

Il sistema informativo ospedaliero

Privacy nell'utilizzo dei sistemi informatici

ing. Michele Bava PhD
PO Informatica, Telefonia e DPO
Ufficio Sistema Informativo
SC Ingegneria Clinica, Informatica e Approvvigionamenti
IRCCS materno-infantile "Burlo Garofolo"

GDPR e nuovo quadro normativo

- “Vecchio” Codice Privacy D.Lgs. 196/03
- GDPR - Regolamento Generale sulla Protezione dei Dati n. 2016/679
- “Nuovo” D. Lgs. 101/18 (10 agosto 2018) - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679

GDPR

Rispetto a precedente normativa

INVARIATI O VARIATI MARGINALMENTE

- Definizione di dato personale / dato sensibile
 - Definizione di trattamento
 - Titolare del trattamento
 - Principi relativi al trattamento di dati Liceità del trattamento (pertinenza, non eccedenza)
- Obbligo di informativa
- Obbligo di consenso
- Protezione delle sole persone fisiche

GDPR

Rispetto a precedente normativa

NOVITA' DEL REGOLAMENTO

- **Accountability del titolare** - Privacy by design
- **Registro dei trattamenti**
- **Valutazione dei rischi**
- Adozione di misure tecniche e organizzative **adeguate** - **Data breach**
- Certificazione dei trattamenti
- **Valutazione d'impatto**
- Durata del trattamento
- Data Protection Officer (DPO)
- **Responsabilità solidale di titolare e responsabile** - Entità delle sanzioni

Regolamento Informatico

3.2 ATTIVITA' DI GESTIONE, SICUREZZA E CONTROLLO	6
CONDUZIONE DEI SISTEMI INFORMATIVI E VIGILANZA	6
OBBLIGO DI SEGNALAZIONE	6
CONTROLLI	6
ORARI DI SERVIZIO	7
SANZIONI	7
3.3 GESTIONE DEGLI STRUMENTI E DELLE RISORSE AZIENDALI.....	8
UTILIZZI CONSENTITI DELLE RISORSE INFORMATICHE AZIENDALI	8
GESTIONE DELLE CREDENZIALI DI ACCESSO	8
CONFIGURAZIONI DI SISTEMA	9
INSTALLAZIONE DI HARDWARE O SOFTWARE	9
SUPPORTI MAGNETICI / OTTICI / A STATO SOLIDO.....	10
GESTIONE DELLE CONNESSIONI ALLE RISORSE LOCALI DELL'ISTITUTO	10
PERMESSI DI ACCESSO ALLE RISORSE LOCALI DELL'ISTITUTO.....	11
UTILIZZO DELLE RISORSE DEL SERVER DI DOMINIO E OBBLIGO DI «BACKUP» DEI DATI.....	11
3.4 UTILIZZO DELLA RETE INTERNET E DEI RELATIVI SERVIZI	12
CONNESSIONE AD INTERNET	12
NAVIGAZIONE INTERNET.....	12
SERVIZI INTERNET	13
3.5 UTILIZZO DELLA POSTA ELETTRONICA.....	13
UTILIZZI CONSENTITI	13
CONTENUTO DEI MESSAGGI.....	14
CONFIDENZIALITÀ DELLA POSTA ELETTRONICA	14
REGOLE COMPORTAMENTALI PER L'UTILIZZO DELLA POSTA ELETTRONICA	14

Regolamento Informatico

SANZIONI

1. Tutti i collegamenti tra apparati e sistemi interni o ad apparati e sistemi esterni NON espressamente autorizzati dall'USI e che verranno rilevati saranno considerati come tentativi di intrusione alla rete telematica dell'Istituto e quindi considerati, secondo l'art. 615 CP «accessi abusivi ad un sistema informatico e telematico».
2. In caso di violazione accertata del presente regolamento, al dipendente si applicano le disposizioni vigenti di carattere disciplinare o valutativo.
3. L'eventuale danno arrecato ai sistemi informatici e telematici dell'Istituto, dovuto ad una navigazione su siti impropri, è da attribuirsi all'utenza connessa ed autenticata al momento dell'insorgenza del danno stesso.
4. Le violazioni normative anche di carattere penale saranno segnalate e perseguite con le azioni civili e penali consentite presso le Autorità competenti.
5. Le apposizioni di firme elettroniche o digitali, nonché l'utilizzo di sistemi e servizi informatici di qualunque tipo, o la paternità di mail e documenti creati, modificati, inviati, ecc... sono attribuibili all'utenza connessa ed autenticata nel momento in cui insorge o viene rilevato l'eventuale problema.

Reati informatici e telematici

- Modifiche al Codice Penale al fine di tutelare la proprietà dei dati informatizzati
- La Legge 547/93 ha introdotto la normativa sui crimini informatici
 - Art. 615 ter “accesso abusivo ad un sistema informatico o telematico”
 - Art. 615 quater “detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici”
 - Art. 615 quinquies “diffusione di programmi diretti a danneggiare o interrompere un sistema informatico”

Reati informatici e telematici

- La Legge 547/93 ha introdotto la normativa sui crimini informatici
 - Art. 616 violazione della corrispondenza “anche per via telematica”
 - Art. 617 quater “intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche”
 - Art. 640 ter “frode informatica”

Sicurezza e Privacy

- Sicurezza / Security (problemi con i virus, con le email “strane”, con la protezione dei dati informatici, con le password, ecc...) -> Ufficio Sistema Informativo / Amministratori di Sistema / AgID
- Privacy (consensi, problemi con la privacy, con il rispetto della normativa, ecc...) -> DPO, Responsabile Privacy, Gruppo Multidisciplinare Privacy / Garante per la Protezione dei dati

helpdesk@burlo.trieste.it

DPO e Gruppo

Multidisciplinare Privacy

- Sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità
- Collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA)
- Informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati
- Cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento
- Supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento

dpo@burlo.trieste.it