Pier Luigi Tucci[1],
Paolo Becherucci[1],
Luciana Biancalani[1],
Elisabetta Cappelli[1],
Andrea Lucca[1],
Valdo Flori[2]

[1] Animatore di formazione della Regione Toscana;
[2] Segretario regionale FIMP Toscana e coordinatore degli animatori pediatri della Regione Toscana

I Pediatri di famiglia toscani e la privacy: cosa avevamo fatto?

Il 24 maggio 2016 è entrato in vigore il Regolamento europeo n. 679/2016 in materia di privacy, detto anche GDPR (*General Data Protection Regulation*). La *ratio* del nuovo Regolamento europeo è quella di garantire la migliore protezione dove esistono maggiori rischi, sia per il numero di dati personali trattati che per la vulnerabilità dei sistemi. I dati sanitari sono considerati molto "sensibili" e quindi da attenzionare particolarmente.

Il Regolamento impone l'adozione di un vero e proprio modello organizzativo per la tutela dei dati con l'introduzione del principio di responsabilità e trasparenza. In caso di problematiche si dovrà dimostrare di aver messo in atto tutte le misure utili e necessarie a minimizzare i rischi.

Gli studi medici, che in precedenza erano già soggetti agli adempimenti per la privacy, sono fortemente interessati dalla nuova normativa europea. Gli obblighi possono essere diversi a secondo della complessità organizzativa della struttura in cui si lavora, ma una rivalutazione delle proprie attività relativamente alla privacy (anche per gli aspetti informatici) si impone a tutti i professionisti.

La Regione Toscana, in accordo con la FIMP, ha inserito nella programmazione formativa dei Pediatri di famiglia (PdF) toscani per l'anno 2018-19 il corso **Gestione della Privacy nell'ambulatorio del Pediatra di Famiglia: un problema o un'opportunità?**

L'obiettivo del corso era di fornire informazioni relativamente agli adempimenti da mettere in atto per ridurre al minimo il rischio di dispersione dei dati sensibili e proporre spunti di riflessione per migliorare la propria organizzazione in relazione alla privacy. Nel corso si sono affrontate le **novità introdotte dal nuovo regolamento europeo per la privacy relativamente agli studi medici, gli adempimenti a secondo della complessità della propria struttura, e la sicurezza relativamente agli aspetti informatici**.

All'inizio del corso è stato consegnato ai partecipanti una Check-List di autovalutazione, da compilare immediatamente e da conservare, al fine di una verifica personale di quale fosse il punto di partenza della attuale gestione degli adempimenti della privacy. Il corso si è svolto nei mesi da novembre 2018 a aprile 2019 e ha interessato la quasi totalità dei PdF toscani. Si è presupposto che i partecipanti avessero già messo in atto alcune misure, pur nella incertezza della normativa al momento vigente (mancavano infatti importanti chiarimenti applicativi da parte del Garante). Le risposte sono state ritirate al termine della giornata formativa.

Sappiamo quanto tutte le novità succedutesi in tema di privacy siano state vissute dai medici con una sorta di fastidio burocratico aggiuntivo, con una possibile sottovalutazione dei rischi connessi ad omissioni o superficialità nella gestione della privacy, specie nella nostra realtà nella quale i bambini, i loro genitori, le nuove e varie situazioni familiari, la presenza di altri soggetti (nonni, parenti, baby sitter …) aumentano la complessità nella gestione della protezione dei dati personali.

RISULTATI

Abbiamo valutato 322 questionari compilati in modo completo su 339 consegnati.

