda e ai dipendenti con dispositivi propri.*

11. Utilizzo in Azienda di dispositivi di telecomunicazione radiomobili o wireless

A causa della concreta possibilità che le attrezzature informatiche ed elettromedicali aziendali siano soggette a malfunzionamenti legati alla presenza di sorgenti di campi elettromagnetici (es. dispositivi mobili con connessione di tipo wireless), nell'allegato C "Raccomandazioni per l'utilizzo in Azienda di dispositivi di telecomunicazione radiomobili o wireless" sono fornite indicazioni di comportamento per tutti gli operatori aziendali.

12. Uso e salvataggio dei dati aziendali

Il SIA provvede al salvataggio dei dati registrati tramite i sistemi informativi aziendali centralizzati.

La politica di backup (creazione di copie di sicurezza), che definisce la frequenza di salvataggio e il tempo di tenuta dei backup, viene adottata dal SIA in linea con indicazioni normative, raccomandazioni e *best practice*.

Al fine di salvaguardare tutti gli altri dati aziendali ritenuti di interesse e utilità per l'Azienda (es. documenti doc, xls, pdf, ecc.), **è vietato memorizzarli sull'hard disk dei PC**: a tale scopo dovranno invece essere utilizzati i dischi di rete e i server gestiti dal SIA (vedi capitolo "Dischi di rete, cartelle personali e cartelle condivise.

Nel caso invece sia indispensabile memorizzare dati aziendali localmente sugli hard disk dei PC, è fatto obbligo agli utenti di effettuare una copia di sicurezza di tali dati, con frequenza almeno settimanale.

Il SIA a questo scopo fornisce, su richiesta, i dispositivi hardware necessari per il salvataggio dei dati su supporto rimovibile. È fondamentale che tali supporti non siano permanentemente accessibili dal PC, onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza: a tal fine si raccomanda di collegare i dispositivi di backup solo per il tempo strettamente necessario alla realizzazione della copia di sicurezza, rimuovendoli opportunamente al termine della copia e riponendoli in luogo sicuro. Vedi anche paragrafo "Supporti di memorizzazione: CD, DVD, hard disk esterni, memory card, pen drive".

È responsabilità degli utenti conservare adeguatamente e proteggere le copie di backup.

13. Norme generali per l'utilizzo dei servizi Internet

13.1. Posta elettronica e navigazione Internet

Relativamente al corretto utilizzo della posta elettronica e della rete Internet si rinvia al relativo regolamento.

13.2. Pubblicazione di contenuti e realizzazione di siti personali

L'utente non è autorizzato in alcun caso a produrre e a pubblicare siti web personali utilizzando risorse aziendali né a pubblicare autonomamente siti riferiti alla struttura di appartenenza.

Ogni eventuale necessità di realizzare siti web personali o di struttura utilizzando risorse aziendali dovrà essere espressamente autorizzata dall'UO Comunicazione e relazione con i cittadini.

È fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza autorizzazione dell'UO Comunicazione e relazione con i cittadini.

È fatto divieto agli utenti di inserire nei siti personali collegamenti (link) al sito aziendale senza autorizzazione dell'UO Comunicazione e relazione con i cittadini.

Si applicano in ogni caso le norme dei Codici deontologici professionali.

È fatto assoluto divieto di realizzare funzioni di Hosting utilizzando risorse aziendali.

13.3. Connessione a provider diversi da quello aziendale

È vietato l'utilizzo di accessi internet mediante Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti Provider, anche con abbonamenti privati.

Infatti tali connessioni rappresentano un potenziale rischio per la sicurezza dell'intero sistema informativo aziendale di cui l'utente è pertanto consapevole.

13.4. Utilizzo dell'ambiente cloud aziendale per la condivisione temporanea di documenti

Nel caso risulti necessario, per esigenze aziendali, condividere o inviare documenti aziendali, anche di grosse dimensioni, con persone esterne all'AORN, è possibile utilizzare il sistema di cloud aziendale contattando il SIA.

Per accedere occorre essere abilitatati previa richiesta come indicato in Allegato B.

Tale sistema è da ritenersi un deposito temporaneo in cui i documenti devono permanere per il tempo necessario per il loro recupero da parte della persona destinataria. Si consiglia di non superare il limite di due settimane.

L'accesso ai documenti deve essere sempre consentito mediante password.

Il tempo di permanenza di file e documenti sul cloud è comunque lasciato alla valutazione e alla responsabilità dell'utilizzatore.

13.5. Utilizzo di server esterni per backup/gestione/condivisione documenti aziendali

È vietato caricare documenti aziendali riservati e dati sensibili su sistemi di memorizzazione esterni cloud quali Dropbox, Google Drive, SkyDrive, icloud ecc.

Ciò in quanto tali sistemi possono essere soggetti ad attacchi informatici e i dati possono essere sottratti o manipolati illegalmente. Inoltre, molti di tali sistemi sono ospitati in paesi non soggetti a regolamentazioni sulla privacy ai sensi del GDPR 2016/679

Non verranno pertanto effettuate abilitazioni specifiche che permettano la connessione a tali sistemi, salvo casi particolarissimi da valutare e autorizzare singolarmente (per es. accessi temporanei per prelevare dati da gruppi di lavoro già esistenti).

Gli utenti universitari e gli utenti aziendali dotati di Office nella versione online possono accedere a OneDrive[2] mediante credenziali universitarie o aziendali; infatti in tal caso si ha la garanzia che i dati siano conservati in Europa, secondo la relativa normativa privacy, tuttavia permane il divieto di collocare su tale cloud dati riservati o sensibili.

