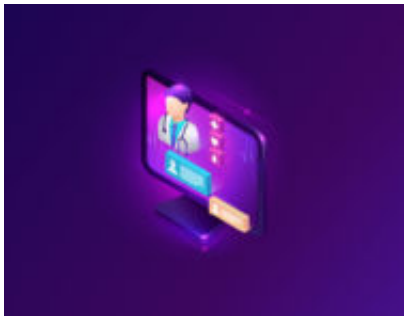
L'approvvigionamento ICT di un ospedale: le questioni da affrontare

Author : Francesco Maldera

Date : 18 Marzo 2020



“Dottore, stia attento...”

Aiutare le grandi strutture sanitarie (pubbliche o private) a effettuare un percorso finalizzato a ridurre i rischi per i dati personali è un mestiere difficile. Di solito esiste un *committment* forte da parte del vertice aziendale che, tuttavia, si infrange, spesso, su uno scoglio che è abbastanza noto in letteratura (illuminante il saggio di Koppel, Smith,Blythe, Kothari)[1] e che suona, più o meno, così *“You want my password or a dead patient?”.*

Infatti il **punto di vista dei clinici**, cioè dei professionisti (medici e non) che si occupano della salute dei pazienti, è che loro trattano dati, appunto, clinici e non si preoccupano del fatto che i dati clinici sono dati personali (secondo il GDPR, appartenenti alle particolari categorie di dati personali) e che, pertanto, devono essere tutelati. Il loro obiettivo è migliorare la salute del paziente: costi quel che costi. Le regole di sicurezza informatica e di protezione dei dati personali sembrano assurde, inutili e faticose da applicare.

Inoltre, un’ulteriore fatica è quella di far percepire loro che, ormai, in (quasi) tutti i **dispositivi medici** che funzionino con l’aiuto dell’elettricità ci sono **dati personali** e che, quindi, è necessario applicare alcune misure di sicurezza: che sia il saturimetro oppure l’acceleratore lineare, ognuno, nel suo “piccolo” o “grande”, contiene un minimo dispositivo “interno” (la sua memoria) che trattiene dati riguardanti la salute del paziente.

E molta memoria c’è negli strumenti di comunicazione che i clinici, sempre in buona fede e sempre per convergere verso la buona salute del paziente, utilizzano disinvoltamente scambiandosi immagini radiologiche su Whatsapp oppure inviando email con esami clinici senza curarsi se li mandano dalla propria casella ad uso personale (tipicamente poco protetta) o da quella istituzionale fornita dall’organizzazione (che si suppone sia stata *costruita* più professionalmente e, quindi, meno vulnerabile).

“Dottore, stia attento...” è l’esortazione più frequente. Ma pochi ci credono.

L’importanza di cominciare bene

Consapevole delle enormi difficoltà che, spesso, si incontrano nel settore sanitario quando si parla di cybersecurity o privacy, l’European Union Agency for Cybersecurity[2] (ENISA) ha voluto cominciare a sciogliere la matassa cominciando dalla fase cruciale per tutta la filiera della cura ed assistenza clinica: l’approvvigionamento di prodotti e servizi di una struttura sanitaria. Ha, quindi, pubblicato le *“Procurement Guidelines for Cybersecurity in Hospitals”*[3] (le Linee Guida per la Sicurezza Informatica nell’Approvvigionamento degli Ospedali) che offrono utili consigli per l’acquisizione di beni e servizi che, già in partenza, dovrebbero poter ridurre al minimo i rischi informatici e sui dati personali.

Il documento parte da alcuni dati significativi:

- è stato calcolato che, negli ospedali statunitensi, funzionano, in media, 10 dispositivi connessi per ciascun paziente ricoverato;
- è emerso che, la maggior parte di questi dispositivi, sono manutenuti da soggetti (la stessa ditta produttrice o altri soggetti) che si collegano tramite connessioni remote.

Questi due elementi, se vogliamo apparentemente banali, fanno scorgere, con una certa immediatezza, la punta dell’iceberg delle **vulnerabilità** che possono essere presenti nei sistemi informativi ospedalieri (HIS).

Anche il Garante per la Protezione dei Dati Personali ha sentito la necessità, conformemente a quanto prevede l’art. 57 par. 1 lettera d) (*“promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento”*), di incidere sulla corretta acquisizione dei dispositivi medici annunciando una collaborazione con CONSIP per inserire idonee misure a tutela dei dati trattati, come ad esempio l'impossibilità per il fornitore, che esegue un'attività di manutenzione a distanza dell'apparecchio, di accedere direttamente ai dati anagrafici dei pazienti presenti nelle immagini diagnostiche[iv]. Il Garante è stato mosso dalla approfondita conoscenza di casi in cui i manutentori hanno approfittatto della propria posizione privilegiata ed hanno utilizzato illecitamente dei dati personali presenti nei dispositivi medici[v].

Il ciclo dell’approvvigionamento

L’ENISA, nel sollecitare la sensibilizzazione delle strutture ospedaliere, definisce le fasi standard del ciclo dell’approvvigionamento: pianificazione, acquisizione ed esercizio e gestione. In ciascuna di queste fasi è necessario assumere specifici comportamenti finalizzati a garantire la **sicurezza delle informazioni** oltre che la tutela dei dati personali.

Tuttavia, l’ENISA suggerisce comportamenti comuni a ciascuna fase che, spesso, vengono trascurati:

- *coinvolgimento della struttura che gestisce i sistemi informativi aziendali*; gli attori che, di solito, partecipano alla definizione dei requisiti dei dispositivi medici appartengono alla

struttura dell'ingegneria clinica e alla specifica struttura sanitaria dove il dispositivo andrà ad operare; come è noto, tuttavia, l'integrazione dei dispositivi nel sistema informativo ospedaliero richiede una profonda conoscenza delle infrastrutture di comunicazione e di elaborazione esistenti e, quindi, il coinvolgimento di chi le gestisce ovvero del servizio ICT ospedaliero; senza questo coinvolgimento si rischia di introdurre pesanti vulnerabilità nell'intero sistema oppure, come di solito accade, di creare *isole* integrabili al prezzo di considerevoli inefficienze;

- *gestione delle vulnerabilità*; in ogni momento dell'approvvigionamento è necessario che ci sia una specifica attenzione alle vulnerabilità sia da parte dell'organizzazione cliente (in questo caso l'ospedale) sia da parte del fornitore che, periodicamente, deve farsi parte diligente nella segnalazione delle vulnerabilità che emergono nel corso della fornitura (scoperte magari in altri contesti);
- *definizione di una politica degli aggiornamenti hardware e software*; non è possibile pensare di mantenere in esercizio sistemi che scontano la naturale obsolescenza; questo vale sia per le componenti hardware (che spesso non *reggono* gli aggiornamenti software) sia per i software di base ed applicativi; occorre, quindi, stabilire intervalli certi per effettuare verifiche e, se necessario, procedere agli aggiornamenti;
- *difesa delle comunicazioni senza fili*; i sistemi di comunicazione senza fili costituiscono un elemento di flessibilità molto diffuso soprattutto in luoghi dove il cablaggio è difficile o impossibile ma, al tempo stesso, possono diventare gli *anelli deboli* dell'intero sistema informativo ospedaliero; diventa, quindi, determinante stabilirne le modalità di esercizio e le relative misure di riduzione del rischio;
- *definizione di politiche di test*; le fasi che precedono l'avvio in esercizio dei dispositivi medici sono cruciali per comprendere a fondo gli effetti dell'interazione con i sistemi esistenti oltre che la loro effettiva funzionalità nel contesto operativo; spesso queste fasi sono trascurate nella definizione di quelle che l'ENISA chiama Request for Proposal (RfP) e che, nel contesto italiano, sono i capitolati speciali di gara;
- *definizione dei piani per assicurare la continuità*; nelle strutture sanitarie, soprattutto in quelle ospedaliere, la continuità del servizio è un elemento essenziale che è necessario valutare in fase di pianificazione, implementare rigorosamente in fase di avvio in esercizio e verificare periodicamente durante le gestione corrente; naturalmente, anche questo è un aspetto che bisogna definire con precisione insieme al partner che fornirà il prodotto/servizio (tipicamente già nella RfP);
- *definizione di programmi di audit e di specifiche di logging*; la *storia d'uso* di una risorsa (sia essa un dispositivo medico oppure un servizio acquisito all'esterno) è un elemento fondamentale per consentire di comprendere il reale livello di rischio ad essa associato; quindi, diventa fondamentale poter condurre attività di auditing (sull'uso ordinario ma anche sugli interventi manutentivi) supportata adeguatamente dal logging delle operazioni svolte;
- *uso della cifratura*; è opportuno precisare che la cifratura non è, in sé, una misura di riduzione del rischio; in qualche caso, se maneggiata con superficialità, può diventare un elemento che aumenta il rischio (per esempio di indisponibilità di dati personali); è, invece, uno degli strumento attraverso il quale è possibile introdurre misure di sicurezza che possono consistere nella pseudonimizzazione ovvero nella anonimizzazione.

Difficile ma non impossibile

I consigli dell'ENISA, per chi si occupa professionalmente di questa materia, sembrano ovvi e quasi banali. Esistono, tuttavia, due ostacoli che si presentano spesso nelle strutture sanitarie:

- i clinici, oltre a quello che è stato già detto nell'introduzione, pensano che i meccanismi richiesti dalla cybersecurity (verifica periodica dei piani di continuità, attività di auditing, ecc.), da eseguire con la loro concreta collaborazione, sottraggano risorse preziose alla cura dei pazienti (in particolare il tempo);
- clinici e informatici parlano lingue diverse; un famoso saggio del 2013[6] tipizza questa divergenza che può avere effetti devastanti sulla sicurezza dei sistemi informativi ospedalieri.

È molto importante, dunque, cercare di coinvolgere i clinici, anche con l'aiuto degli ingegneri clinici, in un *assessment* a raggio più ampio degli aspetti tipicamente diagnostici o terapeutici: sfida difficile, ma non impossibile.

Note

[1] https://pdfs.semanticscholar.org/c74b/d5c43fcb11094dee5ce616d8df61ebce14dd.pdf?_ga=2.267335054.1452898703.1582882795-1984855386.1582882795

[2] https://www.enisa.europa.eu/

[3] https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services/at_download/fullReport

[4] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9283047#2

[5] https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9144941#3

[6] https://www.researchgate.net/profile/Ross_Koppel/publication/242016935_Healthcare_information_technology's_relativity_problems_A_typology_of_how_patients'_physical_reality_clinicians'_mental_models_and_healthcare_information_technology_differ/links/568fb62f08aef987e56b5ff0/Healthcare-information-technologys-relativity-problems-A-typology-of-how-patients-physical-reality-clinicians-mental-models-and-healthcare-information-technology-differ.pdf

Articolo a cura di **Francesco Maldera**