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. Giovanni Buttarelli, segretario generale;

Esaminata la richiesta di verifica preliminare presentata dall'Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa ai sensi dell'art. 17 del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196);

Visti gli atti d'ufficio;

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

Relatore il dott. Mauro Paissan;

PREMESSO

1. Trattamento di dati biometrici di operatori sanitari e pazienti in processi di trasfusione del sangue
L'Azienda ospedaliera civile Maria Paternò Arezzo di Ragusa intende adottare un sistema di sicurezza trasfusionale per prevenire errori di identificazione di pazienti o delle unità di sangue in sede di trasfusioni e scongiurare le conseguenze gravissime che si determinerebbero in caso di errori.
Il progetto ruota intorno all'adozione di un terminale portatile a batterie -denominato *"Securblood"*- dotato di un lettore di codice a barre, di un sensore per la rilevazione delle impronte digitali, di un *display* a tastiera numerica corredato di un *software* che trasforma le immagini delle impronte digitali degli interessati (operatori sanitari e pazienti) in codici numerici (*template*). Mediante l'utilizzo del terminale e secondo le relative procedure tecniche ed amministrative si assicurerebbe la tracciabilità del sangue e la corretta associazione al paziente del campione di sangue prelevato e della sacca di sangue o emoderivati durante la trasfusione.

Secondo l'Azienda, il sistema permette di verificare se le unità di sangue da trasfondere sono le stesse assegnate dal servizio di immunoematologia e medicina trasfusionale (Simt) a un determinato paziente identificato con l'impronta digitale; in caso d'incongruenza dei dati, il sistema si blocca. Il sistema, basato sul riconoscimento biometrico, obbligherebbe poi il personale sanitario a presenziare alle operazioni di trasfusione garantendo la massima assistenza nei primi quindici minuti dall'operazione (tempo ritenuto appropriato per evidenziare eventuali reazioni trasfusionali). Ciò, in osservanza della Raccomandazione europea R (95)15 (capitolo 28, par. 2) sulla sorveglianza clinica.

L'Azienda ha quindi presentato a questa Autorità una richiesta di verifica preliminare ai sensi dell'art. 17 del Codice, corredata da una dettagliata relazione sul trattamento di dati biometrici ricavati dalla lettura delle impronte digitali degli operatori sanitari e dei pazienti interessati alla trasfusione.

2. Formato dei dati biometrici; modalità di registrazione e di trasmissione
In base a quanto attestato dall'Azienda, la raccolta dei dati biometrici (*enrollment*) avverrebbe tramite il lettore di impronte digitali facente parte del terminale. La procedura prevede che il paziente che deve essere sottoposto a trasfusione e l'operatore (infermiere o medico) appoggino un dito sul sensore biometrico, creando un *file* temporaneo contenente l'immagine dell'impronta digitale da trasformare in un algoritmo (il *template*). L'immagine verrebbe utilizzata esclusivamente per creare l'algoritmo e distrutta immediatamente dopo; da esso non sarebbe possibile creare a ritroso il *file* distrutto. Gli algoritmi verrebbero memorizzati all'interno dello stesso apparecchio.

L'Azienda precisa che il rilevatore non ha collegamenti in rete, né porte di comunicazione fisiche; non sarebbe quindi consentito accedere ai circuiti di memoria del dispositivo biometrico dall'esterno e l'estrazione dei dati sarebbe inibita.

L'operazione di registrazione degli operatori sanitari che eseguono trasfusioni di sangue o emocomponenti nel terminale destinato al reparto di competenza verrebbe effettuata da un incaricato dotato di una *password* d'accesso. Nel *data base* del terminale confluirebbero i seguenti dati: numero di *badge* personale, algoritmo dell'impronta digitale, numero di identificazione privato (*pin*) riservato e noto esclusivamente all'operatore. Gli algoritmi numerici delle impronte degli operatori verrebbero associati al numero di *badge* e al numero personale di identificazione. Una volta effettuata la registrazione dei dati, la *password* dell'incaricato della registrazione dell'operazione verrebbe disattivata immediatamente.

2.1. Viene precisato che la memorizzazione dell'algoritmo relativo all'impronta, riportato unicamente sul portatile collocato nel reparto ospedaliero interessato, non potrebbe essere estratto, né copiato o trascritto e nemmeno trasmesso al di fuori del terminale. Vengono ipotizzate robuste misure di sicurezza per la custodia del *server* della B.b.s. s.r.l.; un terzo *server* (posto in una *housing* in Francia) si attiverebbe in caso di guasti.

Il terminale registra non dati personali quali nome, cognome e data di nascita, ma unicamente codici numerici. I dati relativi alle operazioni eseguite durante una trasfusione (non contenenti il codice di *badge* dell'operatore) verrebbero trasmessi automaticamente dal terminale direttamente al *server* della B.b.s. s.r.l. fornitrice dei terminali Securblood

e, da questo, trasferiti al Servizio trasfusionale (Emonet) e a tutti i terminali dello stesso ospedale.

