All. A) Istruzioni operative per i soggetti AUTORIZZATI al Trattamento dei dati

Quando si parla di protezione del dato, è necessario pensare non solo al concetto di "Riservatezza", ma soprattutto a quello di "**Sicurezza** del dato", intesa come **integrità**, **esattezza** e **aggiornamento e disponibilità** dello stesso, nonché come **trattamento lecito e conforme** alle finalità della raccolta.

PRINCIPI GENERALI

Per garantire la sicurezza del dato occorre:

1) **Trattare i dati** ai quali ciascun autorizzato ha accesso, sia su supporto cartaceo che informatico, nell'attività a cui ciascun autorizzato è preposto nel rispetto del **principio di liceità, correttezza e trasparenza,** nonché in attuazione**:**

a. del principio di **MINIMIZZAZIONE** dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità di trattamento;
b. del principio di **LIMITAZIONE** delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
c. del principio di **ESATTEZZA**: garantire l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono raccolti e successivamente trattati.

2) **Utilizzare**, per tutta la durata dell'incarico, ed anche successivamente al termine di esso e/o cessazione del rapporto di lavoro, le **informazioni e i dati personali**, in particolare i dati cd. dati particolari (es. dati sullo stato di salute) **con la massima riservatezza** sia nei confronti dell'esterno che all'interno dell'Azienda e non utilizzarli per altri fini. L'utilizzo a fini personali dei dati costituisce un grave illecito e sottopone il singolo agli obblighi previsti dalla normativa in capo al Titolare.

3) Non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione del Titolare o del Designato
.

4) **Astenersi dal comunicare** a terzi e/o diffondere dati e informazioni appresi in occasione dell'espletamento delle proprie attività.

5) Non comunicare e diffondere i dati personali provenienti da banche dati aziendali, in assenza dell'autorizzazione del Titolare o del designato.

6) Richiedere preventivamente l'autorizzazione al designato ogniqualvolta si renda necessario la comunicazione all'esterno dei dati oggetto di trattamento.

7) **Conservare i dati** rispettando le **misure di sicurezza predisposte** dal Titolare e/o dal soggetto designato, garantendone la protezione in ogni attività di trattamento.

8) **Conservare i dati** in una forma che consenta l'identificazione degli interessati **per un periodo di tempo non superiore al conseguimento delle finalità** per le quali sono trattati.

9) **Segnalare** al soggetto designato eventuali circostanze che rendano necessario od opportuno **l'aggiornamento delle predette misure di sicurezza** al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

10) **Non creare banche dati nuove** senza espressa autorizzazione del Titolare o del Designato.

11) Distruggere e rendere illeggibili, prima di cestinarle, eventuali copie di documenti contenenti dati sanitari.

12) **Osservare tutte le misure di protezione e** sicurezza, già in atto o successivamente disposte, atte ad evitare rischi di distruzione, perdita, accesso non autorizzato, o trattamento non consentito dei dati personali, attenendosi, inoltre, nel trattamento dei dati -con o senza l'ausilio di strumenti elettronici, alle ulteriori particolareggiate istruzioni al fine impartite dal delegato.

13) Controllare, nella stesura delle **determinazioni e delle deliberazioni**, alla luce del dei principi contenuti nell'art. 5 del GDPR, che l'inclusione nel testo di dati personali sia realmente necessaria per le finalità proprie di ciascun provvedimento e verificare che nel testo destinato alla pubblicazione non vi siano dati personali idonei a rivelare lo stato di salute.

14) **Partecipare ai corsi formativi** in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Direttore Generale o suo delegato.

ISTRUZIONI OPERATIVE

1) INFORMARE in modo da garantire la trasparenza del dato, pertanto:

- Prima di procedere alla raccolta e al trattamento dei dati è necessario fornire **l'INFORMATIVA** all'interessato, invitando lo stesso a consultare la pagina web aziendale-sezione Privacy, e/o mediante l'affissione della cartellonistica -predisposta dall'Azienda.

