

AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERAZIONE 19 novembre 2009

Linee guida in tema di referti on-line. (Deliberazione n. 36)

(Gazzetta Ufficiale – Serie Generale n. 288 del 11 dicembre 2009)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti, e del dott. Filippo Patroni Griffi, segretario generale;

VISTA la deliberazione del 25 giugno 2009, n. 21, con la quale l'Autorità ha avviato una procedura di consultazione pubblica su un documento, adottato in pari data, contenente "Linee guida in tema di referti on-line" e pubblicato, unitamente alla medesima deliberazione, sul sito web dell'Autorità e sulla Gazzetta Ufficiale n. 162 del 15 luglio 2009;

VISTI i commenti e le osservazioni pervenute a questa Autorità a seguito della consultazione pubblica per la quale era stato fissato il termine del 30 settembre 2009;

TENUTO CONTO che le osservazioni ricevute hanno riguardato principalmente la necessità di prevedere un periodo di disponibilità del referto on-line superiore a 30 gg., nonché di evidenziare il diverso ambito di applicazione delle presenti Linee guida sia rispetto a quelle in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario, sia in relazione alla specifica disciplina in tema di validità legale del referto;

RITENUTO opportuno, alla luce delle osservazioni ricevute, di apportare alcune modifiche alle "Linee guida in tema di referti on-line" oggetto di consultazione pubblica, ed, in particolare, di prevedere un periodo di disponibilità del referto on-line di 45 gg., tenuto conto che tale maggiore intervallo temporale può considerarsi congruo sotto il profilo delle specifiche cautele che, secondo quanto disposto nelle medesime Linee guida, devono essere adottate al fine di assicurare un idoneo livello di sicurezza dei dati personali in tal modo trattati;

RITENUTO, in base agli approfondimenti svolti e tenuto conto delle suddette osservazioni ricevute, di individuare un quadro unitario di misure e accorgimenti necessari e opportuni da porre a garanzia dei cittadini, in relazione ai trattamenti di dati che li riguardano;

VISTO il Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il prof. Francesco Pizzetti;

DELIBERA:

a) di adottare in via definitiva le "Linee guida in tema di referti on-line", contenute nel [documento allegato](#) quale parte integrante della presente deliberazione (Allegato n. 1);

b) che copia della presente deliberazione, unitamente ai menzionati allegati, sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana, ai sensi dell'art. 143, comma 2, del Codice.

Roma, 19 novembre 2009

IL PRESIDENTE
Pizzetti

IL RELATORE
Pizzetti

IL SEGRETARIO GENERALE
Patroni Griffi

Allegato n. 1

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI LINEE GUIDA IN TEMA DI REFERTI ON-LINE

1. AMBITO DI APPLICAZIONE DELLE LINEE GUIDA

L'Autorità ritiene opportuno fornire alcune indicazioni in merito all'utilizzo dei dati personali nell'ambito di alcune iniziative sorte nel processo di ammodernamento della sanità pubblica e privata che ha generato un maggiore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure.

All'interno di tali iniziative è stato riscontrato essere di recente molto diffusa in numerose strutture sanitarie, soprattutto private, l'offerta di servizi gratuiti generalmente riconducibili all'espressione "referti on-line", consistenti nella possibilità per l'assistito di accedere al "referto" –inteso come la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale- con modalità informatica. Analogamente è concessa all'assistito la possibilità di decidere -di volta in volta o una tantum- di ricevere telematicamente i predetti esiti clinici direttamente attraverso il proprio medico curante o il medico di medicina generale/pediatra di libera scelta (MMG/PLS).

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, che sembra essere il più utilizzato, al paziente viene generalmente fornito un nome utente ed una *password* all'atto della prenotazione o dell'effettuazione dell'esame.

In alcune delle iniziative esaminate è anche possibile effettuare il *download* del "referto" (inteso come il risultato dell'esame clinico o strumentale effettuato, come ad es. un'immagine radiografica, un'ecografica o un valore ematico) assieme al referto stilato dal medico.

Talvolta, il paziente viene avvisato della possibilità di visualizzare il referto attraverso una delle modalità sopra descritte mediante l'invio di uno *short message service* (sms) sul numero di telefono mobile fornito alla struttura sanitaria dallo stesso paziente all'atto dell'adesione al servizio.

Le presenti linee guida non intendono disciplinare gli aspetti relativi alla validità legale del referto -che rimane regolata dalla specifica normativa di settore- ferme restando, ovviamente, anche le disposizioni relative alla firma elettronica del documento informatico, con specifico riferimento alle metodologie dell'autenticazione informatica ove applicabili (*d.lg. 7 marzo 2005, n. 82*).

Allo stato delle notizie acquisite, non consta l'esistenza di una normativa in merito a tali modalità di consegna dei referti. Ciò stante, si è osservato che nella quasi totalità delle iniziative esaminate, la refertazione *on-line* non sostituisce le normali procedure di consegna dei referti, che restano, in ogni caso, disponibili in formato cartaceo -ai sensi e per gli effetti di legge- presso la struttura sanitaria dove è stata erogata la prestazione. Il paziente, infatti, può generalmente ritirare i referti in originale¹. Tali servizi, infatti, non si propongono -di regola- di sostituire la refertazione cartacea, bensì di anticiparla, fornendo un'anteprima dei referti, attraverso la visualizzazione e la stampa dei documenti stessi non appena questi siano resi disponibili dalla struttura erogatrice della prestazione sanitaria.

Si ritiene opportuno precisare che i servizi oggetto delle presenti linee guida sono da considerare del tutto distinti e autonomi dal Fascicolo sanitario elettronico (Fse)², consistendo quest'ultimo nell'insieme delle informazioni relative ai diversi eventi clinici (e, quindi, non solo quelle sui referti) occorsi ad un individuo durante la sua vita, messo in condivisione logica dai professionisti o organismi sanitari-in qualità di autonomi titolari del trattamento- che assistono nel tempo l'interessato, al fine di offrirgli un migliore processo di cura.

Con le presenti linee guida si intende individuare uno specifico quadro unitario di garanzie per i cittadini nei confronti di alcuni servizi, attualmente in uso, consistenti nella possibilità di ricevere via posta elettronica o di consultare telematicamente il referto relativo ad un singolo evento sanitario (es. analisi cliniche) non appena lo stesso sia reso disponibile da parte dell'organismo sanitario presso il quale si è rivolto l'interessato.

2. FRUIZIONE FACOLTATIVA DEL SERVIZIO DI REFERTAZIONE ON-LINE

In base alle disposizioni contenute nel Codice dell'amministrazione digitale, deve essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali (art. 2, d.lg. 7 marzo 2005, n. 82).

Come già anticipato, la mancanza di specifiche disposizioni normative in merito a tali modalità di consegna dei referti determina che tali servizi devono essere considerati facoltativi per l'interessato, ovvero offerti con modalità tali da rendere possibile a quest'ultimo di potere comunque scegliere di ritirare il referto in formato cartaceo.

All'interessato deve essere consentito, infatti, di scegliere -in piena libertà- se accedere o meno al servizio di refertazione *on-line*, garantendogli in ogni caso la possibilità di continuare a ritirare i referti cartacei presso la struttura erogatrice della prestazione.

La struttura sanitaria deve, anche, 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.

Qualora l'interessato abbia scelto di aderire ai suddetti servizi di refertazione, deve essergli concesso -in relazione ai singoli esami clinici a cui si sottoporrà di volta in volta- di manifestare una volontà contraria, ovvero che i relativi referti non siano oggetto del servizio di refertazione *on-line* precedentemente scelto.

Anche nel caso di comunicazione del referto presso l'indirizzo della casella di posta elettronica fornito dall'interessato, a quest'ultimo deve essere concessa la possibilità di confermare l'indirizzo di posta elettronica in cui ricevere tale comunicazione in occasione dei successivi accertamenti clinici. Resta ferma l'operatività del sistema che verrà adottato ai sensi del d.P.C.M. 6 maggio 2009 in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.

Per quanto riguarda la possibilità per l'interessato di acconsentire alla comunicazione dei risultati diagnostici al medico curante o al MMG/PLS dallo stesso indicato, tale volontà deve essere manifestata di volta in volta. All'interessato deve, infatti, essere concesso il diritto di non comunicare sistematicamente al medico curante tutti i risultati delle indagini cliniche effettuate, lasciandogli la possibilità di scegliere, di volta in volta, quali referti mettere a disposizione del proprio medico. Tale garanzia deve intendersi operante sia nel caso più frequente in cui l'interessato autorizzi la comunicazione del referto presso la casella di posta elettronica del medico curante, sia in quello in cui autorizzi la struttura sanitaria a fornire le credenziali di autenticazione direttamente al medico, affinché quest'ultimo effettui il *download* del suo referto.

Nel caso di utilizzazione del servizio di avviso tramite sms della disponibilità alla consultazione dei referti attraverso le modalità sopra descritte, nel messaggio inviato deve essere data solo notizia della disponibilità del referto e non anche del dettaglio della tipologia di accertamenti effettuati, del loro esito o delle credenziali di autenticazione assegnate all'interessato (Cfr. [successivo punto 6](#)).

3. INFORMATIVA E CONSENSO

Per consentire all'interessato di esprimere scelte consapevoli in relazione al trattamento dei propri dati personali, il titolare del trattamento deve previamente fornirgli un'adeguata informativa sulle caratteristiche del servizio di refertazione *on-line* (artt. 13, 79 e 80 del Codice). Tale informativa, che può essere resa anche unitamente a quella relativa al trattamento dei dati personali per finalità di cura ma distinta da essa, deve indicare, con linguaggio semplice, tutti gli elementi richiesti dall'art. 13 del Codice. In particolare, deve essere evidenziata la facoltatività dell'adesione a tali servizi, aventi la finalità di rendere più rapidamente conoscibile all'interessato il risultato dell'esame clinico effettuato.

L'informativa deve rendere note all'interessato anche le modalità attraverso le quali rivolgersi al titolare per esercitare i diritti di cui agli artt. 7 e ss. del Codice.

Al fine di assicurare una piena comprensione degli elementi indicati nell'informativa, il titolare deve formare adeguatamente il personale coinvolto sugli aspetti rilevanti della disciplina sulla protezione dei dati personali, anche ai fini di un più efficace rapporto con gli interessati.

Dopo aver fornito l'informativa, il titolare del trattamento deve acquisire un autonomo e specifico consenso dell'interessato a trattare i suoi dati personali, anche sanitari, attraverso le suddette modalità di refertazione.

4. ARCHIVIO DEI REFERTI

In alcune delle iniziative di refertazione *on-line* in essere, 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 ed ad acquisire un autonomo consenso.

Tali archivi, raccogliendo tutti i referti effettuati nel tempo dall'interessato ed essendo realizzati presso un organismo sanitario in qualità di unico titolare del trattamento (es., laboratorio di analisi, clinica privata), ricadono nella definizione di dossier sanitario, secondo quanto indicato nel richiamato Provvedimento del Garante del 16 luglio 2009, recante "*Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario*". Ciò stante, il titolare del trattamento che intenda offrire all'interessato la possibilità di raccogliere i referti in tali archivi deve tenere conto delle garanzie –anche di sicurezza– individuate nel citato provvedimento per i dossier sanitari.

5. COMUNICAZIONE DEI DATI ALL'INTERESSATO

Secondo quanto previsto dall'art. 84 del Codice, i dati personali inerenti allo stato di salute devono essere resi noti all'interessato solo per il tramite di un medico designato dallo stesso o dal titolare. Il secondo comma di tale disposizione prevede che il titolare o il responsabile possano autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i

medesimi dati all'interessato.

L'abilitazione all'accesso dei suddetti sistemi di refertazione deve, pertanto, essere consentita all'interessato nel rispetto delle cautele previste dalla disciplina di settore già applicabili anche per il cartaceo e richiamate dal Garante nel provvedimento generale del 2005³. In particolare, nel caso di specie, l'intermediazione può essere soddisfatta accompagnando la comunicazione del reperto con un giudizio scritto e la disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato.

I titolari del trattamento, nell'offrire tali servizi, devono tenere conto delle disposizioni di settore che prevedono -nella comunicazione dei referti e nella illustrazione del loro significato diagnostico- una specifica attività di consulenza da parte del personale medico (ad esempio, nel caso di indagini cliniche volte a rivelare direttamente o indirettamente l'infezione da HIV⁴). La necessità di assicurare una consulenza genetica appropriata nell'effettuazione di test genetici⁵ -anche prenatali- fa ritenere di potere, poi, escludere la possibilità di offrire tali servizi di refertazione nel caso in cui l'interessato si sottoponga a tali indagini cliniche.

6. MISURE DI SICUREZZA E TEMPI DI CONSERVAZIONE DEI DATI

La particolare delicatezza dei dati personali trattati mediante i servizi di refertazione on-line impone l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza ai sensi dell'art. 31 del Codice, ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice (artt. 33 e ss.) e, in particolare, laddove applicabili, quelle richieste dalla regola 24 del Disciplinare tecnico in materia di misure minime di sicurezza, allegato B) al Codice, laddove per il trasferimento di dati idonei a rivelare l'identità genetica di un individuo viene richiesto il ricorso alla cifratura.