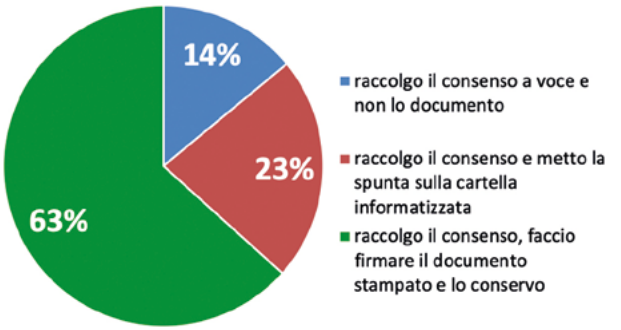
La prima domanda era riferita al ***primo adempimento***

da attuare secondo il regolamento europeo: appendere in sala d'aspetto l'informativa sul trattamento dei dati personali. L'85% dei PdF aveva appeso l'informativa. La complessità dei dati da raccogliere consiglierebbe la predisposizione di una informativa standard, piuttosto che una estemporaneità compilativa: solo il 60% utilizza una versione già predisposta; di questi ultimi solo il 73% utilizza l'informativa standard predisposta dai comuni sistemi informatizzati di gestione dei pazienti.

L'informativa da appendere in sala d'aspetto deve essere dettagliata ed esaustiva e quindi deve essere costruita con attenzione. Alcuni software possono aiutare a compilarla, ma bisogna fare una preventiva ***valutazione dei rischi***, attraverso un'analisi organizzativa della propria struttura professionale. È necessario altresì però fare attenzione a non essere eccessivamente dettagliati; ad esempio, se mettessimo il nome e cognome della segretaria nell'informativa e non scrivessimo più genericamente che i dati potranno essere trattati anche da personale amministrativo adeguatamente formato, al momento che cambiasse la persona i consensi fino ad allora raccolti non sarebbero più validi e quindi dovrebbero essere nuovamente presi!

Predisposta l'informativa prevista dal nuovo regolamento a chi va consegnata? Il fattore tempo ha condizionato le modalità comportamentali dei Pediatri toscani: il 37% lo consegna solo ai nuovi pazienti, il 63% a tutti via via che si presentano. Consegnata l'informativa in forma estesa, oppure una sintesi nella quale si richiama quella esaustiva appesa in sala d'aspetto, il successivo adempimento è l'acquisizione del **consenso** dai genitori o dai tutori del minore; tale adempimento è più complesso rispetto a quanto in precedenza richiesto, e già attuato in modo vario tra regione e regione anche con accordi con l'assessorato alla sanità. Rispetto alla procedura prevista dal regolamento (raccogliere il consenso, farlo firmare e conservarne traccia), attuata dal 63% del nostro campione, troviamo un 15% che si accontenta del solo consenso orale senza registrarlo, con quindi enormi rischi, mentre il 23% raccoglie il consenso sempre per via orale mettendo però la spunta sulla cartella informatizzata, soluzione anche questa che non rispetta il dettato regolamentare (Fig. 1).

Figura 1.
Modalità di raccolta del consenso.



Il regolamento specifica in modo molto dettagliato le caratteristiche dell'informativa, che deve avere forma ***concisa, trasparente, intelligibile per l'interessato e facilmente accessibile***, utilizzando un ***linguaggio chiaro e semplice***, e prevedendo per i minori informative idonee.

L'informativa deve essere data, ***in linea di principio, per iscritto e preferibilmente in formato elettronico*** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se ***sono ammessi "altri mezzi", quindi può essere fornita anche oralmente***, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Quindi, qualsiasi sia la modalità con cui raccogliamo il consenso, dobbiamo essere in grado, in caso di contenziosi, di dimostrare di averlo correttamente fatto e la modalità orale è difficilmente dimostrabile (testimone? Registrazione audio?).

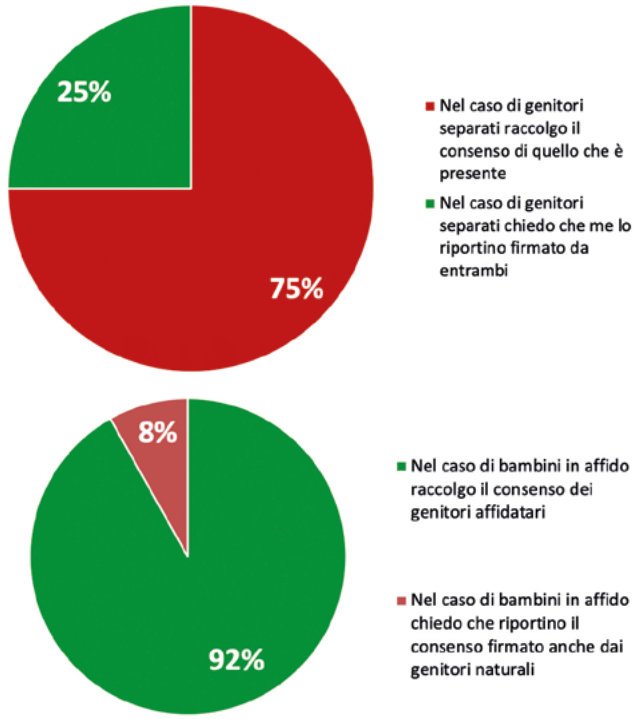
Sarebbe estremamente di aiuto se le Software House che forniscono i gestionali della cartella clinica li implementassero con una modalità di raccolta informatizzata con la possibilità di raccogliere le firme dei genitori tramite una tavoletta, come avviene ad esempio oramai correntemente in banca.

Ma in presenza di bambini i cui genitori sono separati, o che sono in affido, come si comportano i PdF?

Nel caso di genitori separati solo il 25% ritiene indispensabile che il consenso sia firmato da entrambi i genitori, e quindi invitando il genitore che ha accompagnato il bambino a raccogliere la firma dell'altro genitore, a riportare il modulo oppure l'altro genitore a venire in studio.

Figura 2.

Modalità di raccolta del consenso in situazioni particolari.



Nel caso di bambini in affido la quasi totalità reputa sufficiente il consenso dei genitori affidatari.

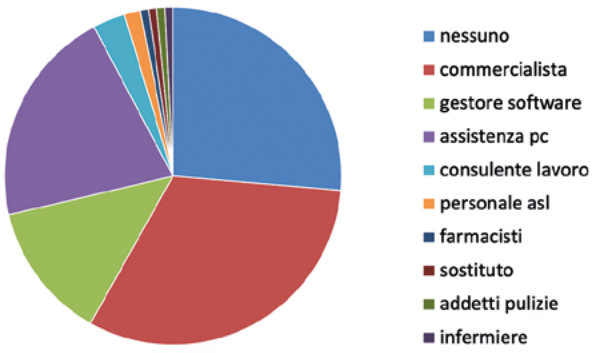
La discussione se fosse obbligatorio far firmare in consenso ad *entrambi* i genitori è stata piuttosto vivace durante gli eventi formativi; il pediatra deve rilevare il consenso dai genitori o da chi ne esercita la responsabilità genitoriale; non c'è alcuna differenza se i genitori sono sposati, separati, divorziati o non coniugati ma riconosciuti legalmente. Il consenso di entrambi i genitori (che esercitano la responsabilità) è necessario solo per gli atti di straordinaria amministrazione che implicano modifiche nei diritti o nella sfera economica del soggetto minore. Per gli atti di ordinaria amministrazione è sufficiente il consenso di un solo genitore, in applicazione del principio generale che gli atti di ordinaria amministrazione possono essere compiuti disgiuntamente da ciascun genitore (art. 320 Codice Civile). In questi casi il consenso dell'altro è considerato implicito. Il consiglio dato dagli esperti al corso è stato di cercare di ***raccogliere il consenso di entrambi (soprattutto in condizioni di possibili contenziosi***, appunto ad esempio separazioni): far firmare il genitore presente, chiedere di far venire anche l'altro e di annotare in cartella di averlo chiesto. Nel principio della *"proporzionalità e sostenibilità delle misure"*, chiaramente definito anche dal GDPR, non è pensabile di andare a cercare il genitore che non ha firmato, così come di non assistere un bambino perché manca la firma di un genitore.

Per quanto riguarda gli **adempimenti a secondo della complessità della propria struttura**, nella Figura 3 sono riportate le risposte dei partecipanti rispetto al quesito di chi avesse accesso ai dati. I soggetti che possono venire in contatto per varie funzioni con i dati sensibili in nostro possesso sono numerosi, e non sempre si pone sufficiente attenzione a questa situazione. Un'accurata analisi di questi aspetti è prodromica alla predisposizione delle **lettere di nomina per i responsabili esterni (sostituti, Software House, commercialista, consulente paghe, tecnico computer ...) e per gli incaricati interni (segretaria e infermiera, nel caso siano dipendenti del medico)**. Caso particolare è quando segretaria e infermiera sono forniti da un soggetto terzo (associazione professionale, cooperativa di servizi, misericordia o affini ...); in questo caso la lettera d'incarico deve essere fatta al fornitore del lavoratore e non al lavoratore stesso.

In caso di lavoro in gruppo, associazione o comunque con personale, solo il 36% dei partecipanti aveva fatto la lettera d'incarico a colleghi e personale e ben il 35% non aveva fatto alcuna lettera di incarico.

Figura 3.

Vari soggetti che possono avere accesso ai dati in uno studio pediatrico.



I **medici sostituti**, che sono a conoscenza e possono gestire i dati sensibili degli assistiti, sono visti nella maggior parte delle risposte come un alter ego del PdF che quindi automaticamente si fa carico della garanzia della tutela della privacy. Solo il 19% del campione ha predisposto una lettera di incarico per tutti i sostituti indipendentemente dalla frequenza e durata del loro utilizzo, il 24% solamente a quelli abituali e ben il 57% a nessuno dei sostituti. La lettera d'incarico va predisposta quindi per tutti i sostituti e, nel caso di una necessità improvvisa con il coinvolgimento di un nuovo sostituto, sarà utile avere nel cassetto una copia di tale lettera in bianco da far compilare e firmare "al volo".

Un ulteriore gruppo di domande voleva chiedere informazioni sulle **Procedure attuate per ridurre il rischio di accessi non autorizzati ai dati sensibili dei propri assistiti,** relativamente ad alcuni aspetti organizzativi legati anche alla variabilità delle modalità lavorative (presenza o meno di personale di segreteria, lavorare in più studi medici, lavorare in studi di proprietà o presso poliambulatori privati, …).

Come vengono chiamati in sala d'aspetto i pazienti per il loro accesso nello studio? La quasi totalità li chiama per nome e cognome (94%), mentre sarebbe opportuno chiamarli solo per nome, o usando sistemi che utilizzano numeri. Questo è particolarmente importante nel caso che la sala di aspetto sia a comune con altri medici, soprattutto di diverse specialità.

La conservazione della documentazione cartacea dei dati sanitari solo nella metà dei casi viene conservata in cassetti/armadi chiusi a chiave, mentre in un terzo dei casi viene semplicemente risposta in un cassetto: è quindi troppo frequente lasciare documentazione sanitaria incustodita, ancora più grave se in sala d'attesa sul bancone della segretaria. Sarebbe utile utilizzare un distruggi-documenti per smaltire le copie di referti, esami, visite che il paziente lascia in visione. Si ricorda anche che, poiché il paziente ha diritto di riavere **gli originali** di radiografie, referti etc., conviene non farseli lasciare ma acquisire direttamente delle copie.

La consegna di documenti sanitari (ad es. un certificato medico o una ricetta) è un altro aspetto di alto rischio di modalità inappropriata di garanzia di tutela della privacy. La domanda del questionario chiedeva il comportamento attuato per le ricette, ma può essere allargata anche ad altri documenti da dare al proprio assistito. Anche perché la consegna di tali documenti è vincolata al soggetto che lo ritirerà, cioè se lui sia il diretto interessato o un delegato riconosciuto del diretto interessato. E se lo fa il personale di segreteria, il documento sanitario deve sempre essere chiuso in una busta (Fig. 4).

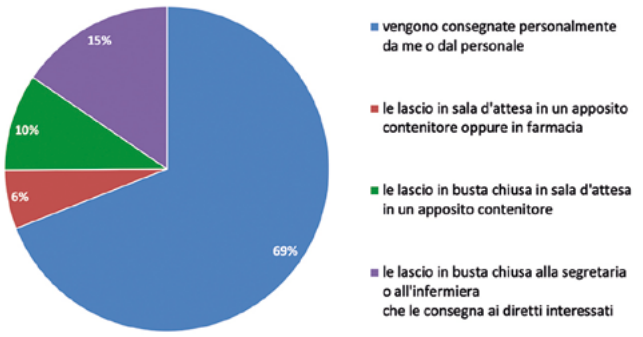
Anche le modalità di ricette o di buste chiuse contenenti i documenti sanitari a disposizione dei pazienti per il ritiro in uno scaffale della sala d'attesa dello studio non sono accettabili, anche perché così facendo non si sa chi è il soggetto che ritira la ricetta o la busta e potrebbe anche succedere che il paziente (magari anche in buona fede) ritiri una busta che non è la sua, o visualizzi ricette non sue.

La **Sicurezza relativa agli aspetti informatici** è molto enfatizzata nel GDPR, che presenta tecniche efficaci per garantire una reale protezione delle informazioni, soprattutto sensibili, quali **la pseudonimizzazione e la cifratura dei dati personali; la capacità di assicurare su base permanente la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; la messa in atto di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.**

L'uso obbligato per legge dell'informatizzazione della cartella clinica e dei sempre più numerosi campi

Figura 4.

Modalità di consegna delle ricette.



di utilizzo ha portato frequenti difficoltà nei colleghi, che ancora vedono come un peso più che un'opportunità questa evoluzione di sistema. Di conseguenza l'attenzione applicativa su come garantire la sicurezza informatica è stata uno degli obiettivi formativi del corso maggiormente sviluppati. E di quanto ce ne fosse bisogno si evince anche dalle risposte al questionario introduttivo su alcuni aspetti informatici.

Infatti, una buona parte dei colleghi (39%) usa il computer di lavoro anche per attività extra-lavorativa, non ha uno screen saver o non lo usa in modo corretto (Fig. 5), non ha una gestione corretta della password di accesso al proprio computer di lavoro. In particolare, il 60% degli intervistati ha una password unica per tutti coloro che accedono al computer e quindi ai dati. Lo screen saver dovrebbe essere impostato che si attivi dopo alcuni minuti di inutilizzo del computer e che sia necessaria la password per disattivarlo; in caso contrario, se ci si allontana dalla postazione di lavoro o si lascia il computer acceso andando via al termine del lavoro, un estraneo potrebbe facilmente accedere ai dati.

Nella Figura 6 sono riportate le modalità di conservazione delle password e del PIN legate alla propria professione.

Riguardo alla presenza di un antivirus sul computer di lavoro, i partecipanti ai corsi si sono divisi quasi equamente fra chi ne aveva uno gratuito e chi lo acquistava; la differenza è sostanzialmente che i secondi sono aggiornati più rapidamente. Ricordiamoci di non tenere attivi due antivirus contemporaneamente (spesso

Figura 5.

Lo screen saver sul computer di lavoro.

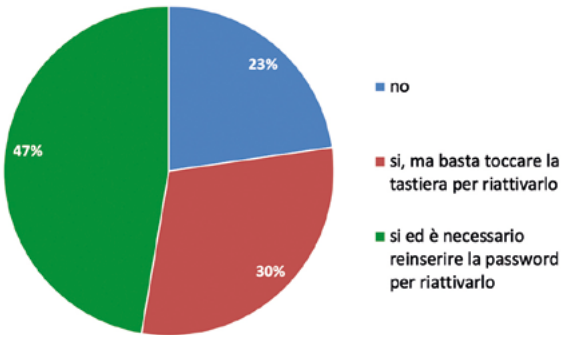
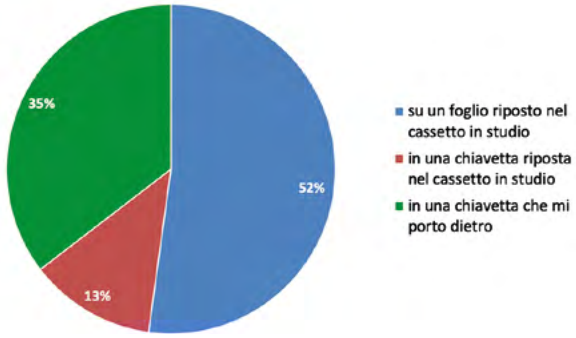


Figura 6.

Modalità di conservazione delle password di lavoro.



windows ne ha uno attivato di default) e scegliamone uno non troppo "invasivo" pena il rallentamento del computer. Il pericolo oggi è però rappresentato soprattutto dai rasomware, ovvero dei programmi, inglobati in mail fraudolente, che si installano nel computer e criptano i dati. Il tema della sicurezza informatica è stato ampiamente sviscerato al corso; nel Box 1 sono riassunti i suggerimenti per le precauzioni da adottare.

Il Regolamento europeo prevede anche la predisposizione e la tenuta di un **registro dei trattamenti dati**, che deve contenere la descrizione delle misure tecniche e organizzative in atto per garantire la sicurezza dei dati personali e le categorie dei destinatari a cui i dati potranno essere comunicati. Solo il 37% del campione analizzato aveva predisposto il registro, elemento indispensabile per ***essere in grado di dimostrare di aver programmato e fatto quello che era possibile fare per evitare problematiche di perdita o diffusione dei dati***.

Una vivace discussione durante gli eventi ha stimolato il concetto del **Data Breach**. Il termine indica ogni "violazione dei dati" e nella pratica può significare ad esempio il furto, la perdita, l'alterazione, la manipolazione di dati cartacei o informatici. In questi casi il titolare dello studio deve **notificare il fatto all'Autorità Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza**. Ma non basta notificare il fatto che si è subita una violazione: bisogna anche dire cosa si è fatto per contenere il danno. Siccome queste eventualità non sono purtroppo rare, è assolutamente indispensabile che il titolare dello studio progetti e rediga una "procedura di emergenza" con la quale fron-

Box 1.

Precauzioni per la privacy "informatica"

Dal sito del SIAF (Sistema Informatico dell'Ateneo Fiorentino) – modificata

Precauzioni nell'utilizzo della posta elettronica

- evitare di aprire allegati che contengono un'estensione doppia o con estensione VBS, SHS, PIF, EXE, COM o BAT (a meno che non attesi e provenienti da mittente conosciuto e di fiducia)
- se si ricevono e-mail non richieste o con contenuti pubblicitari, evitare di seguire i collegamenti a indirizzi Web eventualmente presenti nel testo delle e-mail
- nel caso si riceva un messaggio di e-mail da una persona conosciuta, ma con un contenuto insolito, effettuare un controllo con il mittente prima di aprire l'eventuale allegato; infatti alcuni virus sono in grado di trasmettere messaggi con allegati che sembrano spediti da mittenti conosciuti
- evitare di cliccare su icone dall'apparenza innocua che ricordano applicazioni associate ad immagini o musica, mostrate dagli allegati di posta elettronica in quanto possono nascondere "*worm*"
- configurare il programma di posta elettronica in modo tale che non esegua automaticamente gli allegati.

Gestione delle credenziali

Scelta della password

- la password deve essere composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;
- la password non deve contenere riferimenti aventi attinenza con la vita privata o professionale facilmente riconducibili all'utente (evitare ad es. nome, cognome, data di nascita, numero di telefono, codice fiscale, luogo di nascita, nome di parenti ecc.);
- le password non devono essere parole di senso comune presenti sul dizionario;
- la password non deve contenere una serie consecutiva di soli numeri o di sole lettere;
- la password, nel caso in cui lo strumento elettronico lo permetta, deve essere preferibilmente composta da una sequenza di lettere, numeri e caratteri speciali (es. di caratteri speciali: & @ ? % £ $);
- la password non deve essere costituita da una sequenza ovvia sulla tastiera (es. qwerty, 123456);
- la password deve essere facile da ricordare per l'utente.