I dati da trasmettere al server nelle varie fasi del prelievo e trasfusione sono raccolti:

- durante la fase del prelievo (reparto, data e ora del prelievo, numero di *badge* dell'infermiere, numero di identificazione del paziente – consistente nel codice a barre del braccialetto -);
- all'inizio della trasfusione (reparto, data e ora inizio trasfusione, numero del *badge* dell'infermiere, numero del *badge* del medico, numero di identificazione dell'emocomponente e codice degli emocomponenti);
- alla chiusura della trasfusione (reparto, ora fine trasfusione, *badge* dell'infermiere e reazione trasfusionale).

I dati sopra menzionati sarebbero visibili nella sessione riservata del sito della B.b.s. s.r.l. tramite una *userid* e una *password* criptata in possesso del direttore del Simt, designato responsabile del trattamento.

Dal momento che il terminale è privo di connessioni fisiche, per la trasmissione dei dati a un *server* e viceversa verrebbe utilizzato un sistema con protocollo *Gprs/Ftp* utilizzando sim abilitate alla trasmissione *"machine to machine".*

L'Azienda ha previsto la possibilità di un rifiuto del trattamento dei dati biometrici da parte del dipendente o paziente: in questo caso, si assegnerebbe all'operatore sanitario un codice di identificazione personale e al paziente, un braccialetto da applicare sul polso con inciso un codice a barre (sistema ritenuto meno sicuro) da leggersi sempre mediante il terminale.

3. Durata della conservazione di dati
3.1 I dati del personale dell'Azienda (algoritmi delle impronte digitali, numeri di *badge* e pin) verrebbero conservati all'interno del terminale di competenza di ciascun reparto e cancellati, venendone a mancare la necessità, a cura dell'incaricato designato dal direttore del Simt e dotato di *password* d'accesso. I dati dei pazienti (algoritmi delle impronte digitali, codici della richiesta e *barcode* dei braccialetti) verrebbero invece cancellati automaticamente trascorsi sette giorni dalla richiesta trasfusionale, eventualmente prorogabili fino a un massimo di trenta dal direttore del Simt.

Infine, per quel che concerne i dati in codice numerico trasmessi al *server* della B.b.s.. s.r.l., se ne prevede la cancellazione ogni sei mesi, previa loro copia su supporto magnetico e invio al servizio trasfusionale di competenza.

4. Motivi addotti che rendono necessario l'utilizzo di dati biometrici in luogo di altri sistemi
4.1 L'Azienda ritiene che l'utilizzo del terminale, unitamente alle procedure da adottarsi, possa essere l'unico sistema idoneo per ridurre drasticamente la possibilità di un errore trasfusionale che ha conseguenze particolarmente gravi, fino al possibile decesso del paziente.

L'utilizzo del solo codice a barre apposto al braccialetto del paziente non assicurerebbe quel grado di certezza indispensabile per un'attività così pericolosa come quella della trasfusione del sangue o emoderivati; ciò, senza contare che, come accennato, l'impiego della rilevazione biometrica costringerebbe l'operatore sanitario a essere realmente vicino al paziente nei momenti di maggiore criticità dell'operazione di trasfusione.

5. Rispetto di alcuni adempimenti e delle misure di sicurezza
5.1. Le misure di sicurezza prospettate per la conservazione dei dati personali risultano dagli atti adeguate. Anche per quanto riguarda alcuni adempimenti previsti dal Codice (informativa, consenso e designazione degli incaricati), l'Azienda li ha presi in esame assicurando la loro attuazione. Ciò, salvo che quanto riguarda le società presso le quali saranno detenuti i dati per conto dell'Azienda, le quali dovranno essere opportunamente designate quali responsabili del trattamento ai sensi degli artt. 4, comma 1, lett. g) e 29 del Codice.

6. Necessità, liceità, finalità, proporzionalità e correttezza nel trattamento
6.1. La raccolta e la registrazione di impronte digitali e dei dati biometrici utilizzati per verifiche e raffronti nelle procedure di autenticazione o di identificazione sono operazioni di trattamento di dati personali riconducibili ai singoli interessati (art. 4, comma 1, lett. b)), alle quali trova applicazione la normativa contenuta nel Codice (Provv. 19 novembre 1999, in *www.garanteprivacy.it*, doc. web n. 42058; 21 luglio 2005, doc. web n. 1150679; 23 novembre 2005, doc. web n. 1202254; 15 giugno 2006, doc. web n. 1306530; 1 febbraio 2007, doc. web n. 1381983; doc. di lavoro sulla biometria del Gruppo Art. 29 dei garanti europei, Wp 80). La liceità del sistema deve essere pertanto valutata sul piano della conformità ai princìpi di necessità, liceità, finalità, proporzionalità e correttezza (artt. 3 e 11 del Codice), anche in relazione ai tempi di conservazione dei dati.

