autore

Enrico Menghi

Fisico medico Istituto Scientifico Romagnolo per lo studio e la cura dei tumori, Mendola (FC)

La sicurezza il ruolo del fisi

Tecnologia e sicurezza. Qual è il ruolo del fisico medico? Abbiamo chiesto al dott. Menghi di ripercorrere con noi tutti i passaggi che rendono oggi la figura del fisico medico cruciale nel garantire la sicurezza delle procedure cliniche di competenza delineando i contorni di una collaborazione sempre più stretta con i servizi informatici e con quelli di ingegneria clinica

È innegabile che a partire soprattutto dal decennio appena trascorso si sia assistito ad una irreversibile digitalizzazione e globalizzazione delle nostre abitudini quotidiane sia per quel che concerne il privato sia per ciò che interessa la sfera professionale lavorativa.

Le quantità di informazioni digitali con cui costantemente ci troviamo ad interagire hanno subito e stanno subendo incrementi esponenziali nonché rapidi mutamenti a causa della costante ricerca, e quindi sviluppo, delle moderne innovazioni tecnologiche.

In ambito sanitario non di meno, gli apparecchi medicali non dotati di un proprio software proprietario stanno rapidamente scomparendo da un loro utilizzo clinico, mentre la possibilità di una messa in rete ospedaliera di un qualsiasi nuovo dispositivo elettromedicale risulta essere quasi all'ordine del giorno.

Il tema della sicurezza informatica, o *cybersecurity*, dei dispositivi medici, e quindi dei dati personali, spesso sensibili, contenuti all'interno del dispositivo e/o sempre più circolanti nelle reti ospedaliere, ha assunto un ruolo di primaria importanza.

Da qui la necessità ed il dovere di proteggere e regolamentare in modo efficace i diritti degli interessati in un mondo digitalizzato e globalizzato, per poter garantire al contempo il corretto trattamento dei dati personali digitali, ai fini del loro utilizzo nella cura e nella ricerca scientifica.

Alla luce delle recenti linee guida internazionali della *Food and Drug*

dei dati: co medico 2.0

Administration (FDA) [1], nonché dalla Direttiva Europea 2016/679 [2], in vigore dal maggio 2018, in materia di sicurezza informatica del dato digitalizzato, risulta determinante che anche a livello nazionale ci si avvii nella direzione di una gestione ed organizzazione della materia atta alla messa in sicurezza di tutto ciò che sempre più interessa la tutela del paziente in primis e la tutela di tutti i professionisti operanti nel SSN.
Le raccomandazioni dell'ente governativo statunitense, in particolare emanate dal Centro per le Apparecchiature Mediche e Radiologiche (*Center for Devices and Radiological Health, CDRH*), hanno il compito di fornire un completo scenario sul tema, basandosi sulla gestione e valutazione del rischio, e possono essere applicate a tutti i dispositivi medici in commercio includendo:

1. dispositivi medici provvisti di software (firmware incluso) o parti di software programmabili;
2. software intesi come dispositivi medici, incluse applicazioni mediche per dispositivi mobili (tablet, smartphone).

Come specificato dalle linee guida, l'FDA riconosce che la sicurezza informatica di un dispositivo medico è una responsabilità condivisa che coinvolge più parti, comprese le strutture di assistenza sanitaria, i pazienti, i fornitori e produttori di dispositivi medici.
Viene evidenziato come il mancato mantenimento della sicurezza informatica possa portare a compromettere le funzionalità del dispositivo, fino alla perdita di dati (medici o personali) o della loro disponibilità ed integrità, o anche all'esposizione di questi ad altri dispositivi connessi che potrebbero essere fonti di minacce alla sicurezza. Una mancanza di questo tipo può avere il potenziale per provocare gravi danni, anche irreparabili, alla salute del paziente.

Una efficace gestione del rischio nella sicurezza informatica ha lo scopo fondamentale di ridurre il rischio per i pazienti, diminuendo la probabilità che la funzionalità del dispositivo utilizzato venga, intenzionalmente o meno, compromessa a causa di una *cybersecurity* inadeguata. Dunque un programma efficace di gestione del rischio di sicurezza informatica dovrebbe comprendere tutte le fasi che costituiscono il cosiddetto "periodo di vita" del dispositivo: dall'immissione sul mercato alla fase di post-marketing, affrontando quindi il tema della sicurezza

del dispositivo a partire dalla sua ideazione fino alla sua obsolescenza.

Da quanto suggerito nel documento, nella fase precedente all'immissione sul mercato, l'approccio dovrebbe opportunamente affrontare i seguenti passaggi:

a. individuazione delle risorse, minacce e vulnerabilità;
b. valutazione dell'impatto delle minacce e vulnerabilità sulla funzionalità del dispositivo e sugli utenti finali/pazienti;
c. valutazione della probabilità di una minaccia e che una vulnerabilità venga sfruttata per scopi non autorizzati;
d. determinazione dei livelli di rischio e strategie di mitigazione adeguate;
e. valutazione dei criteri di accettazione del rischio e dei rischi residui.

Tuttavia, poiché i rischi di sicurezza informatica per i dispositivi medici sono in continua evoluzione, non è possibile eliminarli completamente nella sola fase di *premarketing* descritta sopra. È quindi essenziale che i produttori attuino dei veri e propri programmi completi di gestione del rischio della sicurezza informatica. Tali programmi di *cybersecurity* dovrebbero evidenziare e affrontare le vulnerabilità che potrebbero permettere l'accesso non autorizzato, la modifica, l'uso improprio o il non utilizzo o l'uso non autorizzato delle informazioni memorizzate, oltre all'accesso, o il trasferimento da un dispositivo medico a un destinatario esterno, che potrebbe condurre ad un certo danno per il paziente. I produttori sono pertanto invitati, dalle linee guida FDA, a rispondere in modo tempestivo per identificare ed affrontare eventuali vulnerabilità nei propri dispositivi.

Tipiche criticità nella stesura di un programma di *cybersecurity* possono riscontrarsi nei punti di seguito elencati:

a. il monitoraggio costante delle sorgenti da cui derivano le informazioni di sicurezza informatica per l'identificazione e l'individuazione delle vulnerabilità e dei rischi;
b. il mantenimento di solidi processi di aggiornamento dei software (compreso il monitoraggio di eventuali componenti installati da terze parti, nonché la verifica della progettazione e validazione degli aggiornamenti e delle patch che vengono utilizzati per arginare tali vulnerabilità);
c. la capacità di comprendere, valutare e rilevare la presenza e l'impatto di una vulnerabilità;
d. l'uso di opportuni modelli per definire con chiarezza come mantenere la sicurezza e le prestazioni essenziali di un dispositivo attraverso lo sviluppo di appropriate procedure che proteggono e riparano da una possibile messa a rischio;
e. l'adozione e la messa in pratica di una politica coordinata e condivisa sul tema vulnerabilità di un dispositivo medico.

Ulteriori informazioni *postmarketing* sulla qualità della sicurezza informatica del dispositivo medico possono provenire da una molteplice serie di fonti, tra cui ricercatori in tema di sicurezza, in-house test, fornitori di software o di tecnologie hardware, strutture sanitarie. La condivisione e la diffusione delle informazioni sulla sicurezza informatica riguardanti le vulnerabilità e le minacce cui potrebbe essere soggetto il dispositivo medico che si intende utilizzare, è parte integrante di un efficace programma di *cybersecurity*.
Come accennato, la compromissione della sicurezza o delle prestazioni essenziali di un dispositivo può causare danno al paziente ed è necessario un intervento per evitare o ridurre tale danno. Il processo che permette di identificare e modellizzare potenziali minacce (*threat modelling*) diviene di fondamentale importanza per comprendere e valutare le possibili vulnerabilità del dispositivo. I potenti strumenti del *threat modeling* vengono anche utilizzati nella valutazione delle soluzioni proposte e sono in grado di quantificare o meno quanto il rischio di danno al paziente sia ragionevolmente controllato in termini di indici di vulnerabilità e sicurezza.
L'importante figura professionale del Fisico Medico diviene pertanto centrale nella gestione e nella sicurezza dei dati clinici e di ricerca scientifica, trovandosi a collaborare quotidianamente coi Servizi Informatici e le Ingegnerie Cliniche presenti nelle strutture sanitarie, attuando e suggerendo soluzioni di *risk management*. Egli è inoltre titolare del controllo e della protezione di tutti i dispositivi medici dell'area Radiologica, organizzando ed attuando gli appropriati programmi di assicurazione della qualità previsti dalla legislazione vigente (D.Lgs. 187/00). L'Associazione Italiana di Fisica Medica (AIFM), che raccoglie in sé più di 1000 soci iscritti nel panorama Italiano, partecipa attivamente all'argomento ed intende approfondire il tema della *cybersecurity* anche alla luce del Report n. 10 del 2013 sulla "Progettazione, acquisizione, implementazione e gestione di un sistema RIS/PACS" [3]. ■

BIBLIOGRAFIA

1. *https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf*
2. *http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf*
3. *http://www.fisicamedica.it/aifm/documenti/report/2013/report-n10*