

Interviste



SANITA' E SICUREZZA INFORMATICA, FACCIAMO IL PUNTO...

Abbiamo incontrato Paolo Salin, Country Manager di Kroll Ontrack Italia, per inquadrare la situazione dei sistemi informativi in sanità, e la protezione della privacy in Italia.

L'informatizzazione della sanità, pone anche una serie di interrogativi su sicurezza e privacy.

Il processo di informatizzazione della sanità sta diventando una realtà anche in Italia, un passaggio obbligato per le strutture sanitarie ma che inevitabilmente solleva questioni di sicurezza confermate anche dai recenti dati dell'Osservatorio Nazionale per la Sicurezza Informatica (ottobre 2008).

Dalla ricerca emerge, infatti, un elevato rischio per la privacy dei pazienti considerando che il 60% delle ASL coinvolte nell'indagine dichiara di non disporre di strumenti adeguati per la protezione dei dati sensibili; un numero che indubbiamente fa riflettere ed è innegabile che per la tutela della privacy vi sono ampi margini di miglioramento.

Il problema tuttavia sembra essere più di ordine legale, direi anche organizzativo, che tecnologico. Nel primo caso servono probabilmente direttive più mirate per una corretta ed efficace gestione dell'informazione sanitaria nel futuro prossimo, nel secondo una maggiore armonia tra le differenti sperimentazioni tecnologiche che alcune regioni hanno avviato nel campo della sanità elettronica.

Quale è la situazione normativa sui dati sanitari in Italia?

La normativa sulla privacy e il relativo Disciplinare Tecnico contengono diversi tipi di prescrizioni per il trattamento dei dati sanitari. Il problema è che la tecnologia è in continua evoluzione e apre scenari sempre nuovi per la fruibilità del dato, la sanità online ne è un esempio. Il Garante ha di recente dimostrato grande attenzione al tema e presto dovremo assistere ad un intervento sulla cartella clinica e sul fascicolo sanitario elettronico teso a delineare delle linee guida comuni per gli operatori sanitari nella tutela della privacy dei cittadini.

Quale tutela dei dati sensibili, per evitare furti (caso Express Script)?

Garantire la riservatezza dei dati sensibili è una sfida, tanto più in ambito sanitario. Tuttavia sarebbe un errore pensare all'informatizzazione della sanità come a una minaccia. I casi di furto di dati clinici negli Stati Uniti, come il recente esempio del caso Express Script, certamente devono far riflettere anche in Italia sulle misure di sicurezza attualmente implementate nelle strutture sanitarie, non creerei però allarmismo.

È vero che ogni anno negli Stati Uniti sono oltre 250.000 le vittime di furto di identità medica, però è bene ricordare che nella maggior parte dei casi la minaccia viene dall'interno della struttura. Purtroppo è la componente umana e non tecnologica a mostrare "punti deboli". L'adeguatezza dei

sistemi di sicurezza deve ad ogni modo essere valutata e migliorata, gli strumenti per farlo già esistono.

La vulnerability assessment e la risk analysis sono metodologie conosciute che possono dimostrare la loro validità anche in ambito sanitario. Riguardo alla componente umana sarebbero invece opportune attività di sensibilizzazione e di formazione interne alle strutture sanitarie, poiché gli operatori sanitari che accedono ai dati sensibili devono essere consapevoli delle norme di sicurezza e del corretto comportamento da tenere. A tale proposito è auspicabile la corretta definizione di policy interne con il duplice obiettivo di comunicare e di regolamentare l'uso delle tecnologie informatiche nell'Ente.

Cancellazione sicura dei dati per conformità delle aziende sanitarie alle normative vigenti

Uno dei momenti più rischiosi per la riservatezza dei dati è – diversamente da quanto si crede - il termine del ciclo di vita del dato stesso e del supporto informatico che lo contiene. Quasi sempre tutti gli sforzi di proteggere i dati sensibili sono vanificati proprio in questa fase. Si pensi che in oltre l'80% degli hard disk usati/dismessi, provenienti anche da ambienti business, i dati sono spesso recuperabili senza grossa difficoltà.

Una formattazione non distrugge il dato, semplicemente lo “nasconde”. La legge sulla privacy è molto chiara a questo proposito, i dati sensibili che si trovano conservati su supporti di memorizzazione non utilizzati devono essere distrutti con modalità idonee a renderli non intelligibili e tecnicamente non ricostruibili.

Questo risultato può essere garantito solo da appositi strumenti certificati per la cancellazione sicura che implementano idonee tecniche di sovrascrittura o di smagnetizzazione del supporto. Le strutture sanitarie devono quindi garantire la sicurezza del dato lungo l'intero arco del ciclo di vita che comprende anche la dismissione.

A questo proposito, negli Stati Uniti, le soluzioni di cancellazione sicura (e di recupero dati) di Kroll Ontrack hanno ricevuto l'approvazione e sono state giudicate idonee dall'American Hospital Association per le esigenze di sicurezza dei suoi oltre 7000 membri.

www.ontrackdatarecovery.it

(Tratto da www.forumhealthcare.it)