Per la consegna degli esiti dell'attività diagnostica e di analisi biomedica si prospettano attualmente i due diversi scenari sopra descritti che pongono problemi di protezione dei dati da affrontare con differenti approcci.

Scenario 1 – consultazione *on-line* dei referti tramite servizi Web accessibili da Internet.

Nel caso in cui il servizio che si intenda offrire consti nella possibilità per l'interessato di collegarsi al sito Internet della struttura sanitaria che ha eseguito l'esame clinico, al fine di effettuare la copia locale (*download*) o la visualizzazione interattiva del referto, devono essere adottate delle specifiche cautele quali:

1. 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*);
2. 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*;

3. l'utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di *strong authentication*;
4. disponibilità limitata nel tempo del referto *on-line* (massimo 45 gg.);
5. 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.

Scenario 2 – spedizione del referto tramite posta elettronica.

Qualora il titolare del trattamento intenda inviare copia del referto alla casella di posta elettronica dell'interessato, a seguito di sua richiesta, per il referto prodotto in formato digitale devono essere osservate le seguenti cautele:

1. spedizione del referto in forma di allegato a un messaggio *e-mail* e non come testo compreso nella *body part* del messaggio;
2. 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 rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (*Cfr.* regola 24 del Disciplinare tecnico allegato B) al Codice). Tale cautela può non essere osservata qualora l'interessato ne faccia espressa e consapevole richiesta, in quanto l'invio del referto alla casella di posta elettronica indicata dall'interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l'interessato effettuata su specifica richiesta di quest'ultimo;
3. convalida degli indirizzi *e-mail* tramite apposita procedura di verifica *on-line*, 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 deve essere garantita la disponibilità di:

1. idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati), prevedendo il ricorso alla *strong authentication* con utilizzo di caratteristiche biometriche nel caso del trattamento di dati idonei a rivelare l'identità genetica di un individuo;
2. 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.

Il titolare del trattamento deve, inoltre, prevedere apposite procedure che rendano immediatamente non disponibili per la consultazione *on-line* o interrompano la procedura di spedizione per posta elettronica dei referti relativi a un interessato che abbia comunicato il furto o lo smarrimento delle proprie credenziali di autenticazione all'accesso al sistema di consultazione *on-line* o altre condizioni di possibile rischio per la riservatezza dei propri dati personali.

In ogni caso devono essere adottate tutte le misure di sicurezza necessarie per rispettare il divieto di diffusione dei dati sanitari prescritto dal Codice (artt. 22, comma 8 e 26, comma 5).

1 Al riguardo, cfr. art. 5, comma 8, legge 29 dicembre 1990, n. 407 e art. 4, comma 18, legge 30 dicembre 1991, n. 412.

2 Provvedimento del Garante del 16 luglio 2009, recante "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario", pubblicato in G.U. n. 178 del 3 agosto 2009 e consultabile sul sito: www.garanteprivacy.it [doc.web n. 1634116].

3 Cfr. punto 4 del provvedimento del Garante del 9 novembre 2005 "Strutture sanitarie: rispetto della dignità" consultabile sul sito www.garanteprivacy.it - doc. web n. 1191411.

4 Cfr. art. 5, l. 5 giugno 1990, n. 135, Relazione al parlamento sullo stato di attuazione delle strategie attivate per fronteggiare l'infezione da HIV nell'anno 2006, Ministero della salute, Dipartimento della prevenzione e della comunicazione, Direzione generale della prevenzione sanitaria e Manuale di informazioni pro-positive, a cura della Consulta del volontariato per i problemi dell'AIDS presso il Ministero della salute, in merito all'assistenza psicologica e alla consulenza specialistica alle persone che hanno effettuato il test HIV.

5 Cfr. art. 12, Convenzione sui diritti dell'uomo e sulla biomedicina, Oviedo il 4 aprile 1997 e Autorizzazione al trattamento dei dati genetici del 22 febbraio 2007, pubblicata in G.U. n. 65 del 19 marzo 2007, consultabile sul sito: www.garanteprivacy.it -doc. web n. 1389918, la cui efficacia è stata differita con provvedimento del 19 dicembre 2008 pubblicato in G.U. n. 15 del 20 gennaio 2009- doc. web n. 1582871.