6.2. Con riguardo al trattamento di dati biometrici aventi lo scopo di identificare con elevato grado di certezza i dati dei sanitari, dei pazienti e i prodotti ematici relativi alle operazioni di trasfusione, deve rilevarsi che le operazioni da effettuare si caratterizzano per la loro delicatezza e pericolosità e trovano giustificazione nella garanzia che esse offrono per contenere errori possibili di scambi di dati e di sacche di sangue.

Ad avviso dell'Azienda, l'utilizzo di sistemi di autenticazione basati su tecniche biometriche secondo le modalità sopra

descritte darebbe una risposta idonea rispetto alla problematica degli errori, aumentando considerevolmente il grado di sicurezza nelle operazione da tenere sotto controllo, non esistendo un mezzo diverso parimenti efficace. Viene infatti considerato non esente da rischio assicurare con sistemi tradizionali l'autenticazione certa e univoca dei pazienti e degli operatori sanitari, nonché la verifica dei prodotti ematici in fase di trasfusione.

Il rispetto della specifica disciplina in materia (l. 195/2005; dd.lg. 207 e 261/2007; raccomandazione n. 5/2007 del Ministero della salute) obbliga l'Azienda a prestare la massima attenzione possibile alle operazioni da compiere in un settore così delicato in ragione dei dati trattati e dei rischi connessi, per assicurare l'incolumità e la salute del paziente e la tracciabilità del percorso delle unità di sangue e di emocomponenti dal donatore al ricevente e viceversa.

Può ritenersi quindi proporzionata la modalità prospettata dall'Azienda per il trattamento dei dati derivanti dalle impronte digitali (template), sebbene essi verrebbero memorizzati non su supporti in possesso di ciascun interessato (come di regola prescritto da questa Autorità a seguito di verifiche preliminari), ma su ciascun terminale in dotazione ai singoli reparti. Inducono in particolare a tale constatazione le caratteristiche dell'apparecchiatura utilizzata (priva di accessi fisici), le garanzie di sicurezza sopra menzionate, la circostanza che i dati rilevati sono privi di indicazioni nominative e, infine, l'obiettiva difficoltà di produrre per i pazienti singoli badge.

6.3. Per la durata di conservazione dei dati degli operatori sanitari, l'Azienda si è limitata a fornire le indicazioni e le procedure per la loro eventuale cancellazione. Al riguardo, deve ritenersi che tali dati debbano essere conservati per la sola durata in cui gli addetti ricoprono la qualità di incaricati del trattamento ed essere poi prontamente cancellati.

Per i pazienti è stato invece indicato, come termine di conservazione, quello di sette giorni dalla trasfusione, elevabile fino a un massimo di trenta su autorizzazione del direttore del Simt. Non viene però dichiarato in quali casi tale termine minimo possa essere così aumentato.

Riguardo a questi aspetti, i termini indicati non risultano incongrui, dovendosi tener conto della necessità di una più ampia conservazione connessa a particolare vicende che possono emergere nell'attività gestionale; casi che dovranno essere però disciplinati preventivamente dall'Azienda.

7. Notificazione del trattamento

7.1. Il progetto in esame non reca infine indicazioni per quanto riguarda la notificazione del trattamento ai sensi degli art. 37 e 38 del Codice. Per tale aspetto, come per quanto concerne le misure di sicurezza, restano ovviamente fermi gli obblighi previsti dal Codice, cui l'attuazione del progetto dovrà ovviamente conformarsi.

In relazione al sistema in esame risulta in conclusione necessario prescrivere, a garanzia degli interessati, alcuni accorgimenti e misure ai sensi dell'art. 17 del Codice, indicati nel seguente dispositivo.

TUTTO CIÒ PREMESSO IL GARANTE:

in relazione al progetto dell'Azienda Ospedaliera civile Maria Paternò Arezzo di Ragusa volto a trattare dati biometrici di operatori sanitari e pazienti mediante terminali dislocati nei vari reparti prescrive all'Azienda, ai sensi dell'art. 17 del Codice, di adottare i seguenti accorgimenti e misure:

1. designare opportunamente quali responsabili del trattamento le società che trattano i dati dell'Azienda, ai sensi degli artt. 4, comma 1, lett. g) e 29 del Codice, specificando analiticamente i compiti affidati anche per quanto riguarda l'osservanza delle misure di sicurezza (punto 5.1);
2. conservare i dati biometrici dei propri operatori sanitari (infermieri e medici) per la sola durata del relativo incarico (punto 6.3);
3. disciplinare preventivamente i casi in cui sia necessaria la conservazione dei dati biometrici dei pazienti fino ad un massimo di trenta giorni (punto 6.3);

Roma, 19 giugno 2008

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli