Procedure di sicurezza da adottare nel trattamento dei dati privati
in ottemperanza al Regolamento UE 2016/679 e D. Lgs. 196/2003

1. La raccolta ed il successivo trattamento dei dati devono sempre avvenire previo consenso dell'interessato:
- rispettare le procedure di raccolta del Consenso Privacy previsto per ciascun'area/servizio;
- verificare sempre la presenza del Consenso Informato sottoscritto.

2. Per procedere al trattamento dei dati sensibili o di categorie particolari è sempre necessario ottenere un consenso in forma scritta da parte dell'interessato, ad esclusione dei seguenti casi:
- quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica dell'interessato e questi non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere: in questo caso il consenso può essere manifestato da chi esercita legalmente la potestà, oppure da un prossimo congiunto, da un familiare o da un convivente;
- quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di una terza persona, diversa dall'interessato.

3. In caso di trattamento congiunto di dati generici e sensibili/giudiziari, il livello di riservatezza da applicare al trattamento deve corrispondere al più elevato: ai dati generici si applicano le stesse misure di sicurezza previste per i dati sensibili e giudiziari.

4. I dati sensibili (o giudiziari) non devono essere comunicati a terzi non autorizzati e non possono in nessun caso essere diffusi; adoperare tutte le necessarie cautele per evitare che questo avvenga:
- controllare sempre l'accesso agli ambienti dove avvengono conversazioni;
- verificare sempre l'identità dell'interlocutore telefonico e condurre la conversazione telefonica in maniera strettamente riservata, evitando che terze persone possano accedere ai contenuti del colloquio;
- evitare di inviare per fax documenti contenenti dati sensibili: nei soli casi (eccezionali), preventivamente autorizzati dall'Interessato e dal Titolare, verificare telefonicamente l'identità del ricevente, contattandolo per telefono prima dell'invio;
- condurre le conversazioni con i genitori in maniera strettamente riservata, in locali destinati a questa funzione ed in assenza di persone estranee;
- effettuare la eventuale comunicazione a terzi di qualunque informazione relativa all'interessato in maniera strettamente riservata: la comunicazione deve avvenire solo da parte di personale autorizzato, sulla base delle proprie competenze, e deve essere diretta a familiari o persone preventivamente autorizzate dall'interessato, verificando precedentemente l'identità del proprio interlocutore;
- verificare che i nominativi degli interessati non siano in nessun caso riconducibili alle informazioni utilizzate o comunicate a terze parti per studi e ricerche: i dati relativi a studi e ricerche devono essere assolutamente anonimi.

5. La documentazione cartacea contenente dati personali deve essere manipolata in modo da evitare che persone non autorizzate accedano alle informazioni contenute:
- i documenti cartacei devono essere prelevati dagli archivi e custoditi esclusivamente a cura degli incaricati per il solo tempo necessario ad effettuare i propri compiti e devono essere immediatamente riposti al termine delle operazioni;
- in assenza di personale autorizzato, la documentazione deve sempre essere chiusa a chiave in armadi o cassetti disposti allo scopo e le chiavi devono essere accessibili ai soli addetti;
- l'accesso ai locali destinati ad archivio è ammesso dopo l'orario di chiusura esclusivamente al Titolare e ai Responsabili/Incaricati designati.

