

**REGISTRO DELLE ATTIVITA’ DI TRATTAMENTO**

***ex* art. 30 REG. EU. 2016/679**

**Studio XXXXXXXXXX**

**XXXXXX**

**Sede: XXXXXX**

**Documento formato da 47 pag.**

**Sommario**

[SCOPO DEL DOCUMENTO 3](#_Toc1643227)

[ORGANIGRAMMA DELLA SICUREZZA DEI TRATTAMENTI 4](#_Toc1643228)

[DATI DI CONTATTO DEL TITOLARE 5](#_Toc1643229)

[FINALITÀ DEL TRATTAMENTO E BASI GIURIDICHE 5](#_Toc1643230)

[CATEGORIE DI SOGGETTI INTERESSATI E CATEGORIE DI DATI PERSONALI TRATTATI DALLO STUDIO 7](#_Toc1643231)

[DESTINATARI A CUI I DATI SONO COMUNICATI 8](#_Toc1643232)

[REGISTRI DELLE ATTIVITA’ DI TRATTAMENTO DATI PERSONALI 9](#_Toc1643233)

[REGISTRO PARTNERS 9](#_Toc1643234)

[REGISTRO CLIENTI 12](#_Toc1643235)

[MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE 15](file:///\\SERVER01\Dati\SCAMBIO\Moduli%20privacy%20consigliati%20dalla%20CAO\3_REGISTRO%20TRATTAMENTO-REV.docx#_Toc1643236)

[DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE: 16](#_Toc1643237)

[INDIVIDUAZIONE E VALUTAZIONE DEI RISCHI 19](#_Toc1643238)

[INDIVIDUAZIONE E VALUTAZIONE DEI RISCHI 25](#_Toc1643239)

[REGOLE PER LA GESTIONE DELLE PASSWORD 30](#_Toc1643240)

[REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICI/INFORMATICI 31](#_Toc1643241)

[REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS 33](#_Toc1643242)

[INCIDENT RESPONSE E RIPRISTINO 35](#_Toc1643243)

[ISTRUZIONI OPERATIVE: DATA BREACH 37](#_Toc1643244)

[REGOLAMENTO PER L’UTILIZZO DI INTERNET 40](#_Toc1643245)

[PIANO PER LA FORMAZIONE E RESPONSABILITÀ 44](#_Toc1643246)

[CONCLUSIONI 45](#_Toc1643247)

[NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DI DATI PERSONALI 46](#_Toc1643248)

[REVISIONI ED EMISSIONE 46](#_Toc1643249)

# SCOPO DEL DOCUMENTO

Il presente documento individua le finalità del trattamento dati all’interno dello Studio, le categorie dei soggetti interessati, dei dati personali coinvolti e dei destinatari a cui i dati personali sono stati o saranno comunicati. Obiettivo del presente documento, inoltre, è quello di descrivere le misure di sicurezza tecniche e organizzative predisposte all’interno dello Studio con la finalità di eliminare i rischi di distruzione o perdita dei dati, di accesso da parte di soggetti non autorizzati, il trattamento non consentito o non conforme alle finalità di raccolta.

Il sistema descritto nel presente documento deve ritenersi sicuro in quanto intende garantire la disponibilità, l’integrità e l’autenticità, nonché la riservatezza dell’informazione e dei servizi per il trattamento, attraverso l’attribuzione di specifici incarichi, la certificazione delle fonti di provenienza dei dati e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

La stesura del presente documento è aderente alle seguenti linee guida:

* analisi dello stato dell’organizzazione attraverso l’identificazione e distinzione delle responsabilità delle figure soggettive coinvolte nel trattamento; l’identificazione, l’inventario e l’analisi dell’hardware, del software e delle banche dati;
* individuazione e la valutazione del rischio;
* individuazione delle misure preventive e correttive;
* individuazione di istruzioni agli incaricati e la previsione di un programma formativo.

Il presente documento ‒ e, più in generale, il trattamento dei dati personali dei pazienti ‒ viene realizzato nel pieno rispetto e secondo le coordinate sancite nel Reg. UE 2016/679 (oltreché nel D.lgs. 196/03).

# ORGANIGRAMMA DELLA SICUREZZA DEI TRATTAMENTI

**TITOLARE DEL**

**TRATTAMENTO**

**XXXXXXX**

**RESPONSABILI ESTERNI DEL TRATTAMENTO**

* **XXXXX**

**(Studio odontotecnico)**

* [**Studio commerciale e tributa**](https://www.odcec.roma.it/index.php?option=com_wbmalbo&Itemid=433)**rio**

**(Studio commercialista)**

**ALTRI CONSULENTI:**

**Alter Ingegneria S.r.l (consulente strutture sanitarie)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ADDETTI AL TRATTAMENTO**

* **XXXXX(collaboratrice)**
* **XXXXX (collaboratrice)**

**CUSTODE CREDENZIALI**

**XXXXXXXXXX**

Il titolare del trattamento, come si evince dal grafico, è lo Studio XXXXX, su cui gravano le responsabilità *ex* art. 24 Reg. UE 2016/679 per il trattamento dei dati effettuato direttamente o tramite altre persone per suo conto.

# DATI DI CONTATTO DEL TITOLARE

Il Titolare è contattabile ai seguenti recapiti:

Picture 242 a mezzo posta all’indirizzo della struttura: XXXXXXX;

Picture 242 tramite posta elettronica all’indirizzo mail: XXXXXX;

Picture 242 telefono: XXXXXX.

# FINALITÀ DEL TRATTAMENTO E BASI GIURIDICHE

Lo Studio XXXXXXXX Dott. XXXXXX utilizza i dati personali dei propri pazienti per le seguenti ed esclusive finalità:

1. attività di diagnosi, assistenza e terapia sanitaria, ivi compresi servizi diagnostici, programmi terapeutici e qualsivoglia altro servizio sanitario erogato dallo Studio, compresa l’attività amministrativa e di gestione operativa legata ai servizi forniti;
2. attività legate alla fornitura di altri beni o servizi all'interessato (dati trattati da soggetti terzi o da collaboratori/consulenti), per l’erogazione del servizio sanitario richiesto (es. fornitura di ausili e protesi).
3. attività di trasmissione/comunicazione dei dati agli enti competenti, come previsto obbligatoriamente da norme e regolamenti – finalizzate a ottemperare agli adempimenti da essi derivanti, di natura amministrativa, fiscale, burocratica, legale, in quanto connesse alle prestazioni sanitarie erogate;
4. **attività di comunicazione finalizzate a promemoria per gli appuntamenti ai pazienti (via SMS)**;
5. **attività di comunicazione a scopo informativo/promemoria per la visita d’igiene o odontoiatrica (contatto telefonico).**

La base giuridica che legittima il trattamento è, rispettivamente:

* per le lettere a) e b) l’esecuzione di una prestazione sanitaria con un professionista;
* per la lettera c) l’adempimento di obblighi legali;
* per la lettera d) ed e) il **consenso espresso per specifiche finalità**.

# CATEGORIE DI SOGGETTI INTERESSATI E CATEGORIE DI DATI PERSONALI TRATTATI DALLO STUDIO

I soggetti interessati al trattamento sono prevalentemente i pazienti dello Studio XXXXXXX Dott. XXXXX; nel caso in cui un nuovo paziente ci contatti telefonicamente per fissare un appuntamento, i dati richiesti dal personale di segreteria ‒ previa richiesta di consenso al trattamento prestato oralmente - sono:

* nome, cognome;
* numero di telefono, per contattare il paziente ove ci fosse la necessità di modificare il giorno o lorario dell’appuntamento.

Il paziente può chiamare lo Studio attraverso il numero XXXX; il numero di telefono viene custodito dal dottore, che ha il compito di rispondere alle esigenze e domande del cliente, eventualmente consultando un odontoiatra ove lo ritenesse necessario.

Una volta arrivato in sede, il paziente è invitato a compilare la scheda anamnestica per ricostruire la propria anamnesi; gli sono richieste, dunque, informazioni relative al proprio stato di salute.

Per l’emissione di fattura sarà poi necessario anche avere altri dati, tra i quali l’indirizzo di residenza ed il codice fiscale.

# DESTINATARI A CUI I DATI SONO COMUNICATI

I dati personali dei propri pazienti non vengono comunicati e diffusi all’esterno dello Studio; eccezionalmente, e ove ci fosse la necessità, i dati vengono comunicati ai Responsabili del Trattamento esterni indicati nella precedente tabella ed esclusivamente per le finalità terapeutiche e sanitarie connesse alla prestazione richiesta dal paziente (laboratori, ecc.) o per ragioni fiscali (commercialista).

# REGISTRI DELLE ATTIVITA’ DI TRATTAMENTO DATI PERSONALI

Ai sensi dell’art. 30 del GDPR 2016/679



## REGISTRO PARTNERS

Il presente registro è una rappresentazione dell’organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell’art. 30 de GDPR, il Registro riporta le seguenti informazioni:

* + Dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
  + **Finalità del trattamento**, ovvero le finalità per le quali sono trattati tali dati;
  + Categorie di interessati;
  + Categorie di dati personali;
  + Categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  + Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale;
  + Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  + Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

|  |  |  |
| --- | --- | --- |
| **TITOLARE DEL TRATTAMENTO DATI** | **Ragione sociale** | Studio XXXX Dott. XXXXX |
| **P. Iva** | XXXXXX |
| **E-mail** | XXXXX |
| **Pec** |  |
| **N° telefono** | XXXXX |

**TRATTAMENTO: GESTIONE DEI PARTNERS (CONTRATTI, ORDINI, ARRIVI, FATTURE)**

|  |  |
| --- | --- |
| **Struttura** |  |

|  |  |
| --- | --- |
| **Personale coinvolto** | |
| **Persone autorizzate** | Titolare del trattamento  Personale autorizzato al trattamento |
| **Partner** | Responsabile esterno, commercialista |

|  |  |
| --- | --- |
| **Processo di trattamento** | |
| **Descrizione** | Gestore dei contratti di fornitura |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Contratto |
| **Finalità del trattamento** | Gestione del contenzioso (contratti, ordini, arrivi, fatture) Adempimento di obblighi fiscali o contabili  Elaborazione, stampa, imbustamento e spedizione delle fatture Gestione dei fornitori (contratti, ordini, arrivi, fatture) |
| **Tipo di dati personali** | Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)  Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)  Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo  privato, indirizzo di lavoro) |
| **Categorie di interessati** | Partners |
| **Categorie di destinatari** | Consulenti e liberi professionisti anche in forma associata Persone autorizzate  Imprese terze |
| **Informativa** | Si |
| **Consenso** | No |
| **Profilazione** | No |
| **Dati particolari** | No |
| **Frequenza trattamento** | Mensile |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per ulteriori dieci anni dal termine del rapporto lavorativo, salvo differenti valutazioni in  relazione a potenziali controversie. |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | No |

**MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE**

|  |  |
| --- | --- |
| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
| **Strumenti** | Cartelle digitali  Archivi cartacei conservati in scaffalature |
| **Archiviazione** | Archivio |
| **Strutture informatiche di backup** | |

|  |  |  |
| --- | --- | --- |
| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Poco probabile | Limitate | Medio-basso |

* Sono definiti i ruoli e le responsabilità.
* E' applicata una gestione della password degli utenti.
* Sono utilizzati software antivirus e anti intrusione.
* I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili.
* Viene eseguita opportuna manutenzione.

REGISTRI DELLE ATTIVITA’ DI TRATTAMENTO DATI PERSONALI

Ai sensi dell’art. 30 del GDPR 2016/679



## REGISTRO CLIENTI

Il presente registro è una rappresentazione dell’organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell’art. 30 de GDPR, il Registro riporta le seguenti informazioni:

* + Dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
  + **Finalità del trattamento**, ovvero le finalità per le quali sono trattati tali dati;
  + Categorie di interessati;
  + Categorie di dati personali;
  + Categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  + Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale;
  + Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  + Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

|  |  |  |
| --- | --- | --- |
| **TITOLARE DEL TRATTAMENTO DATI** | **Ragione sociale** | XXXXX |
| **P. Iva** | XXXXX |
| **E-mail** | XXXXXX |
| **Pec** |  |
| **N° telefono** | XXXXXX |

**TRATTAMENTO: TRATTAMENTO DATI PAZIENTI**

|  |  |
| --- | --- |
| **Struttura** |  |

|  |  |
| --- | --- |
| **Personale coinvolto** | |
| **Persone autorizzate** | Titolare del trattamento  Personale autorizzato al trattamento |
| **Fornitori** | Responsabile esterno, commercialista  Responsabile esterno, odontotecnico |

|  |  |
| --- | --- |
| **Processo di trattamento** | |
| **Descrizione** | Anagrafica, gestione dei client, anamnesi, esami |
| **Base giuridica per il trattamento per dati comuni (art. 6 GDPR)** | Consenso  Contratto Legge |
| **Base giuridica per il trattamento per dati particolari (art. 9 GDPR)** | Consenso  Contratto  Legge |
| **Finalità del trattamento** | Assistenza e terapia sanitaria  Elaborazione, stampa, imbustamento e spedizione delle fatture Adempimento di obblighi fiscali o contabili  Gestione della clientela (contratti, ordini, spedizioni e fatture)  Promemoria visita  Visita di controllo  Marketing per servizi del titolare |
| **Tipo di dati personali** | Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)  Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)  Nominativo, indirizzo o altri elementi di identificazione personale  (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)  Dati sanitari (stato di salute, assunzione di farmaci)  Dati biometrici |
| **Categorie di interessati** | Clienti ed utenti Consumatori |
| **Categorie di destinatari** | Consulenti e liberi professionisti anche in forma associata Datore di lavoro  Persone autorizzate |
| **Informativa** | Si |
| **Consenso** | Si |
| **Profilazione** | No |
| **Dati particolari** | Si |
| **Frequenza trattamento** | Giornaliera |
| **Termine cancellazione dati** | I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto contrattuale professionale posto in essere e per i successivi dieci anni dalla data di acquisizione degli stessi, in ogni caso saranno rispettate le tempistiche obbligatorie ai sensi di legge e regolamenti vigenti. |
| **Trasferimento dati (paesi terzi)** | No |
| **Autorizzazione del Garante** | Non presente |

|  |  |
| --- | --- |
| **Modalità di elaborazione dati: Mista - elettronica e cartacea** | |
| **Strumenti** | Software gestionale Cartelle digitali  Cartelle cartacee |
| **Archiviazione** | Scaffalature |
| **Strutture informatiche di archiviazione** | |
|  | Struttura interna |
| Sede di riferimento |  |
| Personale con diritti di accesso | Titolare del trattamento  Personale autorizzato al trattamento Tecnico informatico |
| **Strutture informatiche di backup** | |
|  | Struttura interna |
| Sede di riferimento | XXXXXXXX |
| Frequenza di backup |  |
| Tempo di storicizzazione |  |
| Personale con diritti di accesso | Personale autorizzato al trattamento |

|  |  |  |
| --- | --- | --- |
| **VALUTAZIONE DEL LIVELLO DI RISCHIO** | | |
| **PROBABILITÀ** | **CONSEGUENZE** | **LIVELLO DI RISCHIO** |
| Probabile | Gravi | Rilevante |

* Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati.
* Dispositivi antincendio.
* È applicata una gestione della password degli utenti.
* È applicata una procedura per la gestione degli accessi.
* È presenta una politica per la sicurezza e la protezione dei dati.
* Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.
* Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi.
* Le procedure sono riesaminate con cadenza predefinita.
* L'impianto elettrico è certificato ed a norma.
* Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee.
* Sistemi di allarme e di sorveglianza anti-intrusione.
* Sono applicate regole per la gestione delle password.
* Sono definiti i ruoli e le responsabilità.
* Sono stabiliti programmi di formazione e sensibilizzazione.
* Sono utilizzati software antivirus e anti intrusione.
* Viene eseguita opportuna manutenzione.

# MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

## DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE:

INVENTARIO DEI COMPUTER, DEI PROGRAMMI E DELLE BANCHE DATI

(elettroniche e/o su carta)

1. *Identificazione e inventario dei computer*

|  |  |  |
| --- | --- | --- |
| **Posizione dei computer** | **Tipologia (fisso o portatile)** | **Sistema Operativo Utilizzato** |
| UFFICIO | PORTATILE | WINDOWS 10 |
| SALA OPERATIVA | FISSO | WINDOWS 10 |

1. Identificazione, inventario ed analisi dei programmi utilizzati nello Studio:

|  |  |
| --- | --- |
| **Programma** (contabilità, gestionale, gestione del personale…) | **Tipo di trattamento effettuato** |
| Software gestionale | Database per radiografie e fotografie |

1. Identificazione, inventario ed analisi dei supporti cartacei

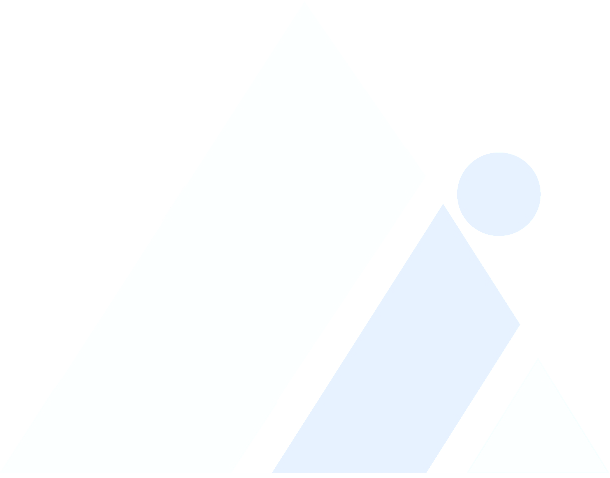
|  |  |  |
| --- | --- | --- |
| **Tipo di supporto** | **Finalità del trattamento** | **Luogo di conservazione** |
| Cartelle anamnestiche pazienti | Gestione medica dei pazienti | Armadio (v. planimetria) |
| Dati fornitori (fatture etc.) | Gestione dei fornitori | Armadio (v. planimetria) |
| Dati del personale (contratti di lavoro, buste paga, documenti..) | Gestione amministrativa | Armadio (v. planimetria) |

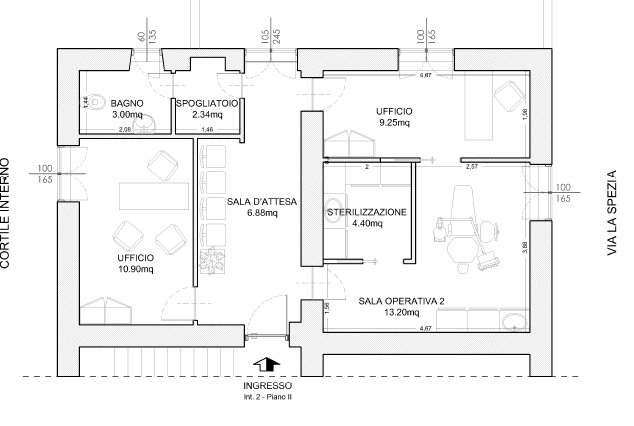
1. *Identificazione, inventario ed analisi dei programmi utilizzati nello Studio:*

|  |  |
| --- | --- |
| **Programma** (contabilità, gestionale, gestione del personale…) | **Tipo di trattamento effettuato** |
| GOOGLE CALENDAR | Organizzazione degli appuntamenti e delle  cartelle anamnestiche dei pazienti |

1. *Identificazione, inventario delle sedi nelle quali vengono effettuati i trattamenti:*

|  |  |
| --- | --- |
| **Identificativo sede** | **Indirizzo** |
| Sede | **XXXXXX** |

 ELABORATO GRAFICO DELLA PRIVACY



**2** 11

**2** 11

**SERVER**

PC

ARCHIVIO

PC

# INDIVIDUAZIONE E VALUTAZIONE DEI RISCHI

La fase di valutazione dei rischi riguarda sostanzialmente tutti i rischi cui potenzialmente sono esposti i dati personali dei nostri pazienti. Al fine di analizzare e valutare i rischi **si suddivide la fase di analisi in settori specifici di valutazione riferibili ad aree omogenee di rischio** (ad esempio: archivio cartaceo, archivio digitale, back up dati, ecc.). Ovviamente il processo di analisi e valutazione riguarda anche quei rischi che non possono essere ricondotti ad un’unica specifica “non conformità” o non interessano un “unico” aspetto legato alla sicurezza ma potrebbero configurarsi come “trasversali” ed interessare contemporaneamente più aree. Conseguentemente, si provvede alla quantificazione del rischio in termini analitici attraverso la valutazione delle modalità operative (frequenza dei back up dei dati, caratteristiche ignifughe degli archivi, presenza di sistemi antivirus, ecc.) secondo una stima delle probabilità di accadimento e dell’entità del danno.

Ai fini dell’attività di valutazione dei rischi, questi ultimi sono suddivisi in tre macro categorie:

* + Rischi trasversali ed organizzativi: derivanti da criticità connesse all’organizzazione del lavoro e delle mansioni, turni di lavoro, monotonia delle mansioni con azioni meccaniche ripetute e non differenziate, criticità derivanti dall’organizzazione dello Studio.
  + Rischi per la conservazione dei dati (Data Breach) connessi a problematiche strutturali: ovvero tutti quei fattori di rischio che possono compromettere la conservazione dei dati personali dei pazienti (e dei collaboratori). In generale, in questa categoria rientrano tutti quei rischi che possono comportare un grave danno all’immobile in cui è sito l’archivio cartaceo e digitale in cui sono conservate le cartelle anamnestiche e i dati personali di tutti i pazienti. A livello strutturale, dunque, tra questi rischi possono essere classificati il rischio d’incendio, rischio di crollo di parti di struttura, allagamenti, terremoti, esplosioni.
  + Rischi per la conservazione dei dati (Data Breach) connessi a problematiche strumentali/informatiche: in questa categoria sono raggruppati i rischi derivanti dalla possibile rottura, perdita, manomissione di quegli strumenti informatici che consentono di archiviare e conservare i dati personali dei pazienti (personal computer, unità di back up etc.) o intromissione di soggetti esterni nella rete interna dello Studio (da remoto, attraverso la rete Wi-Fi, etc.).

La quantificazione e relativa classificazione dei rischi deriva dalla stima dell’entità dell’esposizione ai rischi e dalla gravità degli effetti e conseguenze; infatti, il rischio può essere visto come il prodotto della Probabilità P di accadimento per la Gravità del Danno D:

R = P x D

L’analisi valutativa effettuata può essere, nel complesso, suddivisa nei seguenti due punti principali:

1. Identificazione di tutti i possibili PERICOLI relativi alla perdita dei dati personali dei pazienti;
2. Valutazione dei RISCHI relativi ad ogni pericolo individuato. Successivamente, per ogni pericolo accertato si procede a:
   1. stimare con quale PROBABILITÀ si possa verificare un evento pericoloso. Il valore di probabilità di accadimento di un determinato evento è espresso, generalmente, in una scala una scala semi quantitativa di valori da 1 a 4 (Tabella1)

|  |  |  |
| --- | --- | --- |
| PROBABILITÀ (P) | VALORE | DEFINIZIONE |
| IMPROBABILE | 1 | L’evento potrebbe in teoria accadere, ma probabilmente non accadrà mai. Non si ha  notizia di data breach in circostanze simili |

POSSIBILE 2

PROBABILE 3

Il data breach potrebbe accadere, ma solo in rare circostanze ed in concomitanza con altre condizioni sfavorevoli

L’evento potrebbe effettivamente accadere. Statisticamente si sono verificate ipotesi di data breach in analoghe circostanze.

L’evento si verifica nella maggioranza dei

MOLTO PROBABILE

4 casi, e si sono verificate ipotesi di data breach in azienda o in aziende similari in analoghe

condizioni.

Tabella 1: Scala di Probabilità di accadimento e criterip er l’attribuzione dei relativi valori.

* 1. Determinare le possibili conseguenze considerando ciò che potrebbe ragionevolmente accadere, e stabilire un’appropriata gravità del DANNO, mediante una scala di valori variabili da 1 a 4 (Tabella2)

|  |  |  |
| --- | --- | --- |
| **DANNO** | **VALORE** | **DEFINIZIONE** |
| LIEVE | 1 | I dati perduti sono altrimenti e facilmente reperibile in altri archivi (digitali o cartacei) e non sono entrati nel possesso di soggetti non legittimati |
| MODESTO | 2 | Data breach che comporta un momentaneo inutilizzo di dati e richiede un intervento di manutenzione per il ripristino del possesso degli stessi |
| GRAVE | 3 | Data breach che potrebbe causare effetti difficilmente reversibili, sia per il recupero dei dati che per l’entrata nel possesso di soggetti terzi non autorizzati; |
| GRAVISSIMO | 4 | Data breach che comporta la perdita definitiva di gran parte dei dati conservati e/o entrati nel possesso di soggetti non autorizzati. |

Tabella 1: Scala di Gravità del danno e criteri per l’attribuzione dei relativi valori.

3) Valutare l’entità del RISCHIO in base al prodotto dei due precedenti fattori tramite l’utilizzo della MATRICE DEI RISCHI (Tabella 3).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| MATRICE DEI RISCHI | | | | | | |
| GRAVISSIMO | DANNO | *4* | 4 | 8 | 12 | 16 |
| GRAVE | *3* | 3 | 6 | 9 | 12 |
| MODESTO | *2* | 2 | 4 | 6 | 8 |
| LIEVE | *1* | 1 | 2 | 3 | 4 |
|  | | | 1 | 2 | 3 | 4 |
| PROBABILITÀ | | | |
| IMPROBABILE | POSSIBILE | PROBABILE | MOLTO PROBABILE |

Tabella 3: La matrice dei rischi consente la valutazione dell’entità del rischio a partire dalla stima del danno atteso e la probabilità del suo verificarsi.

I rischi che possono provocare i danni più gravi occupano in tale matrice le caselle in alto a destra (probabilità elevata, danno gravissimo), quelli minori le posizioni più prossime all’origine degli assi (danno lieve, probabilità trascurabile). Il punto di partenza per la definizione delle prioritàà e la programmazione temporale degli interventi di protezione e prevenzione da adottare. La valutazione numerica del livello del RISCHIO comporta l’attuazione di misure di prevenzione e protezione in relazione alla valutazione dei rischi. Questa permette di individuare una corrispondente scala di prioritàà degli interventi da attuare o porre in essere al fine di ridurre in modo sensibile il livello del rischio (Tabella 4).

L’intervento previsto è da realizzare con tempestività e comunque nei tempi tecnici strettamente necessari ad approvare le azioni correttive e il budget per i necessari e relativi investimenti.

ELEVATO

(12 ≤ R ≤ 16)

Azioni correttive Immediate.

PRIORITÀ DI INTERVENTO

CLASSE DI

RISCHIO

NOTEVOLE

(6 ≤ R ≤ 9)

Azioni correttive da programmare con urgenza.

L’intervento previsto è da realizzare in tempi relativamente brevi anche successivamente a quelli stimati con priorità alta.

Azioni migliorative da valutare in fase di programmazione.

ACCETTABILE

(3 ≤ R ≤ 4)

Azioni correttive da programmare a medio termine.

Intervento da inserire in un programma a medio termine, o da

realizzare anche in tempi più ristretti qualora sia possibile attuarlo unitamente ad altri interventi più urgenti.

BASSO

(1 ≤ R ≤ 2)

**Tabella 4:** Priorità degli interventi in relazione alla valutazione numerica del livello del rischio.

## INDIVIDUAZIONE E VALUTAZIONE DEI RISCHI

Nella tabella che segue vengono analizzati i principali fattori di rischio cui sono esposti i dati personali dei pazienti; i rischi sono suddivisi a seconda dell’ambito di provenienza da noi classificata nelle seguenti tre categorie:

* Risorse umane;
* Rete informatica;
* Trasmissione informazioni.

