Cyber(in)sicurezza in sanità: un ponte comunicativo tra medicina, informatica e diritto

Maria Vittoria Zucca*

CYBER(IN)SECURITY IN HEALTHCARE: BRIDGING MEDICINE, IT, AND LAW

ABSTRACT: The advent of digitalization has significantly shaped the healthcare sector, introducing advanced technological solutions while simultaneously exposing health infrastructures to ever-evolving cyber threats. This paper aims to bridge the gap between key disciplines – medical science, IT, and law – realities that are often ideologically distant but must now collaborate to address the growing digital risks in healthcare. To this end, interviews have been conducted with two professionals embedded in the healthcare system – a telesurgeon and a computer engineer – whose insights will be presented. Through their perspectives, this paper seeks to "diagnose" the current and future challenges related to cybersecurity in healthcare.

KEYWORDS: Healthcare; digitalization; cybersecurity; cybercrime; telemedicine

ABSTRACT: L'avvento della digitalizzazione ha plasmato in modo significativo il settore sanitario, introducendo soluzioni tecnologiche avanzate, ma al tempo stesso esponendo le infrastrutture ospedaliere a nuovi rischi cibernetici. Il presente contributo si propone di instaurare un ponte di dialogo tra diverse discipline – medicina, informatica e diritto – troppo spesso ideologicamente distanti, ma che oggi più che mai devono collaborare per affrontare le emergenti minacce digitali in sanità. A tale fine, verranno presentate le interviste condotte con due professionisti inseriti nell'organigramma sanitario: un telechirurgo ed un ingegnere informatico. Attraverso le loro testimonianze dirette, si cercherà di ricostruire e "diagnosticare" le attuali e future sfide legate alla cybersecurity nel settore sanitario.

PAROLE CHIAVE: Sanità; digitalizzazione; cybersicurezza; criminalità informatica; telemedicina

SOMMARIO: 1. Introduzione: sanità sotto attacco – 2. Metodologia: le voci di esperti clinici e tecnici – 2.1. Intervista: nell'ottica di un telechirurgo – 2.2. Intervista: nell'ottica di un ingegnere informatico – 3. Conclusioni, non conclusive.

* *Dottoranda in Cybersecurity, Scuola Superiore Sant'Anna di Pisa e Scuola IMT Alti Studi di Lucca. Mail: maria.zucca@santannapisa.it.* *Contributo sottoposto a doppio referaggio anonimo.*

ISSN 2284-4503

Call

1. Introduzione

Non esiste settore della vita quotidiana che non sia stato profondamente plasmato dalle nuove tecnologie, e l'ambito sanitario non si è mostrato di certo "immune" a tale digitalizzazione. Si è assistito infatti ad un progressivo mutamento del paradigma della medicina tradizionale: da una sanità basata su di un sistema comunicativo burocratico-cartaceo novecentesco, dove le informazioni viaggiavano alla velocità di gambe e mani di assistenti ed impiegati, ad una sanità digitale, contraddistinta da rapidità, automazione, de-materializzazione ed interconnessione[1]. L'elenco delle innovazioni sarebbe assai ampio: dossier e fascicoli sanitari elettronici, dispositivi impiantabili ed indossabili, l'uso di sistemi di intelligenza artificiale (IA), terapie digitali, servizi di telemedicina, nanotecnologia e robotica chirurgica, stampanti tridimensionali, tutto si trova ad essere inglobato nel capiente "termine ombrello" della *e-Health*[2] (o anche, sanità digitale).

Così ad oggi la piattaforma *Image-guided therapy*, lanciata da *Philips*, offre ai medici una guida visiva di alta precisione durante gli interventi chirurgici, ottimizzando l'accuratezza e riducendo gli errori clinici[3]; oppure il progetto di IA *Watson* della IBM è stato sviluppato per processare in contemporanea una vasta mole di immagini (quali radiografie, risonanze, *etc*.) ed informazioni mediche al fine di identificare velocemente percorsi diagnostico-terapeutici specifici[4]; e ancora il servizio *Doctorplus*[5], rivolto ai pazienti cronici, consente di inviare le misurazioni effettuate autonomamente tramite *bluetooth* ad una centralina, che le trasferirà ad una piattaforma *cloud* accessibile a medici, specialisti e alla centrale infermieristica.

Sebbene i benefici sottesi a tale rivoluzione digitale siano d'immediata percezione in termini di maggiore celerità, organizzazione ed efficienza delle cure, parimenti evidenti risultano essere i rischi, le vulnerabilità e le potenziali minacce. Prendendo in prestito il lessico medico, si può infatti delineare il "quadro sintomatologico" della sanità odierna come segue: le infrastrutture ospedaliere nazionali si figurano soggetti estremamente vulnerabili, considerando sia l'ingente mole di dati ultrasensibili[6] in

[1] Per tutto il decorso storico la scienza medica è progredita parallelamente da una parte alle esigenze collettive – la pratica chirurgica a supporto delle campagne di guerra, gli studi sull'origine delle malattie epidemiche a seguito dell'arrivo in Europa della c.d. peste nera – e d'altra parte in parallelo all'evoluzione tecnologica - la diffusione del microscopio, le prime tecniche radiologiche, l'implementazione degli esami fisico-chimici e biologici fino ad arrivare alle moderne sperimentazioni di laboratorio. Approdando così al fenomeno che si erge a nucleo duro del presente scritto: l'avvento della rivoluzione digitale. Si citano, *ex multis*, J. SOURNIA, *Storia della Medicina*, Bari, 1994; M. MORUZZI, *La nuova cultura della sanità dematerializzata*, in *Recenti Progressi in Medicina*, 105, 11, 2014, 407- 409.

[2] Sul punto G. EYSEBENCH, *What is e-Health*, in *Journal of Medical Internet Research*, 3, 2, 2001, 20.

[3] Per informazioni sulla piattaforma https://www.philips.it/healthcare/e/image-guided-therapy

[4] Per informazioni sul progetto https://www.ibm.com/industries/healthcare

[5] Per informazioni sul servizio https://www.vree.it/doctor-plus-servizi-telemonitoraggio-televisita/

[6] Alquanto nota è la formula che consente di qualificare i dati sanitari come "nocciolo (o nucleo) duro" della privacy, locuzione utilizzata da chi rileva come essi si collochino "nel cerchio concentrico più interno" o, se si vuole, all'estremo più elevato della "scala delle durezze" della protezione dei dati personali, risultando invero capaci di far intravedere, quando non di svelare del tutto, la sfera più riservata della persona. L'immagine della scala delle durezze, diffusamente ripresa nella dottrina, si deve a Stefano Rodotà. Cfr. S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica del diritto privato*, 1997, 583-609.

circolo, difficilmente controllabili, sia l'utilizzo di sistemi e dispositivi non sempre progettati seguendo elevati standard di sicurezza-*by-design*.[7]

In particolar modo, si sta assistendo all'emergere di innovative cyber-minacce, che privilegiano lo strumento cibernetico al fine di acquisire (e capitalizzare) dati sensibili[8] o per compromettere l'erogazione di servizi essenziali, infliggendo così il maggior danno possibile a un settore cruciale come quello sanitario, al fine di ingenerare pressione, disordini e massimizzare i profitti[9].

Pertanto, la nuova "patologia" che il settore sanitario si trova a dover affrontare non è altro che una forma sempre più sofisticata e strutturata di criminalità informatica, capace di adattarsi di pari passo con l'evoluzione tecnologica e alle contromisure di sicurezza. A confermare la gravità del fenomeno sono le statistiche ufficiali: la sanità si conferma uno dei principali bersagli di cyber-attacchi, nel tempo sempre più frequenti, distruttivi e pervasivi, mettendo a serio rischio la sicurezza dei pazienti e l'efficienza di intere infrastrutture[10].

2. Metodologia: le voci di esperti clinici e tecnici

La metodologia seguita nella scrittura del presente articolo si è basata sulla raccolta di interviste semi-strutturate, condotte da remoto e della durata di un'ora ciascuna. Le domande, predefinite e condivise in anticipo con gli interlocutori, sono state integrate con ulteriori approfondimenti in base alle risposte fornite, mantenendo così un approccio flessibile di discussione.

La prima intervista riporta la prospettiva di un clinico, quale operatore sanitario che *day by day* si ritrova ad agire in un campo (si potrebbe dire "minato") e a dover tenere il passo rispetto ad una cyber-evoluzione che pone nuovi quesiti ad una professione che oggi più che mai appare fortemente in sovraccarico. La seconda intervista, invece, offre "l'altro lato della medaglia", ovvero il punto di vista di un ingegnere informatico che opera stabilmente all'interno della stessa azienda sanitaria del clinico. Il suo contributo mira a fornire una panoramica sui ruoli e sulle prospettive in gioco, con l'obiettivo di

[7] Sicurezza-*by-design* indica un principio di progettazione che integra la *security* come elemento prioritario fin dall'inizio del "ciclo di vita" del prodotto, garantendo così una protezione più efficace contro le minacce informatiche durante le fasi dello sviluppo di sistemi, software e infrastrutture. Cfr. A. ANTONILLI, *Sicurezza informatica e trattamento dei dati in ambito sanitario*, in *Salute e società*, XVI, 2017, 97-98.

[8] Il fatto che i dati sanitari siano diventati un preciso obiettivo criminale implica l'esistenza di una domanda sul mercato (sommerso) e, di conseguenza, un ritorno economico sugli investimenti. Si riassumono i fini a cui si può indirizzare il furto dei dati sanitari: la costruzione di false identità (su *AlphaBay* il costo di un "pacchetto" completo per ricostruire il *background* di un medico professionista – comprensivo di dati identificativi, diplomi di laurea, licenze mediche e documenti assicurativi – si aggira sui 500 $), la richiesta di denaro come riscatto al fine di rientrare in possesso dei propri dati, frodi assicurative, contraffazione di documenti, emissione di false prescrizioni medicali, e l'ottenimento di farmaci specifici. Cfr. CARBON BLACK, *Healthcare Cyber Heists in 2019: 20 leading CISOs from the healthcare industry offer their perspective on evolving cyberattacks, ransomware & the biggest concerns to their organizations*, 2019.

[9] Laddove un attacco *ransomware* venga sferrato su di una infrastruttura ospedaliera, si verificherebbero: l'impossibilità di accedere alle cartelle cliniche dei pazienti, come anche severi ritardi nel prestare cure e trattamenti da parte degli operatori sanitari (obbligati a ritornare ad una modalità di lavoro "cartacea"), e ancora, più lunghe degenze dei pazienti e/o loro trasferimenti in strutture limitrofe.

[10] Per una più recente panoramica sui cyber-attacchi in sanità, si rimanda al Rapporto *Clusit Healthcare 2024*, al sito https://clusit.it/blog/rapporto-clusit-healthcare-2024/ quale addendum del rapporto CLUSIT 2024.

instaurare un dialogo tra discipline (solo) apparentemente distanti – giuridica, medica e informatica – ma ad oggi inevitabilmente interconnesse.
Le interviste sono corredate da note a piè di pagina al fine di approfondire e chiarire termini e concetti emersi durante la discussione. Entrambe sono state riportate in forma anonima, su richiesta degli intervistati.

2.1. Intervista: nell'ottica di un telechirurgo

Sin da subito le complessità si sono poste in evidenza con estrema lucidità, ovvio è che in ambito medicale si debba operare un netto discrimine fra chi si occupa del settore puramente clinico e chi si occupa di igiene informatica, organizzazione e management, tuttavia*:*

> «È proprio da tale basilare distinzione che si nota il sorgere di una prima problematica: l'informazione ultrasensibile sanitaria, il dato digitale, l'utilizzo del macchinario o strumentazione medica è ad appannaggio esclusivo del clinico, e non dell'igienista, la qual cosa comporta necessariamente una esposizione a molteplici rischi, legata per di più ad una totale incoscienza ed inconsapevolezza rispetto a ciò che il clinico abitualmente mette in moto e pone in essere. Lo scenario, quindi, è semplice ed è il seguente: nessun clinico è realmente consapevole circa quanto egli stesso si espone e quanto a sua volta fa esporre un dato sensibile od un paziente».

Ebbene si prosegua domandando se possa capitare che gli stessi medici, nello svolgimento delle proprie abituali funzioni, si servano di mezzi e strumenti non specificatamente progettati per l'ambito sanitario[11] (come l'uso improprio di una applicazione di messaggistica), bypassando così quel livello di sicurezza che dovrebbe viceversa esser pienamente garantito, la risposta in tal caso risulta immediata:

> «Abitualmente, o meglio quotidianamente, ricevo e-mail, contenenti dati relativi ai pazienti, da parte di altri clinici, che necessitano di ottenere un secondo parere. Questo, per quanto banale, risulta un chiaro indice di quella mancanza di consapevolezza di cui poc'anzi». Così si prosegue: «È comunque una strada che continua ad essere seguita, per esigenze che sono tanto comodità quanto di celerità, ossia per ricevere e fornire risposte rapide ed esaustive in tutti quei casi che siano necessitanti di un celere consulto medico».

Rimane purtuttavia vero il fatto che esistano tutta una serie di sistemi atti ad agevolare la complessità della realtà sanitaria: dalla cartella elettronica a livello regionale, fino all'odierna implementazione del S.I.O (Sistema informativo Ospedaliero) che intende perseguire il progetto di affinare la trasmissione da ospedale ad ospedale, creando una interconnessione più agile all'interno, ma non solo, della stessa regione, fornendo così un concreto supporto, moderno ed efficace, alle quotidiane attività di sia tipo sanitario che amministrativo.
Seguono le parole di commento:

[11] Un report del 2021 commissionato da *Kaspersky* ad *Arlington Research*, condotto a livello globale e composto da 389 interviste fra coloro che operano nel campo della telemedicina ha riportato tali risultati: il 54% dei fornitori di servizi di telemedicina concordano sul fatto che alcuni dei propri medici conducano abitualmente sessioni di medicina a distanza utilizzando applicazioni non specificamente progettate a tal fine, quali: *FaceTime, Facebook Messenger, WhatsApp e Zoom*, ed il 52% degli operatori sanitari ha poi sperimentato casi di pazienti che si sono rifiutati di tenere videochiamate proprio per la diffidenza verso le tecnologie ed il timore in ambito di sicurezza e protezione dei propri dati. Cfr. KASPERSKY, *Telehealth take-up: the risks and opportunities*, 2021.

> «Eppure tutto ciò, fino a questo momento, rimane qualcosa di assolutamente non realizzato e non utilizzato. Si immagini il restare nella impossibilità di poter visualizzare le immagini di un paziente che ha fatto una tac, ad esempio a Vicenza, fintanto che non sia il paziente stesso od i familiari a portare fisicamente il dischetto, o qualsivoglia supporto rigido, su cui poi poter basare le proprie valutazioni mediche. È ovvio quindi che tutti i restanti sistemi di interconnessione siano da sempre risultati largamente più agili ed efficaci, da qui il loro abitudinario utilizzo».

Preciso istante in cui il colloquio *de quo* subisce una interruzione, la quale altro non farà che avvalorare, nella maniera più pratica possibile, quanto detto sin qui, così invero si riprende:

> «Ecco una dimostrazione, mi è appena arrivato un messaggio via Whatsapp da parte di un collega, riportante – il paziente X sta sanguinando lo portiamo o meno in sala? – Certo è indicato solo il cognome, senza nome e senza data di nascita, con la patologia di riferimento, è ovvio comunque che il paziente sia facilmente identificabile».

Così si continua, in un'ottica di commento:

> «Questa è la realtà dei fatti e non è superabile: in una comunicazione all'interno di un medesimo ospedale è stato un collega di un'altra specialità ad informarmi circa la situazione di un paziente ed a pormi di conseguenza domande urgenti su come affrontare la specifica situazione. Sistemi di supporto con fini agevolatori ci saranno in futuro, ma non potranno in alcun modo sostituire una comunicazione come quella che ad oggi avviene abitualmente».

Ciò che si può ricavare quindi è quasi un muoversi in automatismo, dovuto ad una routinaria abitudine, come anche alla necessità di dover gestire il proprio operato quotidiano, nonostante la mancanza di una piena presa di coscienza e consapevolezza circa il valore sotteso al proprio agire, da qui:

> «Sono pienamente convinto del fatto che il collega che mi ha appena inviato tale messaggio non ritenga in alcun modo di aver commesso un errore, nonostante abbia fornito un dato clinico ultrasensibile, riferito ad un paziente identificabile, attraverso uno strumento che non è sicuramente congruo per la tipologia di informazione che viene trasferita».

Ci si interroga pertanto su quanto possa effettivamente essere estesa la mancanza di cyber-cultura in ambito ospedaliero, i fatti di cronaca sembrano parlare chiaro: una larga parte delle intrusioni, violazioni, data breach[12] ed altresì attacchi *ransomware*[13] sono dovuti, o perlomeno facilitati, all'assenza di nozioni e pratiche base di sicurezza informatica, si pensi all'utilizzo di *password* di *default* o al servirsi di sistemi informatici non correttamente aggiornati.
Di seguito la precisazione fornita:

[12] Con la nozione di *data breach* si intende ex art. 4 n. 12 GDPR (UE/2016/679): «*una violazione di sicurezza che comporta […] la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*». Si parla in tali casi di una "falla" (o appunto, breccia) nel sistema, in cui un attore malevolo può insinuarsi ed avere accesso ai dati ivi conservati, violandone riservatezza, integrità e disponibilità.

[13] Il termine *ransomware* deriva dalla crasi delle parole "*malware*" (programma malevolo) e "*ransom*" (riscatto), e sta ad indicare un *malicious software* che, a seconda della sua tipologia, infiltrandosi in un singolo computer (o in una rete) può cifrare, occultare o negare l'accesso a dati o informazioni, come limitare od impedire l'accesso ad un sistema informatico, rendendo inutilizzabili documenti, archivi ed ogni altro contenuto memorizzato, col fine di costringere la persona offesa a versare un importo in denaro per il riscatto del sistema e per il ripristino dei dati.

Call

> «Certo tutte queste tipologie di problemi non competono ad un sanitario, tutt'al più alla Direzione, ossia il centro informatico che ogni ospedale ed ogni ASL presenta, d'altronde io non mi sono mai neanche chiesto se il computer dell'Azienda, che ho qui sulla mia scrivania, sia sufficientemente protetto. Ad esempio, è il sistema stesso a chiedermi il cambio delle password dopo il passare di un tot di tempo, sebbene poi alla fin fine le mie password siano sempre le medesime tre che girano e ricircolano al trascorrere ogni tre mesi. Quindi sì, è possibile che ci sia una superficialità sottesa, come anche una non percezione del rischio reale, ma dirò di più forse anche un po' di arroganza da parte della categoria sanitaria, nel pensare di doversi curare solamente della salute del paziente e poco importa dell'eventualità che i suoi stessi dati possano effettivamente circolare».

Si intervenga allora sostenendo che sebbene sia intuibile la superficialità che si può dimostrare nei confronti di una violazione della privacy, non si può ignorare la necessità di chiedersi se la sensibilità al rischio cambi laddove ad essere in pericolo sia la stessa salute di un paziente, si pensi ai casi di utilizzo di tele-robot chirurgici[14]:

> «In tal caso da clinico ho un interesse al corretto funzionamento dello strumento, al fatto che vi sia una corretta riproduzione del mio input, che il mio feedback visivo sia efficace e affidabile (ossia con latenze che siano le più basse e ravvicinate possibili), e che dalla interazione robot-paziente non derivi alcun danno biologico. Nonostante questo, ciò che vi è fra la console ed il paziente stesso non è un problema di mia competenza, se tra qualche anno, infatti, verrà attuata una implementazione della telechirurgia[15] la tematica delle intromissioni malevoli sarà sì un problema dei sanitari, ma non verrà percepito come tale».

Rimanendo ancora all'interno del "termine ombrello" dell'e-Health si consideri la delicatezza che può attorniare i sistemi di telemonitoraggio[16]:

> «Più attuale e differente risulta tale ambito, siamo dinnanzi ad informazioni che verranno analizzate e utilizzate dal clinico per assumere determinate decisioni, ovvio appare in tal caso l'assunto: se l'informazione fornita è scorretta, il clinico prenderà d'immediata conseguenza decisioni scorrette».

Per esser più chiari si pensi ai casi di telemonitoraggio domiciliare, reso possibile grazie all'utilizzo di dispositivi *wearable* atti a misurare dati quali i parametri vitali di base, col fine di fornire *feedback* lungo

[14] Per telechirurgia si intende una tecnica operatoria che consente al medico di eseguire un intervento chirurgico a distanza, ossia su di un paziente che non si trova fisicamente nello stesso luogo. L'operatore umano si servirà di una apposita *console*, fornita di un *monitor* atto a consentire l'osservazione continua della regione operatoria, andando ad eseguire le manovre necessarie dell'intervento che, teletrasmesse, verranno con estrema precisione ripetute sul paziente da un *robot* chirurgico.

[15] Nel 2015, un gruppo di ricerca dell'Università di Washington ha condotto una sperimentazione sul robot per telechirurgia *Raven II*, analizzandone le vulnerabilità informatiche. Il sistema, composto da due bracci chirurgici controllati a distanza, è stato progettato per operare in condizioni critiche – si pensi a zone di guerra - con connessioni condivise e di bassa qualità, aumentando i rischi per la sicurezza. I ricercatori sono riusciti in via sperimentale ad interferire con i comandi del *robot*, dimostrando la possibilità di manipolare operazioni chirurgiche, ritardare o cancellare istruzioni e persino prendere il controllo totale del dispositivo. Cfr. T. Bonaci, *To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robotics* , in *ArXiv preprint arXiv:1504.04339,* 2015.

[16] Il telemonitoraggio permette di monitorare a distanza i parametri vitali e le condizioni di salute di un paziente attraverso dispositivi connessi. Viene utilizzato per il controllo di pazienti con malattie croniche, post-operatori o soggetti fragili, migliorando l'assistenza e riducendo così la necessità di visite in presenza.

l'arco della giornata relativi ai pazienti, per appurare ad esempio come stia procedendo un post-operatorio. Così si è voluto puntualizzare:

> «Indubbiamente tali dati hanno rilievo, ma importanza ancora maggiore in termini di sicurezza viene rivestita da altre tipologie di informazioni e dispostivi, si pensi ai pacemakers[17] o ai defibrillatori impiantabili[18], anche in questo caso tuttavia la sicurezza verrà data da parte del sanitario per scontata, ossia si confiderà nel fatto che la casa produttrice del dispositivo abbia messo in campo tutta una serie di strategie[19] per far sì che non vi siano intrusioni malevoli od altri incidenti».

Proseguendo nel colloquio, una volta elencate tutte le *capabilities* che paiono esser necessarie al fine di rendere una struttura sanitaria affidabile, efficiente e cyber-resiliente (dalle risorse tecnologiche e strumentazioni mediche adeguate, alle sessioni di *training* e formazione del personale, alla metodologia di gestione del rischio, fino alla compliance normativa nelle nomine di figure quali il DPO, il CISO, od anche il *risk manager*), ci si è domandati se suddetti requisiti vengano concretamente soddisfatti. A seguire le parole di commento:

> «Nelle aziende sanitarie quanto elencato risulta essere presente, sebbene con diversi gradi e complessità, si guardi per esemplificare alla formazione: i corsi che noi sanitari abbiamo come obbligatori da seguire online sono per lo più incentrati proprio sul risk management, od in generale sulle tematiche relative sicurezza, il problema ancora una volta risulta perciò essere alla base. O meglio, è una questione di percezione, capita infatti che per il clinico puro tali tipologie di corsi siano avvertiti quasi come perdite di tempo, ossia quali gravose lungaggini ed inevitabili coercizioni, sebbene possa capitare che le nozioni acquisite risultino anche concretamente utili in occasioni future. Di conseguenza ritengo che sia la trasmissione dell'informazione a dover essere veicolata in una maniera, benché non saprei come, più stimolante per il clinico, cosicché non sia percepita quale rigida imposizione».

[17] Si ricordi il caso del 2018, in cui *Medtronic* emise un avviso riguardante i controller *MiniMed MMT-500 e MMT-503*, utilizzati per controllare i microinfusori di insulina. A causa di vulnerabilità nei segnali *wireless* non criptati, un attaccante avrebbe potuto manipolare l'erogazione dell'insulina, causando rischi di crisi ipoglicemiche o iperglicemiche nei pazienti diabetici. Nonostante ciò, inizialmente l'azienda non richiese la sostituzione dei dispositivi, ma successivamente procedette al ritiro dei telecomandi, riconoscendo la falla nella progettazione e messa in sicurezza dei dispositivi. Si guardi Medtronic, *Urgent Medical Device Recall: MiniMed remote controller (MMT-500 or MMT-503)*, Ottobre 2021, reperibile al sito internet https://www.medtronicdiabetes.com/res/img/pdfs/MiniMed-Remote-Controller-FCA-Patient-Letter.pdf

[18] Si ricordi il caso del 2017, quando la FDA emise un richiamo riguardante circa 500.000 *pacemakers* della *St. Jude Medical*, a causa di vulnerabilità che avrebbero permesso la manipolazione degli input cardiaci. A differenza del caso *Medtronic* di cui alla nota sopra, il richiamo non prevedeva la rimozione dei dispositivi, ma un aggiornamento del firmware, che i medici potevano applicare per correggere le falle di sicurezza. Cfr. B.M. KUEHN, *Pacemaker recall highlights security concerns for implantable devices*, in *Circulation-Cardiology News*, 138/2018, 1597-1598.

[19] Si intendono gli obblighi in capo ai produttori dei dispositivi medicali, sia pre-mercato (identificando requisiti minimi di sicurezza-*by-design*, da adottare in fase di sviluppo, progettazione e fabbricazione dei devices), sia post-vendita, in quest'ultimo caso, al verificarsi di un incidente informatico, si evidenzi come i produttori siano tenuti a svolgere una apposita indagine, nonché ad effettuare una notifica alle autorità competenti in modo da informarle circa la natura del *cybersecurity breach* e dei possibili effetti negativi registrabili sulla salute degli interessati.

D'altronde si ritorna di nuovo a rimarcare quell'ottica individualista, solista ed un poco boriosa che sembra alle volte appartenere alla categoria sanitaria: «in effetti il ragionamento dietro spesso è questo: il mio mestiere è altra cosa, ed è di una nobiltà tale per cui di tutti questi elementi non me ne devo né curare né preoccupare».
Paiono ad ogni modo parimenti giuste, ragionevoli e ben spese anche le osservazioni poste a difesa:

> «noi sanitari siamo soverchiati da problematiche di ordine generale, clinico ed amministrativo, dobbiamo studiare le leggi per la somministrazione dei farmaci, per i piani di cura, ed ancora dobbiamo spendere dai dieci ai quindici minuti di tempo solo per inserire in maniera digitale la somministrazione del farmaco, per poi controllarla e vigilarla. Quindi si immagini la volontà, e voglia, di dedicarsi anche agli aspetti più propriamente inerenti alla sicurezza dei dati, alle possibili intromissioni ed alla cybersecurity in generale».

Ed è in questo momento che traspare maggiormente il forte sovraccarico che un clinico può sentire pesare gravosamente su di sé:

> «chi si occupa di igiene e prevenzione vuole che io sia formato ed informato sulla sicurezza nel luogo del lavoro, chi invece si occupa di gas biomedicali vuole a sua volta che io sia informato sull'uso delle apparecchiature, chi si occupa di ingegneria, ed io devo utilizzare un elettrobisturi, mi chiede di esser informato sulla sua impostazione e su cosa si debba intendere per un malfunzionamento, dando ovviamente per scontato che, a ben vedere, io dovrò essere assolutamente e perfettamente informato circa la patologia che sto trattando, il paziente che ho dinnanzi ed il suo specifico trattamento».

Viene pertanto da pensare che vi sia la forte esigenza di formare nuove figure professionali con competenze altamente specifiche e multidisciplinari che debbano essere inserite nell'organico sanitario al fine di affiancare gli operatori e garantire per loro, attenuando in tal modo tutta una serie di incombenze d'organizzazione, amministrative, nonché di sicurezza di cui si trovano ad essere addossati: «non sto chiedendo che qualcuno mandi e-mail al posto mio, ma che io possa avere ad esempio un sistema di messaggistica imposto dall'Ordine dei Medici che risulti assolutamente blindato».
Questo non significa deresponsabilizzare l'intera categoria, ma trovare un corretto equilibrio fra le diverse figure che possa risultare ottimale, da qui:

> «Noi dobbiamo ovviamente avere chiari i problemi relativi alla cybersecurity, ma dobbiamo parimenti aver chiaro che ci sia qualcuno che quel problema lo può risolvere e lo ha risolto. L'equilibrio sta tutto qui: il problema sì lo dobbiamo conoscere, ma non ce ne dobbiamo concretamente occupare dal momento che non abbiamo tempo, voglia, testa e tantomeno formazione in materia».

Sono parole queste ultime dotate di estrema lucidità, tramite le quali un clinico riconosce la giustezza dell'informarsi, e curarsi circa le tematiche emergenti, che siano anche le più lontane possibili dal suo quotidiano operare, ma ugualmente ne riconosce i limiti: «figure terze devono ad oggi poterci mettere nella condizione migliore affinché i problemi di cybersicurezza siano solo più questioni da dover conoscere e non più di cui doverci concretamente occupare».

2.2. Intervista: nell'ottica di un ingegnere informatico

Pur riconoscendo che diversi gradi di complessità ed eterogeneità possono contraddistinguere l'assetto di ogni struttura ospedaliera, si chieda innanzitutto di tratteggiare l'organigramma di ruoli e figure professionali che orbitano attorno all'ambito della sicurezza, qui la risposta:

«Per tutte le questioni inerenti alla gestione della privacy si guarda al ruolo dei DPO, ma ciò che più mi compete, e di conseguenza maggiormente conosco, è proprio la disciplina settoriale della security informatica. Quest'ultima, badi bene, è purtroppo una branca molto giovane nelle strutture ospedaliere come quella in cui opero, dal momento che l'attenzione e sensibilità verso tale ambito si è raggiunta solamente di recente, proprio in seguito all'inasprirsi degli attacchi informatici ed all'interesse mediatico che ne è conseguito, da tale enfasi ne sono poi scaturiti diversi investimenti in tal senso».

Si domandi pertanto quale sia il panorama normativo di riferimento in tema di sicurezza informatica:

«Attualmente il quadro normativo a cui ci riferiamo e andiamo ad attuare è fondamentalmente il panorama NIS[20], è il nostro punto focale e filone principale, nonché leva per chiedere finanziamenti ed investimenti che, capirà, in aziende come la nostra, con 50.000 prese di rete e 7.000 dipendenti, sono piuttosto elevati e per nulla banali, e comunque in passato spesso sono venuti a mancare. Negli ultimi anni invece sono stati stanziati investimenti importanti e questo lascia ben sperare in una direzione di possibile progredimento».

Addentrandosi più specificatamente nel tema delle cyber minacce, si chieda un commento circa i fattori di vulnerabilità riguardanti una struttura critica come quella ospedaliera, fra cui l'essere dotati di un sistema informatico complesso, l'utilizzo di dispostivi IoMT non sempre progettati seguendo elevati standard di sicurezza, l'articolata catena della *supply chain*[21], nonché il fattore umano[22] cui si faccia affidamento, la risposta:

«Dunque per tutto ciò che riguarda le tematiche propriamente legate all'IT, quale nostro perimetro storico, attualmente stiamo portando avanti progetti che paiono essere promettenti, per tutto ciò che attiene invece agli altri ambiti ci atteniamo a quanto ci viene fornito. Mi spiego meglio: i device elettromedicali per loro natura sono certificati CE tout court (cioè per le componenti hardware, software, di configurazione etc.), quindi se noi volessimo installarci un antivirus non è detto che questo sia possibile, dal momento che si va ad inficiare la certificazione stessa. Per riuscire a sopperire a tale problema si è dovuta elaborare una struttura di securizzazione laterale, in cui i dispositivi medici raffigurano il nucleo, da proteggere tramite "cinta murarie" di sicurezza, affinché il perimetro sia il meno vulnerabile possibile. Come vede dunque la tecnologia ci viene in soccorso, però è proprio qui che scatta il terzo fattore, ossia quello umano, chiaro è che se vedi una postazione di lavoro con una presa USB libera e scarichi i compiti di tuo figlio nel sistema, puoi anche inficiare e far crollare tutto il lavoro che è stato fatto. Vorrei che lei notasse come la parte umana rimanga ad oggi questione davvero rilevante della problematica, veda il dilagante fenomeno del phishing».

[20] Si ricordi l'evoluzione normativa della Direttiva NIS (2016/1148/UE), introdotta nel 2016 per stabilire misure di sicurezza per le reti e i sistemi informativi nell'Unione Europea, mirando a migliorare la resilienza delle infrastrutture critiche. Nel 2020, la Commissione Europea ha proposto una revisione della direttiva, che ha portato all'adozione della Direttiva NIS 2 (2022/2555/UE), entrata in vigore nel 2023. La NIS 2 ha ampliato il campo di applicazione e ha introdotto requisiti più rigorosi e sanzioni più severe per garantire una protezione maggiormente robusta contro le minacce informatiche.

[21] La *supply chain* in sanità riguarda la rete di fornitori, produttori e distributori coinvolti nella gestione di dispositivi medici e farmaci. La sicurezza informatica all'interno di questa catena è cruciale per proteggere i dati sensibili e garantire l'integrità dei dispositivi.

[22] Per fattore umano si intende l'insieme di comportamenti, decisioni ed errori degli individui (operatori sanitari, in questo contesto) che possono influenzare l'intera sicurezza di un sistema informatico.

Appare lampante la sovrapponibilità di tali dichiarazioni con quanto dichiarato in precedenza disquisendo con il clinico, si ricordi come si fosse già confermato l'utilizzo abituale di applicazioni di messaggistica non congrue al trattamento di dati ultrasensibili come possono essere quelli sanitari, si chieda conferma:

> «È assolutamente così, c'è una totale sconsideratezza nell'inviare referti ed analisi tramite WeTransfer o simili, e ciò è tutt'altro che infrequente, anzi è una pratica comune. Per questo stiamo sempre più insistendo nell'ottica di una maggiore sensibilizzazione ed acculturamento, ad esempio tramite campagne di falso phishing, inviando cioè una serie di e-mail e laddove l'operatore sanitario apra il link, contenente tanto per capirci – bravo hai vinto un milione di euro – riveliamo di esserci noi informatici dalla parte opposta, avvertendo gli operatori stessi che un'azione del genere avrebbe portato a tutta una serie di determinate conseguenze dannose. Il fattore umano è dunque altamente impattante in una struttura come la nostra e peraltro vorrei far notare come ci siano molte persone estremamente refrattarie al cambiamento delle proprie, scorrette, abitudini operative».

Si ricordi come nell'ottica del clinico i corsi di formazione sui temi della sicurezza siano spesso percepiti come lungaggini, da dover seguire solo perché obbligati, segue la veloce interruzione:

> «Sì, mi lasci dire che la percezione è che la security sia proprio una gran rottura di scatole, intendendola cioè quasi come una limitazione alla libertà personale, vuoi perché non puoi navigare in Internet a tuo piacimento, ma nei siti indicati, vuoi perché non puoi trasferire su WeTransfer un'immagine clinica per avere un secondo parere medico».

Chiaro è però come vi sia una costante tensione ed un difficile equilibrio da delineare fra la cura propriamente clinica, anche emergenziale, del paziente e la cura degli aspetti maggiormente di *privacy* e *security*:

> «Esatto, questo è proprio uno dei temi su cui spesso ci scontriamo, in quanto limita il nostro operare: poniamo il caso di un chirurgo che necessita, per il bene del paziente, di fare vedere l'immagine di un tumore ad un collega negli Stati Uniti per avere una seconda opinione, ovvio è che la questione sia altamente delicata. Se lei mi chiede se esistano regole specifiche e normative atte a fare in modo che un tale trasferimento avvenga in maniera sicura, le rispondo di sì, ma tale tipologia di flussi, come può immaginare, non è certamente gratuito, anzi presenta un costo non indifferente».

Tornando al tema della cyber-formazione, si rammenti come nell'ottica del clinico puro si dovessero trovare soluzioni innovative e più stimolanti al fine di incentivare l'apprendimento di nozioni di igiene informatica, si proponga ivi una possibile organizzazione di incontri in presenza, laddove il metodo *online* possa apparire alle volte maggiormente gravoso, così la risposta:

> «Io mi occupo della formazione dai tempi precedenti al Covid, di conseguenza non via web, ma in aula, e le persone che avevo dinnanzi si dividevano in due, anzi almeno tre gruppi: gli annoiati, ossia coloro a cui la tematica non importava affatto, che erano presenti solo perché ciò è dovuto, poi una minimissima parte effettivamente interessata all'argomento, e da ultimo una buona parte refrattaria al cambiamento, irremovibilmente radicati ed attaccati alle proprie abitudini, che non sono assolutamente intenzionati a modificare e correggere. Ora addirittura via web non ho nemmeno più questa percezione, basta spegnere la telecamera ed addormentarsi».

A seguire vengono pronunciate parole che richiamano alla memoria quanto già ammesso da parte del clinico:

> «Se devo essere sincero, poi sarà una mia percezione soggettiva, c'è proprio un sentimento di superiorità da parte della classe medica, nel pensare di essere in un ambiente prettamente clinico, in cui il core business è la cura del paziente e tutto quanto il resto dovrà essere assoggettato e seguire le esigenze proprie di tale categoria professionale. Non mi spingo oltre, ma comunque tenga presente che io tutti i giorni ho dei disguidi dovuti proprio ai motivi detti fino ad ora».

Appare irrazionale tale ritrosia al cambiamento, soprattutto davanti ad una cybercriminalità che è in continua crescita, sempre più sofisticata ed invasiva, che non si ferma più solo sul versante della violazione e furto dati, ma che prende di mira le stesse strutture o che s'introduce nelle apparecchiature e dispositivi, si commenta:

> «Per quanto riguarda le intrusioni cyber devo fare un premessa: la telechirurgia deve ancora fare notevoli passi avanti, ad esempio i tele-robot utilizzati nella nostra struttura sono utilizzati solo localmente, il paziente ed il robot si trovano cioè a due metri di distanza dall'operatore chirurgico, ed è una modalità operatoria utilizzata più che altro per annullare eventuali tremori fisiologici ed affaticamenti delle braccia del chirurgo, di conseguenza i problemi legati alle intrusioni malevoli saranno eventualmente preoccupazioni future, che seguiranno di pari passo l'evoluzione della telechirurgia stessa. Più rilevante invece, quale perimetro che ad oggi nessuno sta prendendo seriamente in considerazione, risulta essere quello dell'attuazione meccanica di dispositivi quali le UTA (unità trattamento aria)[23] ad esempio usate nelle sale operatorie. Dal mio punto di vista di ingegnere informatico, con una conoscenza di elettronica, io mi preoccuperei di tali sistemi, dato che sono comandati da un sistema informatico IP, banalmente se un attaccante riesce ad intromettersi può manipolarle a proprio piacimento, agire sugli interruttori, arrivando anche a fare saltare la corrente di tutto l'ospedale. Ecco che il passaggio da un attacco ransomware diretto a cifrare i dati e chiedere un riscatto, ad un attacco di mera guerriglia indirizzato a creare una magnitudo massima di dannosità, pare piuttosto breve. Chiaro che nel secondo caso una volta che il sistema è stato "bruciato" tutto, i pazienti attaccati ad un respiratore muoiono, o comunque soffrono un pesante disservizio. Quindi sì, fra le minacce temute da una azienda come la nostra, un posto è rivestito dal ransomware, ma non escluderei possibili attacchi alle UTA od alle cabine elettriche a fini puramente distruttivi. Qui si inserisce la normativa, che per quanto riguarda le UTA prevede che possano essere aperte o chiuse, ad esempio in funzione di un incendio, "anche" tramite via informatica, bene allora io mi aspetterò che venga studiata, attuata ed implementata "anche" una security informatica in tale direzione».

Procedendo nella discussione si cerchino di riassumere le *capabilities* da adottare affinché una infrastruttura critica sia in grado di mitigare il rischio cyber: risorse tecnologiche adeguate, compliance normativa, sessioni di *training* del personale, metodi di analisi e gestione del rischio, strategie di *business continuity* e *disaster recovery*, periodici test sulla sicurezza dei *device* e soluzioni di *identity management,* da qui il commento:

> «In effetti il quadro NIS prevede tutto questo, e ci stiamo attualmente adoperando affinché tali azioni vengano attuate, cercando di sopperire a ciò in cui siamo carenti, il vantaggio apportato dalle NIS è invero l'avere fatto chiarezza sulla strada da dover intraprendere. Non è che prima non ci fossero buone pratiche adottate, erano tuttavia procedure non scritte, diciamo "tramandate", che a seguire sono state poi delineate dalla normativa, che ha avuto peraltro anche il ruolo fondamentale di spostare i riflettori sull'importanza di tali tematiche».

[23] Con "Unità di Trattamento Aria" in ambito sanitario si intendono dispositivi progettati per garantire la qualità dell'aria negli ambienti chiusi, come sale operatorie, reparti di terapia intensiva o laboratori.

Si domandi quali siano le sfide attuali su cui doversi focalizzare al fine di implementare gli attuali livelli di sicurezza:

> «A parer mio il fattore umano, inteso dalla base al vertice, ossia dall'operatore utilizzatore della specifica tecnologia alla Direzione stessa, rimane devastante, e necessita ad oggi di un'alta sensibilizzazione sui requisiti di security da dover rispettare. Non è più il tempo di una formazione generale e dispersiva, ognuno dovrà essere istruito in misura settoriale sulle proprie competenze: chi compra device ed apparecchiature, o altresì chi fornisce la struttura, tutti possono a loro modo essere impattanti sulla sicurezza della struttura nel suo complesso.[24] A me personalmente come formula piace il concetto di cybersecurity-by-design, da attuare in tutti i campi, ciò significa che se devo comprare una qualsiasi strumentazione, dovrò richiedere fin dal principio agli stessi fornitori il rispetto di tutta una serie di requisiti di compliance ».

Parole conclusive sono poi state spese circa lo stato del proprio settore professionale:
«Vorrei comunque ancora sottolineare come i professionisti della security si stiano facendo solamente adesso, difatti persone della mia generazione orientate in maniera specifica e verticale su tali tematiche sono davvero poche. C'è l'attuale bisogno di formare una classe professionale che svolga il mio stesso lavoro, che abbia le spalle un po' più large, seguendo un'ottica diciamo sempre più "entreprise" ed in Italia sotto questo profilo non siamo tanto avanti».

3. Conclusioni, non conclusive

Traendo spunto delle interviste svolte e tentando di pronosticare l'evolversi della sanità si può, a ben vedere, immaginare uno scenario futuro sempre più diversificato: alcune prestazioni sanitarie permarranno erogate *on site*, ossia alla presenza del paziente (negli ospedali, nelle strutture diagnostiche *etc*.), altre muteranno in ibride, mantenendo un legame fra contesto fisico e virtuale (si pensi al telemonitoraggio), altre ancora diventeranno solo più virtuali (quali una televisita). Il perimetro, dunque, da mettere in sicurezza tenderà ad allargarsi sempre di più, passando da una sanità "ospedalocentrica", ad un coinvolgimento domiciliare del cittadino, con un conseguente numero maggiore di dati in circolo e sempre più soggetti coinvolti nel, già complesso, organigramma sanitario.
Lo sviluppo di una *digital health* nazionale dovrà quindi trovare piena realizzazione all'interno di un progetto di politiche pubbliche che sia organico e lungimirante e che dovrà porre l'attenzione su soluzioni quali: il rafforzamento dell'inter-disciplinarietà delle figure professionali nel settore sanitario (a partire dal ruolo del *risk manager*), l'incremento degli investimenti in *cybersecurity*, ed in tecnologie per la preparazione, la mitigazione ed il ripristino in caso di incidenti informatici, la responsabilizzazione dell'intera "catena di fornitura", affinché ogni figura sia adeguatamente informata, coinvolta e proattiva riguardo alla sicurezza informatica, riconoscendone l'urgenza e superando la marginalizzazione che troppo spesso ha dovuto rivestire in passato.

[24] Da qui l'attuale problema della *supply chain*, che non concerne quindi solamente i fornitori tecnologici (se si acquista *Office 3.6.5* ci si può aspettare, a ben vedere, un certo livello di sicurezza garantito), ma anche coloro che, nonostante siano slegati da aspetti puramente informatici, devono parimenti essere responsabilizzati (si pensi ad un'azienda che distribuisce ossigeno ai pazienti terminali, questa avrà tutta una catena logistica di furgoni, mezzi ed operatori in grado accedere agli archivi di una azienda sanitaria e modificarne i dati contenuti, ad esempio laddove cambi il *caregiver* di un paziente).

È così che si arriva nuovamente a ribadire il problema della formazione: a nulla servirà dotarsi di sofisticati sistemi di *identity management* se poi l'operatore finale sanitario finisce per attaccare con un *post-it* sul proprio pc la *password* per accedere al sistema. Una attuale sfida risulta allora far crescere una sempre maggiore cyber-cultura tramite corsi di aggiornamento e di formazione che appaiano stimolanti per gli operatori e che non vengano percepiti quali gravose lungaggini o perdite di tempo, da dover sostenere solo perché vi si è costretti.[25] Peraltro non è più il tempo di mirare ad una formazione generale (e quindi, dispersiva), sarebbe invero preferibile cucirla *ad hoc* su ogni soggetto (primario, infermiere, fornitore etc.) di modo che ricopra nello specifico i singoli tasselli operativi e gli obiettivi propri di ciascun individuo. Questo risulta ad oggi il punto focale: la cyber-formazione deve essere avvertita come obbligatoria, nonché percepita come indispensabile, ed in sanità tutto ciò risulta difficile perché le priorità avvertite sono altre (quali la cura e l'assistenza puramente clinica dei pazienti). Com'è evidente, sarebbe più facile dotarsi di set documentali, consulenti e di una svariata serie di procedure tecnico-organizzative per ottemperare alla compliance richiesta piuttosto che "calarsi in basso", andando a toccare e correggere automatismi e consuetudini di lavoro profondamente radicati che nessun operatore ha veramente l'intenzione di cambiare. Le proposte ed accorgimenti fin qui delineate possono rappresentare dunque la "terapia" necessaria affinché i vari attori multilivello – individuali (es: operatori sanitari), industriali (es: produttori di apparecchiature medicali) ed infrastrutturali (es: direzione sanitaria) – contribuiscano a trasformare le infrastrutture sanitarie, da entità appunto "critiche" ad enti ad alta affidabilità, come dovrebbero essere.

[25] Come fare concretamente: si ipotizzi la possibilità di programmare incontri diretti (invece che *online*) ravvicinati e collegiali, in presenza di tutti coloro che si ritrovano *day by day* ad operare sui dati, oppure si consideri la creazione di siti web e piattaforme FAQ (ossia, di *Frequently Asked Questions*) facilmente intuibili e dotati di rapide risposte, pare verosimile infatti ritenere che il personale sanitario voglia seguire procedure sicure, che spesso e volentieri però non sappia concretamente come fare