



**Prescrizioni ad un'azienda sanitaria per le operazioni di pagamento dei corrispettivi per le prestazioni erogate attraverso la rete "Sportello amico" di Poste Italiane S.p.A. e mediante il proprio sito Internet - 13 marzo 2014**

Registro dei provvedimenti  
n. 120 del 13 marzo 2014

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti e del dott. Giuseppe Busia, segretario generale;

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

ESAMINATE le segnalazioni pervenute all'Autorità in merito alle modalità con le quali è consentito presso lo "Sportello amico" di Poste Italiane S.p.A. il pagamento dei corrispettivi per le prestazioni sanitarie erogate dall'Azienda sanitaria di Firenze;

VISTE le richieste di informazioni in atti;

VISTI gli atti dell'accertamento ispettivo effettuato il 15 e il 16 ottobre 2013 presso Poste Italiane S.p.A., Ufficio postale n. 1 di Firenze;

VISTA la documentazione inviata dall'Azienda sanitaria di Firenze;

VISTE le linee guida in tema di referti on-line adottate dal Garante il 19 novembre 2009 (consultabile sul sito [www.gdp.it](http://www.gdp.it), doc. web n. [1679033](#));

VISTO il decreto del Presidente del Consiglio dei Ministri dell'8 agosto 2013 concernente le modalità di consegna, da parte delle aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate (pubblicato in GU Serie Generale n.243 del 16-10-2013), su cui il Garante ha espresso parere favorevole il 6 dicembre 2012 (consultabile sul sito [www.gdp.it](http://www.gdp.it), doc. web n. [2223206](#));

VISTO il provvedimento generale circa il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati nell'erogazione delle prestazioni da parte delle strutture sanitarie adottato dal Garante il 9 novembre 2005 (consultabile sul sito [www.gdp.it](http://www.gdp.it), doc. web n. [1191411](#));

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 dott. Antonello Soro;

**PREMESSO**

Sono pervenute alcune segnalazioni nelle quali si lamenta una presunta violazione delle disposizioni in materia di protezione dei dati personali in relazione al servizio offerto dall'Azienda sanitaria di Firenze relativo al pagamento del corrispettivo per le prestazioni sanitarie dalla stessa erogate presso la rete "Sportello amico" di Poste Italiane S.p.A.. Più precisamente, alcuni cittadini lamentano che per effettuare il suddetto pagamento sia necessario presentare allo "Sportello amico" il foglio di prenotazione della prestazione sanitaria. L'esibizione di tale documentazione, in base alle segnalazioni ricevute, consentirebbe all'operatore di sportello di venire a conoscenza di informazioni personali dell'interessato quali la natura delle prestazioni prenotate e la fascia di reddito di appartenenza.

I segnalanti lamentano, inoltre, una possibile violazione delle norme a tutela dei dati personali da parte della citata Azienda sanitaria nella realizzazione del progetto di consegna dei referti per le prestazioni dalla stessa erogate tramite la citata rete "Sportello amico" di Poste Italiane S.p.A..

In merito a quanto segnalato, l'Ufficio ha provveduto a richiedere informazioni all'Azienda sanitaria di Firenze senza, tuttavia, ricevere alcun riscontro.

Attesa la necessità di verificare in loco le concrete modalità di erogazione dei servizi oggetto delle citate segnalazioni, in data 15 e 16 ottobre u.s. l'Ufficio ha effettuato un accertamento ispettivo presso Poste Italiane S.p.A., Ufficio postale n. 1 di Firenze, allo scopo di verificare

l'osservanza delle disposizioni in materia di protezione dei dati personali in relazione ai servizi offerti attraverso la rete "Sportello Amico" di Poste Italiane S.p.A., con specifico riferimento a quelli relativi al pagamento del ticket e al ritiro dei referti per conto dell'Azienda sanitaria di Firenze.

Durante il suddetto accertamento ispettivo è stato verificato che il servizio di consegna dei referti presso la rete "Sportello Amico" per conto della richiamata Azienda non è stato ancora attivato. Con successiva comunicazione l'Azienda sanitaria ha rappresentato a questa Autorità che detto servizio "prevede una fase di sperimentazione che non è stata ancora avviata, essendo in corso di perfezionamento il protocollo informatico di scambio dati" con Poste Italiane S.p.A. (nota dell'Azienda sanitaria di Firenze dell'8 novembre 2013).

Nel corso dell'accertamento ispettivo è stato verificato che il servizio di pagamento del corrispettivo per le prestazioni sanitarie erogate dall'Azienda sanitaria, oggetto delle segnalazioni sopra richiamate, è attivo ed è regolato da un accordo stipulato tra le parti il 7 agosto 2012. Tale accordo prevede che la rete degli sportelli di Poste Italiane S.p.A., denominati "Sportello Amico", acquisiscano il codice fiscale del cittadino quale chiave di ricerca delle prestazioni sanitarie in relazione alle quali si intende effettuare il pagamento del corrispettivo (art. 3.1.a) dell'accordo). Al riguardo, è stato accertato che l'operatore di sportello provvede a chiedere al soggetto che intende effettuare il pagamento solo il codice fiscale dell'interessato cui la prestazione sanitaria si riferisce e non anche il foglio di prenotazione della prestazione rilasciato dall'Azienda. Una volta inserito il codice fiscale dell'interessato nel sistema informativo in uso presso lo sportello, la procedura informatica genera una maschera nella quale sono presenti i numeri di prenotazione delle prestazioni sanitarie prenotate -senza l'indicazione della natura della prestazione-, la data di erogazione e il relativo importo da pagare. All'esito della registrazione del pagamento effettuato, l'operatore accede ad una maschera che consente di stampare l'informativa relativa al trattamento dei dati personali effettuato dalla suddetta Azienda connesso al pagamento della prestazione sanitaria che viene fatta firmare all'utente e conservata da parte dell'Ufficio postale.

Successivamente, l'operatore accede ad un'altra maschera attraverso la quale effettua la stampa della ricevuta fiscale dell'avvenuto pagamento. Nella stampa della suddetta ricevuta il sistema genera un primo foglio contenente la dicitura: "Poste italiane documento contenente dati sensibili ai sensi dell'art. 4 comma 1 lett. d) d.lgs. 196/03" e i restanti due fogli contenenti la fattura della prestazione sanitaria pagata (copia per l'Azienda sanitaria e per l'utente) contenente anche la descrizione della natura della prestazione.

Durante l'accertamento ispettivo è stato constatato che l'operatore di sportello non verifica l'identità dell'utente che si presenta per effettuare il pagamento, al quale consegna le due copie della fattura relativa all'avvenuto pagamento.

Nel corso delle attività istruttorie effettuate dall'Ufficio è emerso poi che l'Azienda sanitaria di Firenze consente il pagamento del corrispettivo per le prestazioni sanitarie prenotate tramite il centro unico di prenotazione (CUP) dell'Azienda e dalla stessa erogate anche mediante il proprio sito Internet (<http://wiasf.cupmet-fi.it/ASFWeb/WICUP/pagamenti/ricercaAppuntamenti.do>).

Analogamente a quanto avviene presso gli uffici postali nei termini sopra descritti, l'utente che intende usufruire di tale servizio on line deve inserire il codice fiscale dell'interessato cui si riferisce la prestazione sanitaria e scegliere la prestazione da pagare tra quelle prenotate. Nell'utilizzo di tale servizio non è previsto un sistema di identificazione dell'utente. Con la nota sopra richiamata dell'8 novembre 2013, l'Azienda sanitaria ha precisato che "il servizio di pagamento di ticket attraverso il sito Internet (...) prevede la visualizzazione del solo codice di prenotazione, della data di esecuzione e dell'importo" e non anche la dicitura relativa alla natura della prestazione erogata.

## OSSERVA

### 1. Premessa

L'Azienda sanitaria di Firenze è titolare del trattamento di dati personali effettuato tramite i servizi di pagamento del corrispettivo per le prestazioni sanitarie erogate dalla stessa offerti attraverso la rete "Sportello amico" di Poste Italiane S.p.A. e mediante il proprio sito Internet: <http://wiasf.cupmet-fi.it/ASFWeb/WICUP/pagamenti/ricercaAppuntamenti.do>.

Dal punto di vista della disciplina in materia di protezione dei dati personali, tali servizi presentano profili di criticità con riferimento alla mancata identificazione dell'utente che effettua il pagamento e che, quindi, ha accesso ad informazioni personali, anche idonee a rivelare lo stato di salute, dell'interessato cui la prestazione sanitaria si riferisce.

### 2. Criticità del servizio di pagamento del corrispettivo per le prestazioni sanitarie erogate dall'Azienda sanitaria di Firenze offerto attraverso la rete "Sportello amico" di Poste Italiane S.p.A..

L'Azienda sanitaria di Firenze, come indicato anche nel citato accordo del 7 agosto 2012 con Poste Italiane S.p.A., è titolare del trattamento di dati personali effettuato nell'ambito del servizio di pagamento delle prestazioni sanitarie dalla stessa erogate offerto attraverso la rete "Sportello amico". In tale contesto, Poste Italiane S.p.A. effettua un trattamento di dati personali in qualità di responsabile del trattamento designato dall'Azienda sanitaria di Firenze (art. 8 del citato accordo del 7 agosto 2012). Il personale addetto allo sportello è stato nominato incaricato del trattamento da parte di Poste Italiane S.p.A., ai sensi dell'art. 30 del Codice, ed è stato formato in merito alle procedure da porre in essere nell'erogazione del suddetto servizio (documentazione acquisita nel corso della richiamata attività ispettiva).

Gli operatori di sportello, in qualità di incaricati del trattamento, nell'erogare il suddetto servizio, vengono, pertanto, correttamente a conoscenza di dati personali dell'interessato cui la prestazione sanitaria si riferisce sia nella fase di pagamento (elenco dei codici di prenotazione delle prestazioni, data di erogazione, importo), sia di stampa della ricevuta fiscale (descrizione della natura della prestazione sanitaria di cui si è effettuato il pagamento). Tale documento, infatti, a norma di legge, deve contenere la descrizione della natura della prestazione oggetto della fattura; tale descrizione, riportando la dicitura in chiaro relativa alla visita o al trattamento medico effettuato (es. visita chemioterapica, radioterapia), può, in taluni casi, essere idonea a rivelare anche lo stato di salute dell'interessato. All'atto della stampa della fattura l'operatore di "Sportello amico" viene reso edotto di tale trattamento di dati sensibili attraverso la dicitura che appare sul video e nel primo foglio della stampa del documento: "Poste italiane documento contenente dati sensibili ai sensi dell'art. 4 comma 1 lett. d) d.lgs. 196/03". L'operatore di sportello, quindi, in qualità di incaricato del trattamento, tratta lecitamente informazioni personali dell'interessato cui la prestazione sanitaria si riferisce, che possono, in taluni casi, anche essere idonee a rivelare lo stato di salute di questo.

Analogamente, l'utente che effettua il pagamento, qualora sia persona diversa dall'interessato, viene a conoscenza dei dati personali di quest'ultimo -in taluni casi anche idonei a rivelare il suo stato di salute- attraverso la lettura della descrizione della natura della prestazione sanitaria presente nella fattura.

Sulla base di quanto accertato in loco, l'operatore di sportello, tuttavia, non identifica l'utente che si presenta per effettuare il pagamento; in particolare, non accerta che tale soggetto sia l'interessato ovvero altro soggetto da questo delegato. L'operatore di sportello, inoltre, consegna a tale soggetto non preventivamente identificato la ricevuta fiscale dell'avvenuto pagamento, in duplice copia, nella quale, come già evidenziato, è riportata in chiaro la descrizione della natura della prestazione sanitaria da erogare.

In tale quadro, pertanto, si ravvisano profili di criticità in materia di protezione dei dati personali in relazione alla circostanza, accertata in loco, che l'operatore di sportello non verifica che il soggetto che effettua il pagamento sia l'interessato cui la prestazione sanitaria si riferisce ovvero sia un soggetto da questo delegato e consegna a tale soggetto la ricevuta fiscale contenente dati personali, anche sensibili, dell'interessato.

### **3. Criticità del servizio di pagamento del corrispettivo per le prestazioni sanitarie erogate dall'Azienda sanitaria di Firenze attraverso il proprio sito Internet (<http://wiasf.cupmet-fi.it/ASFWeb/WICUP/pagamenti/ricercaAppuntamenti.do>).**

L'Azienda sanitaria di Firenze consente ai propri utenti di effettuare il pagamento del corrispettivo per le prestazioni sanitarie prenotate tramite CUP e dalla stessa erogate mediante il proprio sito Internet (<http://wiasf.cupmet-fi.it/ASFWeb/WICUP/pagamenti/ricercaAppuntamenti.do>).

L'utente, collegandosi alla pagina del suddetto sito denominata "Pagamento ticket", accede ad una maschera contenente le istruzioni per effettuare il pagamento "delle visite, degli esami specialistici prenotati tramite CUP e degli esami di laboratorio erogati dall'Azienda sanitaria di Firenze".

Secondo quanto indicato nel predetto sito, non è previsto un sistema di identificazione dell'utente che intende utilizzare tale servizio.

Sulla base di quanto indicato nella pagina "Pagamento ticket" e affermato dall'Azienda sanitaria con la nota sopra richiamata dell'8 novembre 2013, l'utente-non previamente identificato- deve inserire il codice fiscale dell'interessato cui si riferisce la prestazione sanitaria e cliccare sul pulsante "Ricerca prestazioni". Attraverso tale operazione, l'utente accede ad una maschera contenente l'elenco dei codici di prenotazione delle prestazioni sanitarie riferite all'interessato di cui sia stato inserito il codice fiscale, con l'indicazione della data di erogazione della prestazione e del relativo importo. Visualizzato il suddetto elenco, l'utente seleziona la prestazione da pagare ed effettua il pagamento mediante carta di credito, attraverso il collegamento al sito Internet dell'Istituto bancario Intesa San Paolo S.p.A.. Nella suddetta procedura è previsto che l'utente che effettua il pagamento inserisca un indirizzo e-mail al quale è inviato "l'esito del pagamento". Secondo quanto indicato nella pagina "Pagamento ticket" del predetto sito dell'Azienda sanitaria di Firenze, "al termine dell'operazione di pagamento (l'utente ha) (...) la possibilità di stampare la ricevuta che attesta il pagamento della prestazione".

Analogamente a quanto rilevato nel paragrafo 2 del presente provvedimento, nella stampa della fattura relativa all'avvenuto pagamento della prestazione sanitaria è presente la descrizione della natura della prestazione che, in taluni casi, può essere idonea a rivelare lo stato di salute dell'interessato cui la prestazione sanitaria si riferisce.

Il servizio di pagamento delle prestazioni sanitarie offerto dall'Azienda sanitaria di Firenze attraverso il proprio sito Internet è realizzato in modo tale che chiunque, senza essere preventivamente identificato, attraverso l'inserimento del codice fiscale di un assistito della stessa Azienda, possa accedere all'elenco dei codici di prenotazione delle prestazioni sanitarie richieste dall'assistito stesso (con l'indicazione della data di erogazione e del relativo importo). Come già precedentemente indicato, il predetto codice di prenotazione, anche se privo dell'indicazione della natura della prestazione, costituisce, unito al codice fiscale dell'interessato, alla data di erogazione della prestazione e al relativo importo, un dato personale dell'interessato.

Si osserva, inoltre, che il medesimo utente all'atto del pagamento della prestazione sanitaria, senza essere stato preventivamente identificato, può, inoltre, venire a conoscenza anche dei dati idonei a rivelare lo stato di salute dell'interessato mediante la stampa della relativa ricevuta fiscale. Come già rilevato, infatti, tale documento contiene la descrizione della natura della prestazione oggetto della fattura; idonea, in taluni casi, a rivelare lo stato di salute dell'interessato.

Il suddetto servizio, infatti, non identifica l'utente che effettua il pagamento e, quindi, non verifica che questo coincida con l'interessato cui si riferisce la prestazione sanitaria o con altro soggetto a ciò delegato dall'interessato.

Ciò premesso, si ritiene, pertanto, che il servizio sopra descritto consenta ad un utente non identificato in possesso del codice fiscale dell'interessato che abbia prenotato una prestazione sanitaria erogata dall'Azienda sanitaria di Firenze di accedere ad informazioni personali di quest'ultimo (elenco dei codici di prenotazione delle prestazioni, data di erogazione e importo), che possono essere, in taluni casi, anche idonee a rivelare il suo stato di salute, qualora tale utente proceda al pagamento delle suddette prestazioni e alla stampa della relativa fattura, recante, in chiaro la descrizione della natura della prestazione sanitaria.

### **4. Prescrizioni**

Occorre preliminarmente riconoscere l'indubbia semplificazione che l'Azienda sanitaria di Firenze intende introdurre attraverso l'utilizzo dei servizi sopra descritti con specifico riferimento alle modalità attraverso le quali gli utenti possono pagare il corrispettivo per le prestazioni sanitarie dalla stessa erogate avvalendosi della rete "Sportello amico" di Poste Italiane S.p.A. e del servizio on line. In tale contesto, tuttavia, il Garante, al fine di assicurare che la conoscenza dei dati personali, anche idonei a rivelare lo stato di salute, avvenga solo da parte dell'interessato o da persona da questo delegata, ritiene necessario che l'Azienda sanitaria, in qualità di titolare del trattamento, introduca nelle modalità di erogazione dei citati servizi specifiche misure di sicurezza per ridurre al minimo i rischi di accesso non autorizzato (art. 31

del Codice).

4.1. Con specifico riferimento al servizio di pagamento del corrispettivo per le prestazioni sanitarie erogate dall'Azienda sanitaria di Firenze attraverso la rete "Sportello amico" di Poste Italiane S.p.A., si ritiene che l'operatore di sportello debba verificare l'identità del soggetto che effettua il pagamento attraverso l'esibizione di un documento di riconoscimento e provvedere alla registrazione degli estremi dello stesso. Ciò, in analogia con le concrete modalità di ritiro allo sportello della documentazione relativa ad un destinatario determinato (es. raccomandata, plico postale).

Qualora l'operatore di sportello accerti che il soggetto che effettua il pagamento sia diverso dall'interessato, deve procedere all'erogazione del servizio solo previa esibizione, oltre al codice fiscale dell'interessato, anche del codice di prenotazione della prestazione sanitaria rilasciato dal CUP all'atto della prenotazione. In tal caso, la consegna della documentazione relativa all'avvenuto pagamento deve avvenire in busta chiusa o con modalità che non consentano in via diretta di visualizzarne il contenuto (es. foglio piegato e spillato) (cfr. provvedimento del 9 novembre 2005 citato). Ciò, in quanto la ricevuta fiscale reca, in chiaro, la descrizione della natura della prestazione sanitaria, che, in taluni casi, è idonea a rivelare lo stato di salute dell'interessato.

Il titolare del trattamento deve, inoltre, verificare che Poste Italiane S.p.A. fornisca agli incaricati del trattamento idonee istruzioni al riguardo, nonché effettuare controlli periodici -anche a campione- in merito al rispetto delle misure sopra descritte (artt. 28, 29 e 30 del Codice).

4.2. Con riferimento al servizio di pagamento delle prestazioni sanitarie offerto dall'Azienda sanitaria di Firenze attraverso il proprio sito Internet (<http://wiasf.cupmet-fi.it/ASFWeb/WICUP/pagamenti/ricercaAppuntamenti.do>), si ritiene che l'Azienda debba introdurre idonee misure volte a garantire che l'accesso ai dati personali, anche idonei a rivelare lo stato di salute, mediante l'utilizzo del suddetto servizio sia consentito solo all'interessato ovvero ad altro soggetto da questo delegato.

Ciò stante, il titolare del trattamento deve prevedere che l'utente che intende procedere al pagamento delle prestazioni attraverso il sito Internet dell'Azienda debba inserire in un apposito campo della maschera di accesso al predetto servizio di pagamento, oltre al codice fiscale dell'interessato, anche il codice di prenotazione della prestazione sanitaria rilasciato dal CUP all'atto della prenotazione.

#### **TUTTO CIÒ PREMESSO IL GARANTE:**

a) ai sensi dell'art. 154, comma 1, lett. c) del Codice prescrive all'Azienda sanitaria di Firenze di adeguare -entro 3 mesi dalla data di adozione del presente provvedimento- le operazioni di pagamento dei corrispettivi per le prestazioni sanitarie dalla stessa erogate effettuate attraverso la rete "Sportello amico" di Poste Italiane S.p.A. e tramite il proprio sito Internet alle misure indicate nel punto 4 del presente provvedimento;

b) ai sensi dell'art. 157 del Codice, richiede all'Azienda sanitaria di Firenze, di comunicare quali iniziative siano state intraprese al fine di dare attuazione al presente provvedimento entro i dieci giorni successivi al termine prescritto nella precedente lett. a). Il mancato riscontro alla presente richiesta è punito con la sanzione amministrativa di cui all'art. 164 del Codice.

Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'Autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 13 marzo 2014

IL PRESIDENTE  
Soro

IL RELATORE  
Soro

IL SEGRETARIO GENERALE  
Busia