6. La documentazione cartacea contenente dati sensibili (o giudiziari) deve essere manipolata in modo strettamente riservato ed in maniera tale da evitare che persone non autorizzate accedano alle informazioni contenute:
- i documenti cartacei devono essere prelevati dagli archivi e custoditi esclusivamente a cura degli Incaricati per il solo tempo necessario ad effettuare i propri compiti e devono essere immediatamente riposti al termine delle operazioni;
- la compilazione e l'aggiornamento o l'integrazione della documentazione deve avvenire in maniera strettamente riservata, in locali ad accesso controllato e solo ad opera di personale autorizzato;
- la documentazione cartacea non deve essere lasciata in vista o incustodita e non deve risultare accessibile alla vista di terzi non autorizzati, ad esempio, attraverso superfici vetrate;
- la documentazione cartacea deve essere trasportata da un ufficio/area all'altro/a (ad es. dai locali del laboratorio, alla sala accettazione) in contenitori o buste chiusi e anonimi, se in presenza di persone terze non autorizzate e solo ad opera di Incaricati al trattamento;
- ogni altro documento contenente dati sensibili (ad es. cedolini paga) devono essere consegnati agli interessati o a terzi legittimati in busta chiusa;
- il Titolare o un suo incaricato verifica che alla documentazione non accedano mai persone prive di autorizzazione;
- in assenza di personale autorizzato, la documentazione deve sempre essere chiusa a chiave in armadi o cassetti disposti allo scopo e le chiavi devono essere accessibili ai soli addetti incaricati;
- l'accesso ai locali destinati ad archivio è ammesso dopo l'orario di chiusura esclusivamente al Titolare e ai Responsabili/Incaricati designati;
- la documentazione contenente dati sensibili non più utilizzabile per cui non è prevista archiviazione o ne sono scaduti i termini, deve essere distrutta tramite tritacarte, preferibilmente nello stesso locale destinato al trattamento o al più in un locale attiguo.

7. I dati sensibili registrati su supporti esterni devono essere manipolati in modo strettamente riservato ed in maniera tale da evitare che persone non autorizzate accedano alle informazioni contenute:
- eventuali CD, dischi USB e altri supporti di memoria portatili non dovranno essere mai identificati con nominativi degli interessati;
- i supporti esterni utilizzati per le copie di back-up (HD) vanno manipolati con estrema cura per evitare la perdita o la distruzione di dati.

8. L'utilizzo degli strumenti elettronici, attraverso i quali viene effettuato il trattamento di dati personali generici e/o sensibili (o giudiziari), deve essere soggetto alle cautele di seguito specificate:
- l'accesso agli strumenti elettronici e alle base dati (dei PC client, delle apparecchiature elettromedicali e del computer server) deve avvenire tramite il proprio codice di identificazione personale (User Id) e la propria parola chiave (password);
- la parola chiave deve essere composta di un numero di caratteri non inferiore a 8 e deve essere scelta in modo da non contenere riferimenti diretti alla propria persona, quali ad esempio: data di nascita, nome proprio o dei propri figli, ecc;
- la parola chiave è strettamente personale e deve essere tenuta rigorosamente segreta; non deve essere scritta né all'interno dello strumento elettronico né su fogli accessibili a terzi;
- la parola chiave deve essere sostituita con cadenza almeno semestrale a cura dell'incaricato;
- lo strumento elettronico non deve essere mai lasciato incustodito durante una sessione di lavoro: se lo strumento elettronico è acceso e/o se il programma è aperto, l'incaricato non deve allontanarsi dalla postazione e deve evitare che persone non autorizzate possano accedere alle informazioni visibili a schermo o lanciare stampe della documentazione;
- i dati personali, sensibili o giudiziari non devono mai essere inviati per posta elettronica;
- il trasferimento dei dati sensibili in formato elettronico è cifrato o separato: i dati anagrafici sono disgiunti da quelli sanitari.

9. Il Titolare aggiorna periodicamente la validità e l'efficacia delle procedure operative e di sicurezza:
- individua l'ambito di trattamento consentito ai singoli incaricati o alle unità organizzative e lo aggiorna con cadenza minima annuale;

- redige la lista degli incaricati per classi omogenee di incarico dei relativi profili di autorizzazione.

Glossario

titolare	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità de trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
responsabile	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
incaricato	la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile
dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
dato identificativo	dato personale che permette l'identificazione diretta dell'interessato
dato sensibile	dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (articolo 9 Regolamento UE 2016/679.
dato giudiziario	dato personale idoneo a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di in indagato ai sensi degli articoli 60 e 61 del codice di procedura penale
dato anonimo	dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile
interessato	la persona fisica cui si riferiscono i dati personali
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
comunicazione	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
diffusione	il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione
banca di dati	qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti
strumento elettronico	elaboratore, programma per elaboratore o qualunque altro dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento
parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica