

Pre-intesa per il rinnovo dell'ACN della MG siglata in data 22 dicembre 2008

Analisi dell'art. 5 – Flusso informativo

Criticità sotto il profilo della protezione dei dati: considerazioni preliminari.

Premesso che:

- Le “informazioni elementari” trattate possono essere dati personali (art. 5 com. 2)

Ai sensi del comma 2 dell'art. 5 dell'ACN, le informazioni trattate dal medico di assistenza primaria e da questi trasmesse all'Azienda sanitaria competente “devono riferirsi al singolo caso”, **con specifica indicazione dell'assistito.**

Qualora al contenuto informativo sia associata l'indicazione del soggetto (persona fisica, nel caso di specie) al quale il contenuto informativo si riferisce, tali informazioni rientrano nella categoria dei **dati personali** ai sensi del decreto legislativo 196/2003 (cd. Codice privacy).

Ne discende la possibilità di un'ampia applicazione al caso in esame del Codice privacy, tanto con riferimento alla normativa sui dati personali, quanto con riferimento a quella sui dati sensibili, quanto, infine, con riguardo alla disciplina specificamente prevista a tutela dei dati sanitari (Titolo V – Trattamento di dati personali in ambito sanitario).

Si rammenta, infatti, che per “dati sensibili” si intendono, ai sensi dell'art. 4 comma 1 lettera d del Codice privacy “i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché **i dati personali idonei a rivelare lo stato di salute e la vita sessuale degli individui**”.

Nell'ambito della categoria "dati sensibili" il Codice privacy contempla poi la sotto categoria dei "dati sanitari".

Più specificamente, sono "dati sanitari" i dati sensibili idonei a rivelare lo stato di salute e la vita sessuale dell'interessato **qualora (1) essi siano trattati da organismi sanitari pubblici e da esercenti professioni sanitarie per perseguire (2) finalità di tutela della salute o dell'incolumità fisica dell'interessato, di terzi o della collettività.**

Ne deriva che l'art. 5 potrebbe contemplare un flusso informativo avente ad oggetto in grande misura dati personali e, nell'ambito di questi, sia dati sensibili che dati sanitari e che dunque la regolamentazione di tale flusso informativo possa ricadere in ampia misura nella disciplina del Codice privacy.

Qualora invece le informazioni siano trattate in forma anonima e/o in forma aggregata (caso cui si fa riferimento per esempio al comma 3 dell'art. 5: trasmissione dei dati dall'Azienda ai componenti dei Comitati Aziendali e Regionali) non si applicherà il decreto legislativo 196/2003, in quanto se al contenuto informativo non è connessa l'informazione circa l'identità del soggetto cui quel contenuto si riferisce non vi sono problemi di privacy.

Date le suddette premesse, dall'analisi tecnico giuridica dell'art. 5 dell'ACN possono rilevarsi le seguenti criticità sotto il profilo della privacy:

1 - Titolarità dei dati personali (art. 5 comma 3)

Secondo l'art. 5 comma 3 "le suddette informazioni **sono patrimonio della stessa Azienda e dei medici** e vengono utilizzate per le finalità di comune interesse".

Dalla dizione letterale della norma parrebbe doversi desumere una situazione di "con-titolarità" dei dati personali trattati tra Azienda sanitaria e medici.

Pare opportuno ricordare che per "titolare" ai sensi dell'art. 4 comma 1 lettera f del D.Lgs. 196/2003 si intende "la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente,

associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza”

Da tale situazione di “con-titolarietà” deriverebbe, quindi, una posizione di equiparazione tra Azienda e medico con riferimento alle decisioni in ordine alle finalità e alle modalità di trattamento dei dati, ivi compreso il profilo della sicurezza.

In concreto, una tale situazione di “con-titolarietà” dei dati potrebbe risultare poco opportuna allo scopo giustamente perseguito di una snella e organizzata gestione del patrimonio informativo, ovvero potrebbe essere mantenuta qualora si disciplinassero nel dettaglio competenze e responsabilità di ciascun “con-titolare”.

Infatti, nel caso in cui venisse mantenuta la “con-titolarietà”, Azienda e medici dovrebbero **congiuntamente prendere le decisioni che si rendessero di volta in volta necessarie in relazione alle finalità e alle modalità di trattamento dei dati. Ovvero si dovrebbe provvedere a stabilire, anticipatamente rispetto all’inizio del trattamento e con il debito dettaglio, le rispettive competenze e responsabilità.**

Ci permettiamo di suggerire, eventualmente, la scelta di un diverso assetto delle rispettive responsabilità in ordine al trattamento dei dati tra Azienda e medici, eventualmente introducendo, accanto alla figura del titolare anche quella del o dei responsabili del trattamento (si veda l’art. 4 comma 1 lett. g Codice privacy) e individuando nell’Azienda il titolare del trattamento e nei medici i singoli responsabili.

Pertanto alla comprensione delle effettive modalità di gestione dei dati “patrimonio comune” e delle rispettive responsabilità in ottica privacy tra Azienda e medici, sarebbe di conforto una più esplicita descrizione delle citate “finalità di comune interesse”.

Una volta individuate tali finalità, ai sensi della norma citata, sarà poi sulla base di quelle che dovrà essere valutata la legittimità del trattamento dei dati.

Poiché, infatti, ai sensi dell’art. 11 comma 1 del Codice privacy, i dati personali oggetto di trattamento devono essere **“trattati in modo lecito”** e, più specificamente, **“raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con**

tali scopi”, ed inoltre i dati trattati “non (devono essere) eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati”, al fine di garantire la legittimità del trattamento risulta opportuna una previa indicazione, sia pure di massima, delle finalità del trattamento stesso.

2 - Le finalità di *governance* del SSR (art. 5 comma 3)

In considerazione di quanto sopra illustrato, la stessa espressione “finalità di *governance* del SSR” dovrebbe essere auspicabilmente specificata con modalità più esaustive.

In proposito va ripreso un principio di grande rilevanza, con riferimento al trattamento “lecito” dei dati personali: il principio di necessità, in base al quale il dato personale va trattato solo qualora tale trattamento sia assolutamente indispensabile alla finalità perseguita, altrimenti l’informazione va trattata in forma anonima (art. 11, comma 1 lett. d: “I dati personali oggetto di trattamento sono (...) non eccedenti rispetto alle finalità per i quali sono raccolti e successivamente trattati”).

Con specifico riguardo ai sistemi informativi, l’art. 3 comma 1 del Codice privacy prescrive quanto segue: “I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l’utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità”.

Nella progettazione e realizzazione del flusso informativo descritto all’art. 5 dell’ACN sarebbe quindi d’uopo, al fine della sua conformità al Codice privacy, prevedere il trattamento dei dati personali **solo qualora esso risulti necessario** e, viceversa, provvedere all’anonimizzazione dei dati in tutti gli altri casi, **quando cioè la finalità per cui le informazioni sono trattate non richieda l’individuazione dell’interessato**.

In particolare, riprendendo quanto citato nelle premesse, dato comunque un trattamento effettuato da organismi sanitari e/o esercenti le professioni sanitarie, è differente la disciplina normativa applicabile a seconda che esso sia effettuato a scopo di tutela della salute dell’interessato, di terzi o della collettività (in questo caso si applicano gli articoli sui dati sanitari, di cui al Titolo V – Trattamento di dati personali in

ambito sanitario, artt. 75 e segg.), da un trattamento effettuato da questi stessi soggetti a scopi diversi (per esempio, amministrativi, contabili, etc...).

In questo ultimo caso, infatti, si esce dall'ambito di disciplina specifico del dato sanitario, per tornare all'applicazione delle norme del Codice privacy (di carattere più generale) relative ai dati personali e sensibili.

Risulta quindi **molto importante** chiarire quali siano di volta in volta le finalità di *governance* (Finalità sanitarie? Tutela della salute del singolo e della collettività? Amministrative? Economico-finanziarie? Organizzative? Altro?...) che rendono necessario il trattamento, al fine di sapere quali articoli del Codice privacy applicare.

3 - Valutazione della sicurezza delle infrastrutture (Art. 5 comma 4)

L'opportuna valutazione della sicurezza della infrastrutture potrà essere effettuata avendo quali parametri di confronto e di supporto le reti regionali già esistenti (Lombardia, Emilia – Romagna, Puglia, Abruzzo, Sardegna...).

La valorizzazione delle esperienze già a regime - quali il sistema CRS-SISS lombardo o il SOLE emiliano-romagnolo - potrà consentire un'adequata verifica degli altri sistemi di sicurezza regionali e un allineamento degli stessi a livello nazionale. Sarà così possibile avviare il flusso informativo nei tempi (piuttosto ristretti) previsti dall'ACN.

L'allineamento delle esperienze regionali a livello nazionale potrebbe costituire tuttavia passaggio non trascurabile al fine di assicurare i requisiti dell'interoperabilità e della cooperazione applicativa.

4- Necessità dell'aggiornamento del dato (Art. 5 comma 2)

Rientra nei criteri che sovrintendono al trattamento del dato personale (e a maggior ragione del dato sanitario) quello del suo necessario aggiornamento (art. 11 comma 1 lett. c). Qualora il dato non sia aggiornato, l'interessato può richiederne l'aggiornamento ai sensi dell'art. 7 comma 3 lett. a (si pensi, con

particolare riferimento ai dati sanitari, ai danni derivanti al paziente dal trattamento di un dato non aggiornato).

La previsione di cui all'art. 5 comma 2 dell'ACN secondo cui il dato deve essere trasmesso con cadenza mensile entro il decimo giorno del mese successivo può risultare per un verso dilatata, qualora si tratti di informazioni a contenuto sanitario da impiegarsi a tutela della salute del singolo e della collettività, e dall'altro in alcuni casi adempimento che potrebbe risultare gravoso per i medici, qualora invece si tratti di informazioni a contenuto sanitario impiegate a scopo amministrativo (dunque, in base a quanto premesso non di dati sanitari, ma di dati sensibili o personali).

5 – Necessità di apposita informativa e consenso informato

Con riguardo a quelli, tra i dati trattati nel flusso informativo, aventi natura di dati sanitari, sarà necessario procedere alla raccolta del consenso informato del paziente.

Affinché tale consenso sia **effettivamente informato**, sarà necessaria la predisposizione di un'informativa adeguatamente esaustiva, che descriva in modo sufficientemente dettagliato all'interessato le caratteristiche, i contenuti, le finalità e le peculiarità tecniche del flusso informativo.

Si legga, a questo riguardo, in particolare l'art. 78 comma 5, il quale, con riferimento all'informativa resa dal medico di medicina generale precisa: "L'informativa resa ai sensi del presente articolo **evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici** per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati: (...) c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica".

6 – La costituzione di uno o più archivi informatici

Il flusso informativo medici-Azienda, così come descritto all'art. 5, potrebbe comportare la creazione di uno o più archivi digitali contenenti informazioni sanitarie, collocati fisicamente presumibilmente presso le Aziende o le Regioni.

A questo proposito, oltre a ribadire la necessaria e generale applicazione delle misure di sicurezza previste dal Codice privacy e dall'allegato B, con particolare riguardo ai dati sensibili e sanitari, va citato l'art. 22 del Codice, il cui comma 6 stabilisce che i dati sensibili (e dunque anche i dati sanitari) contenuti in banche di dati e tenuti con l'ausilio di strumenti elettronici, "sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, **li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi** e permettono di identificare gli interessati solo in caso di necessità". Il successivo comma 7 aggiunge: "I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo".

Le indicate prescrizioni legislative sono ribadite in relazione alla predisposizione delle misure minime di sicurezza, la cui mancata adozione è, come noto, penalmente sanzionata dal nostro legislatore. L'abbinamento dato identificativo-dato sanitario dovrà avvenire solo a seguito di un'ulteriore operazione di decifratura o di immissione di codice identificativo.

La realizzazione in termini tecnici delle indicazioni del legislatore pare quindi configurare la separazione fisica, a livello di database, dei dati identificativi rispetto a quelli idonei a rivelare lo stato di salute. Il *matching* tra i dati identificativi e quelli sensibili dovrà poi essere effettuato, a livello d'interfaccia utente, tramite l'inserimento di un codice identificativo univoco del paziente in modalità sicura.

Roma, 9 gennaio 2009

Il Gruppo di lavoro "Sicurezza e Privacy" della SIT

Società Italiana Telemedicina e sanità elettronica