• Per i pazienti ricoverati, è necessario fornire la relativa informativa ed acquisire il **consenso** da parte dell'interessato qualora necessario (es. per comunicazione del suo stato di salute a terzi, etc,), avendo cura di inserire il relativo modulo nella cartella clinica quale parte integrante della stessa.

2) ADOTTARE LE OPPORTUNE CAUTELE NEI RAPPORTI CON IL PAZIENTE/UTENTE

- **IDENTIFICARE** gli interessati nell'ambito dell'accesso alle prestazioni, o presentazione di un'istanza o dichiarazione, invitando l'interessato ad esibire un proprio documento di identità.

- **RACCOGLIERE** i dati dell'interessato con la massima cura, verificando l'esattezza dei dati stessi.

- Trattare i dati sanitari ed eventualmente quelli giudiziari contenuti in elenchi, registri o banche dati tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, ove possibile, con tecniche di cifrature o mediante l'utilizzazione di codici identificativi o di altri sistemi, che permettano di identificare gli interessati solo in caso di necessità.

- Garantire il rispetto del **segreto professionale** connesso con la prestazione sanitaria, ed in particolare:
  a) **prevenire**, durante colloqui, prestazioni sanitarie e consegna documentazione sanitaria, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
  b) **rispettare la dignità** dell'interessato in occasione della prestazione professionale e in ogni operazione di trattamento dei dati;
  c) **fornire** notizie a terzi relative allo stato di salute dell'interessato solo in presenza di **specifica autorizzazione** dello stesso.

- Nei **RAPPORTI DI FRONT OFFICE:**
  a. rispettare le **distanze di sicurezza**: per quanto riguarda gli operatori allo sportello (cd. Front-office) deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostare dietro la linea tracciata sul

pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza, ove esistenti;

b. rispettare l'**obbligo di riservatezza e segretezza:** l'autorizzato al trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice sulla privacy;

c. adottare opportune cautele **per la corretta comunicazione dei dati:** la comunicazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato per iscritto.

- Per **TELEFONO:**

Nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati trattati, procedere nel seguente modo:

a) **chiedere l'identità** del chiamante e la motivazione della richiesta;
b) **richiedere** il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
c) **verificare** che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante (ad es. caserma dei carabinieri, …);
d) procedere immediatamente a **richiamare** la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza.

3) COLLABORARE CON IL SOGGETTO DESIGNATO

- **Informare** prontamente il Soggetto Designato di tutte le questioni rilevanti in materia di Privacy, segnalando eventuali criticità.
- Informare il designato e il DPO, qualora si verifichi qualsiasi evento che possa compromettere la sicurezza dei dati personali (anomalie, furti, perdite accidentali dei dati) al fine di attivare, nel caso sia riscontrato un rischio per i diritti e le libertà delle persone fisiche , la procedura aziendale di Data Breach.

4) RISPETTARE LEMISURE DI SICUREZZA

- Rispettare le **misure di sicurezza** adottate dal titolare e dal soggetto Designato, atte a salvaguardare la riservatezza e l'integrità dei dati. In particolare i dati personali oggetto di trattamento devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche ed organizzative adeguate, da trattamenti non autorizzati o illeciti e della perdita, della distruzione o dal danno accidentale, mediante il rispetto delle seguenti misure di sicurezza:

  - **accedere ai dati**, contenuti in archivi cartacei o su supporti informatici, che siano strettamente necessari all'esercizio delle proprie funzioni e competenze, unicamente durante l'orario di espletamento del servizio;
  - **non lasciare incustoditi ed accessibili a terzi**, chiavette o hard disk esterni, fogli, cartelle cliniche, documentazione sanitaria,…;
  - **non lasciare incustoditi ed accessibili a terzi** gli strumenti elettronici (Spegnere elaboratore, porlo in posizione di stand-by, adottare un sistema di oscuramento cd. Scren-saver);
  - **conservare** la documentazione sanitaria (cartacea o su supporti informatici) in archivi (stanze, armadi, schedari, contenitori, …) chiusi a chiave;
  - **utilizzare la parola chiave (password)** composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema, **Si ricorda che la password è personale ,** deve essere mantenuta riservata e deve essere modificata con cadenza almeno trimestrale;
  - Per garantire la corretta conservazione e salvataggio dei file contenenti dati personali di pazienti o altri soggetti è necessario archiviare gli stessi nelle cartelle di rete a disposizione di ogni struttura e non mantenerli su PC;

  - **verificare che il programma antivirus** installato sulle postazioni di lavoro sia sempre attivo ed aggiornato, richiedendo assistenza tecnica qualora si riscontrassero anomalie;
  - richiedere tempestivamente qualora le postazioni di lavoro presentassero **malfunzionamenti o errori** che potrebbero essere causati da virus o altri software indesiderati;
  - **utilizzare** la posta elettronica per scopi di ufficio. Per la spedizione di documentazione sanitaria per posta elettronica si rimanda al punto 6;
  - **non installare** e usare **qualunque software, né utilizzare piattaforme** non previste dall'Azienda senza la previa autorizzazione del Titolare e7o suo delegato;
  - **segnalare all'assistenza tecnica eventuali esigenze di utilizzo o installazione di software** non disponibili sulle postazioni di lavoro in modo che si possa verificare preventivamente la congruità dei sistemi;
  - **non utilizzare supporti removibili** per salvare dati senza la previsione di credenziali di accesso e crittografia.

5) PROTEGGERE IL DATO NELLA CIRCOLAZIONE INTERNA ED ESTERNA

- Consegnare ai vari servizi la documentazione contenente dati sensibili **obbligatoriamente in busta chiusa**.
- Consegnare all'interessato la documentazione in **busta chiusa** con **apposizione del timbro** "*Da aprirsi a cura dell'interessato*".
- Non riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o ricondurre alla patologia.

- **6) PROTEGGERE IL DATO NELL'INVIO DELLA DOCUMENTAZIONE VIA E-MAIL (nota aziendale prot. n. 2676 del 17.02.2020 consultabile sulla Intranet aziendale- Sezione Privacy)**

- Procedere, al momento della compilazione del modulo, **all'identificazione del paziente** attraverso un documento di identità personale valido.
- Verificare, prima dell'invio, **l'avvenuto pagamento del ticket, se dovuto**.
- Controllare che tra i destinatari **non ci siano altri indirizzi** oltre quello del richiedente.
- Spedire, prima del primo invio, **un messaggio di prova** alla casella e-mail indicata dal paziente, attendendo un riscontro positivo da parte dello stesso.

- Procedere alla **compressione del file** contenente il referto impostando la password indicata dal paziente sul modulo. Qualora per ragioni diverse il richiedente non abbia compilato il modulo, la password per decriptare il file non deve essere scritta nell'e-mail di invio, ma comunicata telefonicamente.

- Spedire il file compresso come allegato al messaggio**, avendo cura di non riportare nel testo alcun tipo di dato sanitario.**

- **<u>7</u>) CONSULTAZIONE CARTELLE CLINICHE (nota aziendale prot. n. 2687 del 17.02.2020 consultabile sulla Intranet aziendale- Sezione Privacy)**

Nel caso di richiesta di consultazione di cartelle cliniche presso l'Ufficio Cartelle Cliniche per proseguimento cure/ricerca scientifica, etc.:

- non utilizzare presso l'Ufficio Cartelle Cliniche supporti removibili per salvare la documentazione richiesta, ne' effettuare fotografie della documentazione:
- raccogliere solo i dati necessari per la realizzazione della tesi/pubblicazione/ricerca e non utilizzarli per fini diversi;
- pseudonimizzare i dati raccolti e trattare gli stessi, ai fini della pubblicazione, solo in forma aggregata, attenendosi alle istruzioni previste nel documento "*Deidentificazione;*
- conservare i dati raccolti solo per il tempo necessario per la realizzazione della tesi/pubblicazione/ricerca;
- procedere alla distruzione dei dati raccolti dopo la conclusione della tesi/pubblicazione/ricerca;
- garantire la riservatezza sulle informazioni e sui dati trattati e dei quali sia comunque venuto a conoscenza durante la consultazione.