PERCORSO OSS

LEZIONE 11

Videolezione 11.1 – Privacy e gestione dei referti

Introduzione

In questa lezione vedremo come conciliare la moderna società dell'informazione con i diritti di protezione dei dati nell'ambito dei referti sanitari on-line. Per farlo ci rifaremo alle linee guida che sono state emanate dall'Autorità Garante dei dati personali.

I referti on line

Le Linee guida emanate dal Garante nascono dalla constatazione che è molto diffusa nelle strutture sanitarie l'offerta di servizi di "referti on-line", consistenti nella possibilità per l´assistito di accedere al "referto" con modalità informatica. Naturalmente, per "referto" si intende la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale.

Tale modalità di conoscibilità dei referti viene generalmente realizzata attraverso due modalità:

1) la ricezione del referto presso la casella di posta elettronica dell'interessato;
2) il collegamento al sito Internet della struttura sanitaria ove è stato eseguito l'esame clinico, al fine di effettuare il download del referto.

In quest'ultimo caso al paziente viene generalmente fornito un nome utente ed una password all'atto della prenotazione o dell'effettuazione dell'esame.

In alcuni casi è anche possibile effettuare il download del "reperto" (inteso come il risultato dell'esame clinico o strumentale effettuato, come ad es. un'immagine radiografica, un'ecografia o un valore ematico) assieme al referto stilato dal medico.

Il diritto di decidere

I cittadini, sulla base del Codice dell'Amministrazione Digitale, hanno diritto alla disponibilità di tutte le informazioni e i documenti stilati dalle Amministrazioni Pubbliche in formato digitale.

Questo diritto non comporta per il cittadino l'obbligo di accettare la trasmissione digitale. La struttura sanitaria deve garantire all'interessato di decidere liberamente (sulla base di una specifica informativa e di un apposito consenso in ordine al trattamento dei dati personali connessi a tale servizio) di aderire o meno a tali servizi di refertazione, senza alcun pregiudizio sulla possibilità di usufruire delle prestazioni mediche richieste.

Anche nel caso di comunicazione del referto presso l'indirizzo della casella di posta elettronica fornito dall'interessato, a quest'ultimo dovrebbe essere concessa la possibilità di confermare l'indirizzo di posta elettronica in cui ricevere tale comunicazione in occasione dei successivi accertamenti clinici.

Per quanto riguarda la possibilità per l'interessato di acconsentire alla comunicazione dei risultati diagnostici al medico curante, al medico di medicina generale, o al pediatra di libera scelta dallo stesso indicato, tale volontà dovrebbe essere manifestata di volta in volta.

L'informativa

Il titolare del trattamento, per consentire all'interessato di esprimere scelte consapevoli in relazione al trattamento dei propri dati personali, deve previamente fornirgli un'idonea informativa sulle caratteristiche del servizio di refertazione on-line.

Tale informativa deve indicare, con linguaggio semplice, la facoltatività dell'adesione a tali servizi, la cui principale finalità è rendere più rapidamente conoscibile all'interessato il risultato dell'esame clinico effettuato.

L'archiviazione dei referti

In alcune delle iniziative di refertazione on-line è offerto all'interessato anche un servizio aggiuntivo, solitamente gratuito, consistente nella possibilità di archiviare, presso la struttura sanitaria, tutti i referti effettuati nei laboratori della stessa. Il suddetto archivio è generalmente consultabile on-line dall'interessato, il quale può anche effettuare il download dei referti ivi raccolti.

Il titolare del trattamento che intenda offrire all'interessato tale servizio di archiviazione è tenuto a fornire allo stesso una specifica informativa e ad acquisire un autonomo consenso.

La sicurezza del trattamento dei dati per la consultazione on-line dei referti

Naturalmente, in tutti questi casi che abbiamo appena descritto (cioè la possibilità per l'interessato di collegarsi al sito Internet della struttura sanitaria che ha eseguito l'esame clinico, al fine di effettuare il download o la visualizzazione interattiva del referto), devono essere adottate delle specifiche cautele quali:

- protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – Secure Socket Layer);
- tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;
- l'utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
- possibilità da parte dell'utente di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.

La sicurezza del trattamento dei dati per spedizione tramite posta elettronica

In caso, invece, l'interessato scelga di ricevere copia del referto nella propria casella di posta elettronica, per il referto prodotto in formato digitale dovranno essere osservate le seguenti cautele:

- spedizione del referto in forma di allegato a un messaggio e-mail e non come testo compreso nella body part del messaggio;
- il file contenente il referto dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una password per l'apertura del file o in una chiave crittografica. La chiave crittografica o la password devono essere rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti;
- convalida degli indirizzi e-mail tramite apposita procedura di verifica online, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio.

In ogni caso, per il trattamento dei dati nell'ambito dell'erogazione del servizio online agli utenti dovrà essere garantita la disponibilità di:

- idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento di dati idonei a rivelare l'identità genetica di un individuo;
- separazione fisica o logica dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per scopi amministrativo-contabili.

Principio generale

Indipendentemente dal modo scelto per visualizzare il referto, devono essere sempre adottate tutte le misure di sicurezza necessarie per rispettare il divieto di diffusione dei dati sanitari.

È fondamentale considerare che le cautele elencate dal Provvedimento, precedente all'entrata in vigore del Regolamento europeo, sono da considerarsi "minime": il principio di accountability impone, invece, al titolare del trattamento, "tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche", di mettere in atto misure tecniche ed organizzative adeguate.

È pertanto necessario che il titolare individui, in relazione alle specificità del servizio offerto e sulla base di una puntuale valutazione del rischio, le misure di sicurezza più idonee a garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati.

La formazione

Sotto il profilo della sicurezza, di cruciale importanza diventa oggi, anche alla luce del GDPR, la formazione di tutti i soggetti autorizzati al trattamento. Chiunque abbia accesso a questi dati o possa effettuare attività di trattamento su di essi deve essere istruito in tal senso.

Questo non solo nell'ottica della migliore gestione e protezione dei dati stessi, ma anche in un'ottica di tutela degli interessati. Va ricordato infatti che, anche per assicurare una piena comprensione degli elementi indicati nell'informativa, specialmente quando si tratta di servizi molto specifici attinenti a categorie particolari di dati personali, il titolare deve formare adeguatamente il personale coinvolto ai fini di un più efficace rapporto con gli utenti del servizio.

Conclusioni

In questa lezione abbiamo esaminato le norme emanate dal Garante per la protezione dei dati personali in merito ai referti on-line, mettendo in evidenza l'importanza delle decisioni che l'interessato, proprietario dei dati, vuole assumere.