13.6. Assistenza da remoto (VPN e altre tipologie)

Sono ammessi collegamenti remoti dall'esterno per l'accesso alle risorse aziendali, sia per manutenzione di attrezzature da parte di ditte esterne, sia per lo svolgimento di specifiche attività da una sede esterna, ma devono essere autorizzati dal SIA.

[2] Si tratta del servizio fornito da Microsoft con il pacchetto Office online

14. Modalità di prestazione dei servizi

Il SIA si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità di interromperli esclusivamente per le manutenzioni ordinarie e cercando di arrecare il minor disagio possibile agli utilizzatori. Salvo impedimenti le interruzioni saranno comunicate agli utenti.

Per poter fornire assistenza e supporto tempestivi nel caso di guasti e malfunzionamenti, su ciascun computer fisso o portatile è installata un'applicazione che consente ai tecnici del SIA di collegarsi remotamente, senza bisogno di intervenire sul luogo.

Pertanto, la manutenzione alle stazioni di lavoro viene generalmente effettuata, in prima battuta, mediante tali sistemi software di manutenzione remota. Solo nel caso di mancata soluzione del problema in modalità remota, viene effettuato un intervento in loco.

Si informa che i sistemi di controllo remoto suddetti sono configurati affinché gli operatori che intervengono per la manutenzione possano farlo esclusivamente previo consenso dell'utilizzatore della postazione (consenso che viene richiesto in tempo reale sullo schermo del pc); non sarà richiesta l'autorizzazione solo nei casi in cui si renda necessario effettuare installazioni o aggiornamenti software da remoto, che non prevedono la possibilità di accesso ai dati presenti.

Inoltre, l'utente può verificare l'attività effettuata in remoto dal tecnico rimanendo presso la postazione.

Gli interventi sono eseguiti da personale identificato e autorizzato dal SIA: tale personale afferisce al SIA direttamente o tramite contratti di fornitura di servizi.

15. Acquisto su progetti finanziati (PO)

Tra i servizi erogati dal SIA vi è anche l'acquisto di beni e servizi per l'attività ordinaria aziendale e per la realizzazione di progetti obiettivo con finanziamenti dedicati. Utilizzando fondi derivanti da progetti finanziati si possono acquistare solo attrezzature analoghe a quanto viene acquistato con fondi "standard", ciò anche in ottica di ottimizzare l'assistenza tecnica ai sistemi e alle infrastrutture. Eventuali eccezioni devono essere giustificate e autorizzate.

16. Installazione di Microsoft Office sulle postazioni di lavoro

Le postazioni di lavoro fornite dal SIA sono provviste di Microsoft Office licenziato.

17. Disposizioni finali

17.1. Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente regolamento, la disponibilità a un utente dei servizi informatici aziendali cesserà totalmente nel caso non sussista più la condizione di dipendente o di collaboratore esterno; inoltre può cessare o essere limitata nei privilegi assegnati in caso di:

- revoca dell'autorizzazione all'uso fornita dal Responsabile (per es. per cambio di mansione, ruolo, CDR ecc.);
- accertato uso non corretto o comunque estraneo alla sua attività lavorativa dei servizi informatici aziendali;
- accertate manomissioni e/o interventi illeciti sull' hardware e/o sul software;
- accertate diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. e altre informazioni tecniche riservate;
- accesso illecito e intenzionale dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili, in particolare se l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- violazione delle regole essenziali stabilite dal presente regolamento.

Si precisa che in caso di cessazione della condizione di dipendente o collaboratore a una certa data la casella di posta dell'utente sarà immediatamente bloccata. A partire da tale data non sono consentiti né l'accesso alla casella, né la ricezione tramite inoltro.

Casi particolari devono essere esplicitamente autorizzati dalla direzione aziendale.

Si ricorda inoltre che, una volta cessata la condizione di dipendente o collaboratore è vietato asportare dati aziendali prodotti nell'attività istituzionale. Non sarà dato seguito, pertanto, alla richiesta di scarico massivo (per es. su supporto esterno) delle mail dell'utente, né di altri file contenuti nei file server o nei personal computer.

17.2. Responsabilità dell'utilizzatore delle risorse informatiche

- L'utente è direttamente e totalmente responsabile dell'uso che egli fa del servizio di posta elettronica e di accesso a Internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.
- All'utente è consentito di utilizzare il servizio solo per ragioni professionali connesse alla propria attività, in modo individuale, salvo eccezioni riportate del relativo regolamento.
- Con l'accettazione di questo regolamento l'utente è informato e consapevole del fatto che la conoscenza della password da parte di terzi consente a questi ultimi l'accesso alla rete aziendale e l'utilizzo dei relativi servizi in nome dell'utente e l'accesso ai dati cui il medesimo è abilitato, con le conseguenze che la cosa può comportare, quali ad esempio la visualizzazione di informazioni riservate, la distruzione o la modifica dei dati, la lettura della propria posta elettronica, l'uso indebito di servizi ecc.
- L'utente prende atto che è vietato servirsi o dar modo ad altri di servirsi della rete aziendale e dei servizi da essa messi a disposizione per utilizzi illeciti che violino o trasgrediscano diritti d'autore, marchi, brevetti, comunicazioni private o altri diritti tutelati dalla normativa corrente, per utilizzi contro la morale e l'ordine pubblico, per recare molestia alla quiete pubblica o privata, per recare offesa o danno diretto o indiretto all'Azienda o a terzi.

17.3. Informativa sul trattamento dei dati da parte del SIA

Ai sensi dell'art. 13 del D. Lgs. n. 196/2003 e s.m. si informa che i dati relativi all'utilizzo dei servizi informatici da parte degli utenti sono trattati nel rispetto della legge e degli obblighi di riservatezza cui è ispirata l'attività dell'AORN.

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

Finalità e modalità del trattamento

L'AORN si impegna a trattare i dati relativi all'utilizzo dei servizi informatici unicamente per motivi volti a garantire la sicurezza e il corretto funzionamento dei servizi informatici e per finalità direttamente pertinenti all'attività lavorativa del dipendente.

Le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate per finalità di sicurezza del sistema.

L'attività di registrazione avviene attraverso i file "log" di sistema a cura del SIA o dell'articolazione aziendale che detiene la responsabilità organizzativa dei sistemi o servizi.

Per quanto riguarda l'utilizzo dei sistemi informativi aziendali, le operazioni effettuate servendosi delle credenziali di autenticazione potranno essere memorizzate al fine di garantire la tracciabilità del trattamento dei singoli dati. Le informazioni relative alla tracciabilità del dato (inserimento, modifica, cancellazione) vengono gestite con le stesse modalità del dato a cui si riferiscono.

Le registrazioni potranno essere utilizzate, su richiesta del Titolare o dei Responsabili del trattamento dei dati personali, per finalità statistiche e di valutazione della qualità in riferimento a taluni servizi erogati, esclusivamente da parte di personale dell'Azienda appartenente al SIA.

L'AORN si riserva di effettuare dei controlli, anche a campione, concernenti l'utilizzo corretto degli strumenti di lavoro, fermo restando il divieto di controllo a distanza dei lavoratori stabilito dall'art. 4 della L. 20.5.1970, n. 300.

Comunicazione e diffusione

I dati relativi all'utilizzo degli strumenti informatici sono trattati, per le finalità indicate al punto precedente, dagli operatori del SIA e possono essere portati a conoscenza, esclusivamente nei casi consentiti dalla legge, del responsabile dell'U.O. di appartenenza dell'utente.

Infine, i log potranno essere oggetto di provvedimenti dell'Autorità giudiziaria e amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo all'interno dell'Azienda.

Titolarità

Il Titolare del trattamento dei dati è l'A.O.R.N. A. Cardarelli, con sede legale in NAPOLI, Via A. CARDARELLI, N. 9.

Il Direttore Generale ha individuato con del. ____ delegati di funzioni i del trattamento dei dati i Direttori delle macro articolazioni aziendali, i Responsabili degli Uffici di TPA, i Direttori di UOC e UOSD, nonché i Coordinatori del personale Sanitario del comparto

Diritti dell'utente "interessato"

A seguito del trattamento dei dati, si possono esercitare i diritti previsti ai sensi del CAPO III del GDPR 2016/679, e più precisamente l'utente, in qualità di "interessato", può conoscere i dati trattati, nonché può richiedere l'aggiornamento, la rettifica e, ove abbia interesse, l'integrazione, nonché le altre "azioni" previste dalla Legge.

È possibile in qualsiasi momento far valere i diritti di cui sopra con la sola richiesta avanzata al Titolare del trattamento attraverso info@aocardarelli.it o al Responsabile della Protezione dei dati dpo.privacy@aocardarelli.it

17.4. Disposizioni transitorie

A integrazione di tale regolamento, per il rispetto di quanto indicato dalla circolare AgID n°1/2017 nel corso del 2019 saranno condotte le seguenti attività:

1. sarà inibito l'utilizzo di qualsiasi client locale di posta. L'unico accesso consentito sarà tramite il servizo webmail del sistema di posta Aziendale, che rispetta tutti i requisiti imposti dalla circolare.
2. Sarà impedita la visualizzazione automatica del contenuto dei file da qualsiasi sistema gestionale (posta, esplora risorse, accesso da chiavette usb, CD, DVD ecc.).
3. Saranno fornite istruzioni operative e strumenti per la crittografia dei file dove non già noti e disponibili.
4. Sarà potenziata e migliorata l'infrastruttura centrale al fine di facilitare al massimo gli utenti a non conservare file sui sistemi locali, ma di conservarli sempre centralmente in file server sicuri gestiti dal SIA.

Inoltre:

è vietato all'utente che disponga dei diritti per farlo, alterare le impostazioni del sistema operativo o degli applicativi in senso contrario a quanto indicato dalla circolare AgID (es. attivazione dell'esecuzione automatica di macro nei file di office, visualizzazione automatica del contenuto dei file ecc.

Allegato A – Elenco applicativi di base e specifici autorizzati

Applicativi di base (sono esclusi dall'elenco i sistemi operativi)

Inserire elenco applicativi.

#	Applicativi di base	Note
AB1	ADOBE READER	7-8-9-10-11
AB2	ANTIVIRUS MCAFEE	10.5
AB3	CCLEANER	5.5.0-5.5.2
AB4	GOOGLE CHROME	71
AB5	INFOCERT DIKE	6
AB6	INTERNET EXPLORER	11
AB7	MICROSOFT OFFICE	2007-2013-2016
AB8	NET FRAMEWORK 3.5 SP3	Su Windows 10 NET Framework 4.0
AB9	REAL-VNC	5.05
AB10	VLC	3.0.6
AB11	WIN RAR	5.6.1

Applicativi specifici

#	Applicativi Amministrativi	Utilizzo	Note
AA1	ALA	Ufficio Vigilanza e ALA	Client Server
AA2	AMBIPSOA	UOC GREF	Client Server
AA3	APP ECUPT	Pazienti	Web Application
AA4	APP PS	Visitatori, Accompagnatori e Pazienti	Solo Lettura - App
AA5	ARUBA PEC	Tutti	Web Application
AA6	BIOGESTNT	UOC GAT	Web Application
AA7	CENTRO SERVIZI	Front-Office, Back-Office	Web Application
AA8	CONSIP	UOC ABSE, UOC GATIB	Web Application
AA9	EASYDOC DETERMINE E DELIBERE	Direzione Sanitaria, Amministrativa e Generale, UOC GEF, UOC ABSE, UOC GATIB, Affari Generali e Patrimonio, Affari Legali	Web Application
AA10	EASYDOC FASCICOLO PERSONALE	UOC GRU	Web Application
AA11	EASYDOC PROTOCOLLO	Tutti	Web Application
AA12	ENTRATEL	UOC GREF	Client Server
AA13	FTPS NOIPA	UOC GRU	Client Server
AA14	GOP	Tutti	Web Application
AA15	INAIL	UOC GRU	
AA16	LETTORE PRESENZE BIOMETRICI	UOC Trattamento Economico Personale	Web Application
AA17	MEPA	UOC ABSE, UOC GAT	Web Application
AA18	NOIPA	UOC GRU, Dipendenti	Web Application
AA19	OFFICE 365 - POSTA ELETTRONICA	Tutti	Web Application
AA20	PENSIONI S7	UOC GRU Previdenza	Client Server

AA21	PENTAHO	UOC Controllo di Gestione	Web Application
AA22	PERSWEB	UOC GRU, Trattamento economico	Web Application
AA23	PORTALE ENTI	UOC Farmacia	Web Application
AA24	QUANI SDO	UOC Epidemiologia	Client Server
AA25	SCANSHEAR	UOC GRU	Web Application
AA26	SDM (CARTELLE CLINICHE CSA)	Front-Office, Back-Office, Direzione Medica di Presidio, Operatori medici autorizzati	Web Application
AA27	SIAC	ABSE, GREF, UOC Farmacia	Web Application e Client Server
AA28	UNIMONEY	UOC GREF	

#	Applicativi Sanitari	Utilizzo	Note
AS1	AIFA	Medici Prescrittori	Web Application
AS2	ARMADIETTO DI REPARTO	Tutte le UO	Web Application
AS3	ATHENA	Anatomia Patologica	Client Server
AS4	BIOLOGIA MOLECOLARE	Genetica Medica	Client Server
AS5	CPI	Tutte le UO	Web Application
AS6	EBIT	Emodinamica	Client Server
AS7	ELIOT	Trasfusionale	Client Server e Web Application
AS8	EOS	Genetica Medica	Client Server
AS9	FENIX	Radiologia	Web Application
AS10	GALILEO	Neurofisiopatologia	Client Server
AS11	GEDON	CRT	Client Server
AS12	INFOTHAL	Microcitemia	Web Application
AS13	LOG 80	Oncologia ed Ematologia	Web Application
AS14	LURTO	CRT	Client Server
AS15	MALATTIE RARE	UO Abilitate	Web Application
AS16	MYSTAR	Diabetologia, Endocrinologia	Client Server
AS17	OLYMPUS	Gastroenterologia e Fisipatologia Respiratoria	Client Server
AS18	OPENLIS	Laboratorio	Client Server
AS19	PACS	Radiologia e tutte le UO	Web Application
AS20	SANIARP	Farmacia, UO abilitate	Web Application
AS21	SISTEMA INFORMATIVO TRAPIANTI	CRT	Web Application
AS22	TALETE WEB	Medicina Legale	Web Application

AS2 3	WEB HOSPITAL	Tutte le UO	Web Application

Allegato B – Istruzioni per il rilascio e il rinnovo di credenziali aziendali a personale dipendente e non dipendente

Per accedere ai servizi informatici aziendali qualsiasi nuovo utente dovrà fornire i propri dati personali, prendere visione del presente regolamento e compilare il modulo per l'utilizzo dei servizi informatici aziendali.

Il modulo dovrà essere consegnato alla struttura aziendale deputata alla creazione degli accessi ai sistemi o servizi di cui si richiede l'abilitazione (corrispondente al SIA nella maggioranza dei casi), "autorizzato" dal Responsabile della struttura organizzativa a cui l'utente appartiene.

Nel caso dei sistemi informativi aziendali centralizzati (es. Anagrafe Sanitaria, GRU, Farmacia ecc.), va raccolta la firma per autorizzazione anche del Responsabile organizzativo dei sistemi o servizi di cui si richiede l'abilitazione.

Attraverso la rete Intranet aziendale si ha accesso alla modulistica per effettuare la richiesta di abilitazione all'utilizzo di servizi e procedure informatiche:

L'utilizzo dei servizi informatici aziendali richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) e una parola chiave segreta (password).

Per le attività di rouitine legate all'utilizzo della cartella clinica informatizzata è stato introdotto un ulteriore processo di identificazione del personale, consistente nell'immettere un pin all'atto del salvataggio e/o validazione di una procedura informatica, che sostituisce nei casi consentiti la firma digitale laddove tale firma comporterebbe una sottrazione di tempo rilevante per le attività medico-sanitarie.

Sia nel caso di disattivazione del codice di identificazione personale che nel caso in cui l'utente si dimentichi la propria password, per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo per l'utilizzo dei servizi informatici aziendali, allegare la fotocopia di un documento di identità e consegnarlo al SIA firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.

Quanto riferito sopra vale anche per la firma rafforzata relativa alla cartella clinica informatizzata.

In caso di rinnovo, la password o il pin possono essere consegnati esclusivamente di persona.

In nessun caso possono essere forniti al telefono o inviata con altri mezzi.

La password non potrà essere ceduta a terzi, neppure temporaneamente e dovrà essere mantenuta segreta.

Qualsiasi azione svolta sotto l'autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all'utente titolare del codice userid, salvo che l'utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi.

Non sono previsti codici di accesso anonimi.

L'utente deve conservare la password con la massima riservatezza e con la massima diligenza. La password non deve essere banale né contenere riferimenti facilmente riconducibili all'utente.

È modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni due mesi.

Dopo sei mesi di non utilizzo dei servizi, o nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, la userid e la password vengono automaticamente disattivati. In quest'ultimo caso, i messaggi di posta elettronica in giacenza vengono eliminati.

L'utente si impegna a comunicare immediatamente al SIA l'eventuale furto, smarrimento, perdita ovvero appropriazione a qualsivoglia titolo da parte di terzi della password.

Allegato C – Raccomandazioni per l'utilizzo in azienda di dispositivi di telecomunicazione radiomobili o wireless

1. Definizioni

Campo elettromagnetico

Fenomeno fisico che consiste nell'esistenza contemporanea di un campo elettrico e di un campo magnetico mutuamente accoppiati al punto da costituire un'unica entità fisica. L'intensità del campo magnetico diminuisce con la distanza dalla sorgente.

Le fonti di campo elettromagnetico sono le più svariate: apparecchi elettrici e elettronici, radio, televisione, radar, antenne per la telefonia cellulare, forni a microonde ecc.

Compatibilità elettromagnetica (EMC)

La capacità di un sistema o apparato elettrico e/o elettronico di funzionare correttamente nel suo ambiente elettromagnetico senza introdurre disturbi che possano interferire con il funzionamento di altre apparecchiature presenti nello stesso ambiente.

Interferenza elettromagnetica (EMI)

La sovrapposizione in un ambiente di segnali elettromagnetici riferibili a diversi dispositivi, tale da poter indurre disturbi al corretto funzionamento dei dispositivi stessi.

Dispositivo di telecomunicazione portatile

Apparecchiatura radiomobile aziendale o personale (es. smartphone, tablet, chiavette UMTS/LTE, router mobili, cordless, PC portatili ecc.)

Dispositivo Medico (DM)

Qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; di diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi (Direttiva 2007/47/CE recepita da D. Lgs n. 37 del 25 gennaio 2010);

Apparecchio Elettromedicale

Apparecchio elettrico dotato di una parte applicata o che trasferisce energia verso il o dal paziente o rileva tale trasferimento di energia verso il o dal paziente e che è: dotato di non più di una connessione ad una particolare alimentazione di rete ed è previsto dal fabbricante per essere impiegato nella diagnosi, trattamento o monitoraggio del paziente o per compensare, lenire una malattia, le lesioni o menomazioni (Norma CEI EN 60601-1);

Wireless

Comunicazione tra dispositivi elettronici che non fa uso di cavi. Per estensione sono detti wireless i rispettivi sistemi o dispositivi di comunicazione che implementano tale modalità di comunicazione. Sono wireless le tecnologie di comunicazione basate su onde radio come il Bluetooth, il Wi-fi, le reti cellulari (GSM, GPRS, EDGE, UMTS), le reti satellitari ecc.

Wi-fi

Standard (IEEE 802.11) per collegamenti wireless ad alta fedeltà attuati su bande a radiofrequenza specifiche.

Access point

Dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata, o anche, per esempio, ad un router, permette all'utente mobile di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di scheda wireless.

2. Premessa

La grande diffusione e l'incalzante sviluppo tecnologico dei sistemi di telecomunicazione portatili introducono un nuovo fattore di rischio nelle aree destinate ad un uso sanitario, in quanto si presenta la concreta possibilità che tali sistemi, quali sorgenti di campi elettromagnetici, possano essere utilizzate in stretta prossimità di dispositivi e apparecchiature elettromedicali. Si tratta del fenomeno noto con il termine di interferenza elettromagnetica (electromagnetic interference, EMI) che solo recentemente ha ricevuto l'attenzione dovuta da parte sia della comunità scientifica sia degli enti tra i cui fini figurano la promozione e la tutela della salute. Conosciuti anche come fenomeni EMI, sono particolarmente dannosi in ambito medicale, in quanto un loro effetto può comportare degrado delle prestazioni, malfunzionamenti, guasti e condizioni di pericolo nell'utilizzo di dispositivi e apparecchiature elettromedicali, e conseguentemente danni non solo ai dispositivi o alla strumentazione in uso, ma anche agli stessi pazienti ed operatori coinvolti. I fenomeni EMI sono studiati e affrontati nella disciplina conosciuta come compatibilità elettromagnetica. Obiettivo della compatibilità elettromagnetica è di garantire il corretto funzionamento, nel medesimo ambiente operativo, di apparecchiature elettriche, elettroniche e delle telecomunicazioni, secondo la loro funzione. In ambito europeo, la compatibilità elettromagnetica è regolamentata principalmente dalla direttiva 2004/108/EEC, la quale nei suoi due requisiti essenziali, impone che un qualsiasi apparecchio elettrico o elettronico per poter essere immesso sul mercato comune europeo debba soddisfare ai criteri di compatibilità ed immunità: da un lato il criterio di compatibilità secondo il quale le perturbazioni EM prodotte dall'apparecchio non devono raggiungere un'intensità tale da impedire il funzionamento delle apparecchiature radio e delle telecomunicazioni e dall'altro, il criterio di immunità secondo il quale l'apparecchio deve presentare un livello di immunità alle perturbazioni EM prevedibili nelle condizioni d'uso cui è destinato tale da preservarne il normale funzionamento da un deterioramento inaccettabile.

3. Scopo del documento

Questo documento ha lo scopo di fornire alcune raccomandazioni per l'utilizzo dei dispositivi mobili con connessione di tipo wireless, ovvero dei dispositivi in grado di emettere in varia misura un significativo campo elettromagnetico, ai fini di una corretta prevenzione dei possibili effetti sulla salute dei pazienti e del personale che accede o opera presso le strutture aziendali, con particolare riferimento alla compatibilità elettromagnetica e alle potenziali interferenze con altri dispositivi elettromedicali e di telecomunicazione presenti nell'AORN A. Cardarelli.

I destinatari del presente regolamento sono pertanto:

- Il personale interno all'Azienda (medici, infermieri, dipendenti, convenzionati, collaboratori ecc.).
- I pazienti, i loro accompagnatori e i visitatori.
- Il personale esterno all'Azienda (fornitori, consulenti, addetti alla manutenzione ecc.).

4. Dispositivi oggetto di regolamentazione

Di seguito si riporta una lista, da ritenersi non esaustiva in quanto soggetta a continua evoluzione, dei dispositivi oggetto della presente regolamentazione, che è da intendersi estesa in via generale a tutti i dispositivi in grado di emettere un campo elettromagnetico:

- Dispositivi Radiomobili Privati dell'Azienda e in particolare del servizio 118 (analogici, a standard Tetra ecc.).

- Dispositivi Radiomobili Aziendali e Personali con connettività anche GSM/UMTS/LTE (telefoni cellulari GSM, smartphone UMTS/LTE/Wi-Fi, Tablet UMTS/LTE/Wi-Fi, chiavette USB UMTS/LTE, Router Mobile Wi-Fi/UMTS/LTE ecc.).
- Dispositivi cordless telefonici o con connettività fonia/dati solo wi-fi e/o bluetooth: cordless telefonici, telefoni wi-fi, tablet e PC portatili wi-fi, auricolari ecc.
- Cercapersone.
- Altri dispositivi assimilabili ai casi precedenti.

5 Classificazione

Per maggiore semplicità di trattazione, i dispositivi di cui al punto precedente possono essere raggruppati nelle seguenti macro categorie o tipologie:

- **Tipo A**: dispositivi radiomobili dell'Azienda e in particolare del servizio 118 (analogici, a standard Tetra ecc.), ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile fino a qualche metro di distanza.
- **Tibo B**: dispositivi radiomobili pubblici aziendali e personali (telefoni cellulari GSM, smartphone UMTS/LTE/Wi-Fi, Tablet UMTS/LTE/Wi-Fi, chiavette USB UMTS/LTE, Router Mobile Wi-Fi/UMTS/LTE ecc.), ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile fino a diverse decine di centimetri di distanza.
- **Tipo C**: es. dispositivi cordless telefonici o con connettività fonia/dati solo wi-fi e/o bluetooth, quali cordless telefonici, telefoni wi-fi, tablet e PC portatili wi-fi, auricolari, ecc., ovvero dispositivi in grado di emettere un campo elettromagnetico non trascurabile anche fino a qualche centimetro di distanza. Rientrano in questa classe anche gli access point wi-fi
- **Tipo D**: es. dispositivi cercapersone in sola ricezione (dispositivi cercapersone bidirezionali, che possono trasmettere anche dati e/o fonia in continuità che potrebbero essere meglio raggruppati, a seconda della tecnologia utilizzata, in una delle categorie superiori).

6. Metodologia di lavoro e documentazione

In carenza di documentazione certificata e di supporto normativo, le informazioni e raccomandazioni del presente documento derivano da uno studio eseguito da un gruppo multidisciplinare costituito nel 2015 presso l'Azienda USL di Bologna, con la collaborazione di un supporto professionale esterno3, ha realizzato dettagliate misure dell'inquinamento elettromagnetico generato da una molteplicità di apparecchiature.

Tutti i dati riportati sono rilevati con i sistemi in funzione ovvero durante una conversazione o in trasmissione e ricezione dati.

In estrema sintesi si è rilevato che:

1. I sistemi tablet aziendali, i cordless e i cellulari smartphone aziendali di ultima generazione generano un campo elettromagnetico ridotto (il rischio si presenta in prossimità o quasi a contatto dei DM). Gruppi B, C e D
2. I sistemi radio in uso al 118 presentano un rischio da interferenza piuttosto elevato. Lo stesso grado di rischio potrebbe aversi con i telefoni cellulari di più vecchia generazione. Gruppo A.

Per approfondimenti sui test eseguiti dal gruppo di lavoro su richiamato, il documento di studio è reperibile presso l'Azienda USL di Bologna, dove è possibile visionare l'allegato in cui sono riportati anche i riferimenti normativi disponibili e a cui si rinvia per ogni dettaglio.

3 Laboratori Guglielmo Marconi S.p.A.

7. Raccomandazioni

L'utilizzo dei telefoni cellulari per ragioni di lavoro in ambito sanitario, in particolare per arricchire il patrimonio informativo su casi clinici o per la sicurezza, porta un sicuro miglioramento ai percorsi di cura dei pazienti. Tuttavia, anche alla luce di recenti pubblicazioni, che riportano incidenti o eventi sentinella correlati all'utilizzo non controllato e disattento del cellulare come causa di una diminuzione dell'attenzione durante l'effettuazione di attività sanitarie articolate e complesse, si raccomanda di utilizzarli in modo limitato e solo in caso di necessità. A questo si aggiunga che in relazione alla possibile interferenza che tali apparati possono avere con il funzionamento di dispositivi elettromedicali è necessario che l'utilizzo avvenga secondo alcune semplici raccomandazioni di cautela e di prudenza qui di seguito elencate.

Ciò premesso, valgono le seguenti raccomandazioni:

Dispositivi di **tipo A**

Deve essere evitato l'utilizzo in prossimità di dispositivi elettromedicali. Se in conversazione la distanza di sicurezza raccomandata è di **almeno 3 metri**. In stand by o in solo ascolto sono assimilabili ai dispositivi di classe B.

Dispositivi di **tipo B, C e D**

Deve essere evitato l'utilizzo in estrema prossimità di dispositivi elettromedicali. Se in conversazione o in trasmissione dati la distanza di sicurezza raccomandata è di **almeno 30 centimetri**. Nella modalità stand by la distanza può scendere fino a un massimo di 10 cm.

Access point Wi-Fi e dispositivi Wi-Fi mobili

I dispositivi che emettono il segnale dati e che nel loro insieme costituiscono la rete Wi-Fi aziendale (access point), seguono le regole di cui al punto precedente (classe C). Poiché essi sono in genere posizionati sulle pareti o sul soffitto non sussiste il rischio di interferenze. Tuttavia, particolare attenzione va posta nel caso di dispositivi elettromedicali posizionati su carrelli nel caso questi fossero disposti in estrema prossimità di un access point fisso. In particolare, quest'ultimo potrebbe essere accidentalmente o intenzionalmente rimosso dalla sua posizione fissa e quindi trovarsi in area a rischio interferenza.

Infine si assiste alla diffusione di dispositivi Wi-Fi mobili, peraltro di minuscole dimensioni, collegati alla rete dati pubblica mediante SIA dati. Questi oggetti potrebbero essere posizionati in prossimità di un dispositivo elettromedicale dallo stesso paziente o da parenti e visitatori o anche dalle ditte esterne in caso per es. di interventi per manutenzione. Anche per questi casi si raccomanda la massima attenzione e di seguire le indicazioni date.

Allegato D – Raccomandazioni per l'utilizzo in azienda di software medicali e per la connessione delle tecnologie biomediche alla rete dati aziendale

1. Definizioni

Dispositivo Medico (DM)/Software Medicale (SDM)

Qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; di diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi (Direttiva 2007/47/CE recepita da D. Lgs n. 37 del 25 gennaio 2010).

Dispositivo Medico – Diagnostico In Vitro

Qualsiasi dispositivo medico composto da: un reagente, un prodotto reattivo, un calibratore, un materiale di controllo, un kit, uno strumento, un apparecchio, una attrezzatura o un sistema, utilizzato da solo o in combinazione, destinato dal fabbricante ad essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, unicamente o principalmente allo scopo di fornire informazioni su uno stato fisiologico o patologico, o su una anomalia congenita, o che consentano di determinare la sicurezza e la compatibilità con potenziali soggetti riceventi, o che consentano il controllo delle misure terapeutiche. (Direttiva 1998/79/CE recepita da D. Lgs n. 332 del 8 gennaio 2010).

Tecnologia biomedica

Insieme delle apparecchiature e dei prodotti che afferiscono alla sanità, impiegati quindi nell'intero ciclo della diagnosi, terapia e riabilitazione del paziente, ad eccezione dei farmaci.

Rete IT-Medicale

Rete IT che incorporano almeno un DM.

Apparecchio Elettromedicale

Apparecchio elettrico dotato di una parte applicata o che trasferisce energia verso il o dal paziente o rileva tale trasferimento di energia verso il o dal paziente e che è: dotato di non più di una connessione ad una particolare alimentazione di rete ed è previsto dal fabbricante per essere impiegato nella diagnosi, trattamento o monitoraggio del paziente o per compensare, lenire una malattia, le lesioni o menomazioni (Norma CEI EN 60601-1);

Assistenza da remoto

Collegamento remoto dall'esterno alla rete dati aziendale per la manutenzione di attrezzature sanitarie attraverso una rete virtuale protetta (V.P.N. - Virtual Private Network).

Wireless

Comunicazione tra dispositivi elettronici che non fa uso di cavi. Per estensione sono detti wireless i rispettivi sistemi o dispositivi di comunicazione che implementano tale modalità di comunicazione.

Wi-fi

Standard (IEEE 802.11) per collegamenti wireless ad alta fedeltà attuati su bande a radiofrequenza specifiche.

Access point

Dispositivo elettronico di telecomunicazioni che, collegato ad una rete cablata, o anche, per esempio, ad un router, permette all'utente mobile di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di scheda wireless.

2. Premessa

Con l'avvento dell'I.T. le tecnologie biomediche si sono evolute in sistemi biomedicali nei quali la parte applicativa di controllo, elaborazione, archiviazione e gestione dei dati clinici e medici in formato digitale è generalmente preponderante. Questo ha comportato da un lato importanti benefici per i pazienti e operatori sanitari, ma dall'altro anche rischi derivanti da possibili minacce informatiche provenienti dalla rete interna ma anche dall'esterno.

3. Scopo del documento

In ambito sanitario è auspicabile che le informazioni generate dalle tecnologie biomediche e gestite attraverso software dedicati siano anche integrate con i sistemi informativi delle Aziende Sanitarie.

Questo documento ha l'obiettivo di fornire alcune raccomandazioni per l'utilizzo nell'A.O.R.N. A. Cardarelli dei software medicali, nonché per il collegamento delle tecnologie biomediche alla rete dati aziendale, individuando i percorsi da intraprendere al fine di rendere l'utilizzatore e il gestore dei sistemi medicali consapevoli dei rischi connessi.

I destinatari del presente regolamento sono pertanto:

- Il personale interno all'Azienda (sanitario e non sanitario).
- Il personale esterno all'Azienda (fornitori, consulenti, addetti alla manutenzione ecc.).

4. Dispositivi oggetto di regolamentazione

Di seguito si riporta una lista, da ritenersi non esaustiva in quanto soggetta a continua evoluzione, dei dispositivi oggetto della presente regolamentazione, che è da intendersi estesa in via generale a tutti le tecnologie sanitarie da interfacciare con il sistema informativo aziendale:

- Apparecchiature elettromedicali;
- Apparecchiature da laboratorio;
- Software medicali.

5 Utilizzo rete dati aziendale

La rete dati aziendale è gestita dalla U.O.C. Gestione Servizi Informativi che definisce l'architettura tecnologica hardware e software dei sistemi informativi aziendali per garantire una corretta disponibilità e gestione sicura del patrimonio di informazioni. Per l'installazione di software medicali, nonché per l'inserimento delle tecnologie biomediche (Apparecchiature elettromedicali e da laboratorio) e relativi apparati informatici annessi agli stessi per il loro funzionamento (PC, Monitor) nella rete aziendale, è indispensabile regolamentare in maniera chiara e univoca la metodologia di intervento del personale tecnico e non, nel rispetto delle imprescindibili regole sulla sicurezza informatica.

5.1 Acquisto e/o installazione di SDM e tecnologie biomediche connesse a rete

Prima dell'acquisto di tutti gli apparati, attrezzature, device, software e/o di qualsiasi tecnologia che debbano connettersi alla rete Aziendale, la U.O.C Gestione Servizi Informativi predisporrà le caratteristiche informatiche di compatibilità e di sicurezza, nonché gli strumenti informatici necessari per il corretto utilizzo in conformità alla normativa vigente a cui è fatto d'obbligo di adeguarsi da parte dei fornitori esterni. In tutti casi all'atto dell'acquisizione (anche, e soprattutto in caso di adesioni a convenzioni stipulate da Consip/So.Re.Sa), e prima del collaudo tecnico amministrativo, la ditta aggiudicataria dovrà interfacciarsi con la U.O.C. Gestione Servizi Informativi, congiuntamente con il Servizio di Ingegneria Clinica per individuare le soluzioni tecniche più efficaci a garantire il corretto

flusso di dati nella rete aziendale anche, e soprattutto, ai fini della protezione degli stessi, in ottemperanza al Regolamento Europeo in materia di Protezione dei Dati Personali - G.D.P.R. 2016/679- (D.Lgs. n°101/2018).

5.2 Installazione nuovi punti rete

Nella realizzazione di lavori di ristrutturazione (ove sia previsto l'ampliamento e/o il rifacimento degli impianti di rete) si dovrà preventivamente richiedere la consulenza della U.O.C. Gestione Servizi Informativi per la corretta attestazione di eventuali nuovi punti rete.

5.3 Dispositivi e/o access point

Sulla rete dati aziendale non dovranno essere installati dispositivi diversi da quelli autorizzati: non è consentita l'installazione di switch, HUB o access point non appartenenti alla infrastruttura di rete istituzionale.

5.4 Accesso da Remoto (VPN)

Il servizio VPN è disponibile solo per i fornitori di servizi dell'A.O.R.N. A. Cardarelli che hanno rappresentato alla U.O.C Gestione Servizi Informativi, attraverso il Servizio di Ingegneria Clinica, la necessità di operare come se fossero connessi direttamente alla rete aziendale dalla loro sede remota (ad es. per utilizzo e monitoraggio dei propri applicativi, verifica di funzionamento ed aggiornamento di apparecchiature elettromedicali). L' accesso in VPN dell'utenza in questa modalità viene gestito centralmente dal gestore della rete; gli utenti connessi tramite opportuna autenticazione, vengono mappati su una classe di rete dedicata e possono raggiungere solo i sistemi indicati e solo per i servizi richiesti. Tutti gli accessi VPN sia on demand che site to site dovranno essere effettuati solo attraverso l'infrastruttura aziendale; non dovranno essere installati appliance o router o altri dispositivi diversi da quelli in nostra dotazione.

6. Conclusioni

Le tecnologie biomedicali ed informative consentono ora di erogare prestazioni sanitarie sempre più efficaci, attendibili e sicure, perché basate su dati, informazioni e documenti accurati, dettagliati e precisi, che possono essere resi disponibili e condivisi tra tutti gli attori del Servizio Sanitario in condizione di Business Continuity. L'attivazione e la fruizione di queste tecnologie complesse, in particolare se inserite in un sistema informativo, richiedono delle condizioni abilitanti che non sono solo tecnologiche ma anche organizzative che devono prevedere il coinvolgimento delle professionalità sanitarie o infermieristiche, delle ingegnerie cliniche e dei sistemi informativi aziendali. Il fallimento, l'inefficienza, l'inefficacia o l'improduttività sono rischi reali poiché tali progetti nascondo molteplici e grosse criticità, complicazioni e problematiche, delle quali si deve avere piena conoscenza e consapevolezza già nella fasi di progettazione ed installazione, al fine di poterle risolvere, riducendo, il più possibile a zero, il rischio di danni ed oneri.