Per ogni pericolo individuato, viene stimata la probabilità di accadimento e generata la specifica matrice di rischio. In base alla valutazione numerica del rischio stabilito vengono individuate le misure adottate.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Risorsa*** | ***Fattore di rischio*** | | | ***R*** | ***Misura adottata/adottanda*** |
|  |  | | |  |  |
| Risorse umane | 1.Turn-over (posizione scoperta soprattutto per il personale posto  all’ingresso) | | | **1** | **Ufficio privato con accesso esclusivamente a personale autorizzato.** |
| 2. Allontanamento dalla propria postazione | | | **3** | **Predisposizione di linee guida per il personale incaricato al trattamento dei dati personali nell’eventualità di allontanamento della persona autorizzata.** |
| 3. Ignoranza procedurale | | | **3** | **Formazione del personale addetto attraverso corsi specifici in materia di privacy / Descrizione delle linee guida cui deve attenersi il dipendente o il collaboratore nell’apposito modulo di incarico al trattamento dei dati personali.** |
| Risorse tecnologiche | 4. Guasto tecnologico | | | **6** | **Manutenzione e aggiornamento affidati ad un consulente tecnico esterno** |
| 5. Danneggiamento | | | **2** | **Manutenzione e aggiornamento affidati ad un consulente tecnico esterno** |
| 6. Incendio | | | **2** | **Prevenzione e protezione antincendio, manutenzione degli estintori e dei sistemi antincendio.** |
| 7. Uso illegittimo | | | **4** | **Formazione e aggiornamento personale + sistemi di accertamento e sanzionatori.** |
| 8. Virus | | | **8** | **Sistema operativo WINDOWS 10**  **con firewall WINDOWS DEFENDER e antivirus AVIRA.** |
| 9. Impossibilità d’uso | | | **2** | **Aggiornamento hardware e software.** |
| 10. Obsolescenza | | | **2** | **Aggiornamento hardware e software, acquisto di nuovi computers in caso di obsolescenza.** |
| 11. Copia abusiva | | | **3** | **Responsabilizzazione degli incaricati al trattamento, attraverso la sottoscrizione di apposita scrittura privata.** |
| 12. Validità licenza d’uso | | | **1** | **Certificazioni aggiornate.** |
| 13. Interruzione d’uso | | | **1** | **Aggiornamento software.** |
| 14. Furto di dati | | | **8** | **Previsione di password all’accensione e all’ingresso nel gestionale, wi-fi protetto con rete dedicata esclusivamente al personale** |
|  | | | | |
| 15. Accesso fraudolento | | | **8** | **Verifica e revisione password assegnate.** |
| 16. Modifica non  controllata | | | **6** | **Chiavi di accesso e sistemi di autorizzazione.** |
| 17. Impossibilità di  ripristino | | | **6** | **Protezione del sistema ed utilizzo di software gestionale** |
|  | | 18. Cancellazione | **6** | | **Protezione del sistema ed utilizzo di software gestionale** |
| 19. Comunicazione illegittima | **6** | | **Formazione e aggiornamento personale + sistemi di accertamento e sanzionatori.** |
| 20. Diffusione illegittima | **6** | | **Formazione e aggiornamento personale + sistemi di accertamento e sanzionatori.** |
| 21. Distruzione | **3** | | **Protezione del sistema ed utilizzo di software gestionale** |
| 22.Mancanza  documentazione | **2** | | **Protezione del sistema ed utilizzo di software gestionale** |
| Trasmission**i** | | 23. Interruzione  trasmissione | **1** | | **Software gestionale aggiornato.** |
| 24. Malfunzionamento | **2** | | **Aggiornamento e contratto assistenza con il fornitore del software gestionale.** |
| 25. Intercettazione volontaria | **3** | | **Sistemi di accertamento e sanzionatori.** |

Alla luce della suesposta valutazione dei rischi per i dati personali dei pazienti, nello Studio xxxxxxxxxxxxx sono state adottate, pertanto, le seguenti misure di sicurezza:

1. Misure strumentaliimage29.png

Obbligo di segretezza delle credenziali

Definizione di credenziali di autenticazione (user e password) personaliimage29.png

Obbligo di diligente custodia delle credenziali con specifiche prescrizioni

Modifica trimestrale delle password relative a programmi contenenti dati personali

image29.pngAntivirus aggiornato semestralmente

Obbligo di custodia di copie di sicurezza

Piano per il ripristino della disponibilità dei dati

Revisione almeno annuale della conservazione dei profili di autorizzazione

Obbligo di impartire istruzioni per il salvataggio dei dati con frequenza almeno settimanale

image29.pngFormazione del personale

image29.pngRevisione annuale della lista degli incaricati

Aggiornamento semestrale dei programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggere i difettiimage29.png

Protezione di strumenti elettronici e dati da trattamenti illeciti e da accessi non consentitiimage29.png

Misure di sicurezza per il trattamento di dati personali affidato a soggetti esterni alle strutture

Istruzioni agli incaricati per assicurare la segretezza e la custodia delle passwordimage29.png

Istruzioni in caso di assenza prolungata o impedimento dell’incaricato

Istruzioni per la custodia e l’uso dei supporti rimovibili al fine di evitare accessi non autorizzati

Istruzioni sui supporti rimovibili contenenti dati sensibili non utilizzati

Idonee procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e del sistema

image29.pngIstruzioni per la custodia dei supporti e per l’installazione dei programmi operativi

del sistema

image29.png Obbligo di non lasciare incustodito ed accessibile lo strumento elettronico

Redazione dei criteri per il ripristino dei dati in seguito a danneggiamento e

distruzione

image29.png Descrizione dei criteri da adottare per garantire le misure minime in caso di

trattamento affidato a soggetti esterni alla struttura

image29.png Redazione degli incarichi al trattamento per gli addetti

image29.png Redazione di nomine a “Responsabile del trattamento” per i collaboratori esterni.

1. Misure Fisiche

image29.png Misure per garantire la protezione delle aree e dei locali rilevanti ai fini della

custodia o della accessibilità

image29.png Vigilanza della sede

image29.png Ingresso controllato

image29.png Sistemi di allarme e/o sorveglianzaimage29.png

Registrazione degli accessi

image29.png Autenticazione degli accessi

image29.pngCustodia in armadi chiusi a chiave

Custodia in armadi blindati e/o ignifughi

Deposito in cassaforteimage29.png

Custodia dei supporti in contenitori sigillatiimage29.png

Dispositivi antincendioimage29.png

Continuità dell’alimentazione elettricaimage29.png

Controllo sull’operato degli addetti

1. Misure logiche

image29.pngControlli aggiornamenti antivirusimage29.png

Controlli periodici circa l’obsolescenza dei computers

image29.pngAnnotazione della fonte dei dati

image29.png Controllo sull’operato degli addetti al trattamento

image29.png Controllo su operato addetti alla manutenzione

image29.pngControllo supporti di manutenzione

I dati informatici vengono salvati sul disco fisso del client ed è in via di predisposizione un sistema di back up esterno o attraverso una piattaforma di cloud computing.

## REGOLE PER LA GESTIONE DELLE PASSWORD

Tutti gli addetti al trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale e password.

User-id e password iniziali sono assegnati dal custode delle password e non possono essere divulgate al personale non addetto.

Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore.

Ogni tre mesi il tecnico informatico provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dal Titolare dello Studio e sono conservate in busta chiusa in un luogo protetto.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dal Titolare del trattamento al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione il Titolare deve ripristinare nuove credenziali di autenticazione che devono essere custodite.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo; per la definizione/gestione della password devono essere rispettate le seguenti regole:

* la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
* deve contenere almeno un carattere alfabetico ed uno numerico;
* non deve contenere più di due caratteri identici consecutivi;
* non deve contenere lo user-id come parte della password;
* la nuova password non deve essere simile alla password precedente;
* la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso alle banche dati contenenti dati personali;
* la password termina dopo sei mesi di inattività;
* la password è segreta e non deve essere comunicata ad altri;
* la password va custodita con diligenza e riservatezza;
* il Titolare deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione esterna.

## REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICI/INFORMATICI

* l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo previa autorizzazione;
* tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione del Titolare del trattamento o di un suo delegato;
* divieto di utilizzare cd o pendrive come mezzo per il backup;
* divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo XX minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro;
* divieto di memorizzazione di archivi con dati personali dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
* divieto di installazione di software di qualsiasi tipo sui personal computer senza apposita autorizzazione da parte del responsabile del trattamento dati;
* divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche;
* L'utilizzo del fax è consentito unicamente agli incaricati del trattamento
* Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
* La stampa di documenti contenenti dati personali è effettuata su stampanti poste in locali ad accesso controllato e presidiate dagli addetti di segreteria/amministrazione
* La manutenzione dei computers, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il Registro del Trattamento ex art. 30 Reg. UE. 2016/679 e di aver adottato le misure minime di sicurezza previste dalla vigente normativa in materia di privacy.

## REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

* divieto di lavorare con diritti di amministratore sui sistemi operativi che supportano la multiutenza;
* limitare lo scambio fra computer di supporti rimovibili (pendrive, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
* controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
* evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di “scaricare“ da internet ogni sorta di file, eseguibile e non. La decisione di “scaricare” può essere presa solo dal responsabile del trattamento;
* disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;
* disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su “chiedi conferma” (il browser avvisa quando uno script cerca di eseguire qualche azione);
* attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
* non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
* non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
* non utilizzare le chat;
* consultare periodicamente il fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
* seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
* conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
* conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
* conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
* conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
* conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

## INCIDENT RESPONSE E RIPRISTINO

Tutti gli addetti al trattamento devono avvisare tempestivamente il Titolare del Trattamento nel caso in cui constatino le seguenti anomalie:

* Modifica e/sparizione di dati;
* Trattamento evidentemente non conforme da parte degli altri incaricati al trattamento o dei Responsabili esterni;
* Irregolarità nell’uso dell’archivio digitale e cartaceo;
* Accesso fraudolento da parte di soggetti esterni all’archivio digitale o cartaceo.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere i dati personali dei pazienti;
3. evitare danni economici;
4. limitare i danni all'immagine dello Studio.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso da internet;
3. spegnere il sistema oggetto dell’incidente. Una volta spento il sistema oggetto dell’incidente non deve più essere riacceso;
4. documentare tutte le operazioni;
5. avvisare l’utenza tecnica.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura del Titolare o, se questi lo ritiene opportuno, del tecnico informatico, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

* se l'incidente riguarda i dati, eseguire una copia bit to bit degli hard disk del sistema compromesso;

1. se l'incidente riguarda il sistema operativo, il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

## ISTRUZIONI OPERATIVE: DATA BREACH



L’art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) impone al titolare del trattamento di notificare all’autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L’obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all’interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l’eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L’eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell’obbligo di notifica, invece, pone l’autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l’esercizio dei poteri previsti dall’art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l’art. 83 GDPR.

Per **“Violazione di dati**” si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall’art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l’incidente di sicurezza in genere, quindi, comprendere che l’incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall’incidente vi sono dati personali.

L’art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all’autorità di controllo di verificare il rispetto della norma.

L’art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E’ importante che sia dimostrabile il momento della scoperta dell’incidente, poiché da quel momento

decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un’alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell’entità dei rischi:

* 1. **Rischio assente**: la notifica al Garante non è obbligatoria.
  2. **Rischio presente**: è necessaria la notifica al Garante.
  3. **Rischio elevato**: In presenza di rischi “elevati”, è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l’acquisizione della chiave di crittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

* coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
* riguardare categorie particolari di dati personali;
* comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
* comportare rischi imminenti e con un’elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
* impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

## REGOLAMENTO PER L’UTILIZZO DI INTERNET

Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso di internet e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Principi generali

Lo Studio XXXXXXX Dott. XXXXX si avvale dell’utilizzo di internet tramite WI-FI protetta da password e firewall, con distinzione di rete dedicata ai pazienti e rete dedicata (esclusivamente) al personale.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, il personale si impegna ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina, nel rispetto dell'integrità dei sistemi e dei dati personali dei pazienti dello Studio e dei propri colleghi, in osservanza delle leggi, norme e obblighi contrattuali.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione. Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore.

Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare è vietato:

usare internet in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da



quanto previsto dal presente regolamento;

image31.png utilizzare internet per scopi incompatibili con l'attività professionistica;

image31.png utilizzare una password a cui non si è autorizzati;

image31.png cedere a terzi codici (USER ID e PASSWORD) di accesso al sistema;

image31.png conseguire l'accesso non autorizzato a risorse internet;

image31.png violare la riservatezza di altri utenti o di terzi;

agire deliberatamente con attività che influenzino negativamente la regolare operatività di internet e ne restringano l'utilizzabilità e le prestazioni per altri utenti;



image31.png fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, banche dati, ecc.);

image31.png installare o eseguire deliberatamente o diffondere su qualunque computer e su internet, programmi

destinati a danneggiare o sovraccaricare i sistemi o internet (p.e. virus, trojans, worms,

spamming della posta elettronica, programmi di file sharing - p2p);

image31.png installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le

attività istituzionali;

image31.png cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi

personali;

image31.png installare deliberatamente componenti hardware non compatibili con le attività istituzionali;

image31.png rimuovere, danneggiare deliberatamente o asportare componenti hardware;

image31.png utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;

image31.png utilizzare le caselle di posta elettronica per scopi personali e/o non connessi all’attività lavorativa;

image31.png utilizzare la posta elettronica con le credenziali di accesso di altri utenti;

image31.png utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi;

image31.png utilizzare l'accesso ad Internet per scopi personali;

image31.png accedere direttamente ad Internet con il proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;

image31.png connettersi ad altre reti senza autorizzazione;

image31.png monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;

image31.png usare l'anonimato o servirsi di risorse che consentano di restare anonimi su internet;

image31.png inserire o cambiare la password se non dopo averla espressamente comunicata al Titolare

ed essere stati espressamente autorizzati;

image31.png abbandonare il posto di lavoro lasciandolo incustodito o accessibile;

Attività consentite

È consentito al Titolare e, su sua delega, al tecnico informatico:

image32.png monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori; creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura;

image32.png rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

image32.png rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

Soggetti che possono avere accesso ad internet

Hanno diritto ad accedere ad internet il personale sanitario, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività professionali per il periodo di collaborazione.

Il titolare del trattamento può regolamentare l'accesso ad internet di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti interni.

# PIANO PER LA FORMAZIONE E RESPONSABILITÀ

Il Titolare del trattamento dei dati personali valuta, per ogni incaricato a cui ha affidato il trattamento dei dati personali, sulla base dell’esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall’evoluzione tecnologica, la pianificazione della relativa formazione in materia di privacy.

La previsione di interventi formativi degli incaricati del trattamento, sia attualmente operativi o neo assunti, ha lo scopo principale di renderli edotti sui rischi che incombono i dati personali conservati presso lo Studio, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

La formazione è programmata già al momento dell’ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali ed in occasione dell’introduzione della nuova normativa in materia di privacy ad opera del Reg. UE 679/2016.

La responsabilità della formazione degli incaricati è a carico del Titolare del Trattamento dei Dati.

Il corso di formazione comprende nozioni sul nuovo codice di protezione dei dati personali, e dei tecnicismi a lui associati, ed è esteso a tutto il personale dipendente.

Il presente documento sarà oggetto di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all’utilizzo di nuovi strumenti informatici o in genere a un mutato assetto organizzativo.

# CONCLUSIONI

A seguito della valutazione dell’entità e della mole dei dati trattati nella struttura si ritiene non necessaria la previsione della figura del un responsabile della protezione dei dati personali (Data Protection Officer).

Sulla base dell’analisi del rischio specifico riscontrato presso la Struttura, i miglioramenti consigliati sono i seguenti:

* Aggiornare tutti i Pc, controllando che siano attivi i software di protezione;
* Prevedere un’unità di back-up dotandosi di apposite unità per la memorizzazione dei dati, anche attraverso la definizione di un contratto con una piattaforma di cloud computing;
* Implementare il piano della formazione per tutto il personale;
* Sottoporre il presente documento ad opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all’utilizzo di nuovi strumenti informatici o in genere a un mutato assetto organizzativo.

Documento redatto il XXXXXXXXX

Il Titolare

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

per presa visione

clip_image001

# NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DI DATI PERSONALI

Ai sensi dell’art. 28 del Regolamento UE 2016/679

Il sottoscritto Dott. XXXXXX in qualità di titolare del trattamento (di seguito il “Titolare”) dei dati ai sensi del GDPR - Reg. UE 2016/679 (di seguito il “GDPR”)

NOMINA

La Società **XXXXXXXXXXX**, Responsabile del trattamento dei dati per il titolare sopraindicato, effettuato presso la sede di XXXXXXXXXXXXXXXX con strumenti elettronici/automatizzati e cartacei, per le attribuzioni, competenze e funzioni assegnate in materia di consulenza ed offerta di servizi alle strutture sanitarie.

In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le istruzioni impartite dal Titolare.

In particolare, il Responsabile si impegna a:

* adottare misure di sicurezza adeguate al rischio dei dati personali;
* garantire che i propri dipendenti/collaboratori abbiano assunto obblighi di riservatezza;
* non ricorrere ad altro Responsabile senza autorizzazione scritta del Titolare e, comunque, imporgli il rispetto delle misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR;
* assistere il Titolare con misure tecniche e organizzative adeguate al fine di dare seguito alle richieste dell’interessato e di garantire la sicurezza dei dati personali, la valutazione sulla protezione dei dati e la consultazione preventiva di competenza del Titolare;
* mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare gli obblighi previsti dal presente atto;
* contribuire alle attività di revisione ed informare il Titolare di eventuali “data breach”, nonché in presenza di istruzione del Titolare contraria alla normativa sulla protezione dei dati personali;
* restituire o cancellare i dati personali al termine del rapporto contrattuale, in conformità con quanto previsto dalla normativa vigente.

L’incarico di Responsabile del trattamento dei dati decade automaticamente alla scadenza o alla revoca dell’incarico affidato.

\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_ Il titolare del trattamento

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

firma per accettazione

# REVISIONI ED EMISSIONE

|  |  |  |
| --- | --- | --- |
| **Revisione** | **Causa della Revisione** | **Data** |
| 00 | Prima Emissione | 05.02.2019  . |
| 01 | Aggiornamento |  |
| 02 |  |  |
| 03 |  |  |