Cautele per la segretezza della password

- non comunicare ad altri le proprie credenziali di accesso e le password
- mantenere e custodire le proprie *password* con la dovuta riservatezza**;**
- evitare di scrivere le proprie *password* su foglietti di carta o agende, a meno che tali supporti cartacei non vengano custoditi in cassetti o armadi chiusi a chiave;
- nel digitare sulla tastiera la password, prestare attenzione ad eventuali sguardi indiscreti
- evitare di "salvare" la password sul computer, come proposto dal sistema operativo
- modificare immediatamente la password nel caso sia stato necessario fornire le credenziali ai tecnici intervenuti per la manutenzione del computer o del software

Modifica della password

- modificare la password temporanea assegnata dall'amministratore, al primo utilizzo (primo log-on);
- cambiare immediatamente la password nel caso si sospetti abbia perso il requisito della segretezza;
- in caso di trattamento di dati sensibili (es. dati personali inerenti lo stato di salute) e giudiziari la password deve essere modificata almeno ogni tre mesi.

Precauzioni nella gestione della postazione di lavoro informatica.

Se devo allontanarmi momentaneamente dal mio computer	Evitare di lasciare incustodito e accessibile lo strumento elettronico durante una sessione di lavoro che comporti trattamento di dati personali: bloccare manualmente il computer oppure **attivare il blocco automatico** dopo 5 minuti di inattività. Lo sblocco dello screen saver deve avvenire tramite le credenziali di accesso e non tramite la semplice pressione di un tasto.
Al termine della sessione di lavoro se sono connesso ad un server	Effettuare la procedura di disconnessione ("logoff"/"logout"/"esci") e NON semplicemente bloccare il computer.
Al termine della sessione di lavoro sul mio computer	Effettuare la procedura di arresto del sistema ed attendere che sia terminata prima di lasciare lo studio.
Quando eseguo operazioni a video sulla cartella del paziente	Posizionare il video in modo che non possa essere visto da persone che non autorizzo.
Se, allo spegnimento del computer, sta scaricando degli aggiornamenti	Aspettare che li abbia completamente scaricati ed installati, in modo da essere certi dello spegnimento dello stesso.

teggiare simili evenienze. La segnalazione al Garante non deve essere vista come una "autodenunzia", bensì come una procedura per proteggersi da eventuali successive denunzie che soggetti terzi potrebbero fare, qualora si verificasse veramente una violazione dei dati.

In conclusione, la Privacy è sicuramente un ulteriore aggravio burocratico nel nostro lavoro, ma può rappresentare anche uno stimolo ad una revisione di alcune modalità di lavoro. Nel Box 2 sono riassunte le principali incombenze per il PdF.

Box 2.

Adempimenti dello studio pediatrico per la Privacy

- Redigere l'**informativa** sul trattamento dati ed affiggerla in sala d'attesa
- Acquisire il **consenso** dai genitori o tutori del minore
- Fare una **valutazione d'impatto** della protezione dei dati; non è obbligatorio costruire formalmente un D.P.I.A. (Data Protection Impact Assesment).
- Fare le **lettere di incarico** per il trattamento dati al personale di studio, se presente
- Fare le lettere di incarico per il trattamento dati ai sostituti
- Fare le lettere di incarico per il trattamento dati ai colleghi in caso di pediatria di gruppo o in associazione
- Fare le lettere di incarico per il trattamento dati per la società di software che fornisce il gestionale della cartella clinica, ma anche alle eventuali ditte a cui sia stato affidata l'assistenza informatica (e modificare eventuali contratti precedentemente firmati)
- Fare le lettere di incarico per il trattamento dati al commercialista o al consulente del lavoro (ad esempio che gestisce i rapporti con il personale)
- Definire **procedure** scritte per la riduzione del rischio (e condividerle con il personale di studio, se presente)
- Redigeree mantenere aggiornato il **Registro dei Trattamenti**
- Mettere in atto tutti gli accorgimenti relativi alla "**sicurezza informat**ica" della propria postazione di lavoro e dei vari software
- Garantire regolari **salvataggi** dei dati
- **Notificare** al Garante l'eventuale avvenuta violazione dei dati trattati.