La cura delle informazioni digitali in telepediatria alla luce della normativa europea

Andrea E. Naimoli[1], Fabio Capello[2]
[1] Dipartimento di Ingegneria e Scienza dell'Informazione, Università di Trento
[2] UO Pediatria Territoriale, Dipartimento Cure Primarie, AUSL Bologna

La tecnologia ha profondamente modificato il modo di lavorare delle persone, consentendo di superare tanti ostacoli, ma anche presentando nuove sfide da affrontare. Nel campo della medicina le frontiere aperte dalle strumentazioni sempre più raffinate in ambito diagnostico hanno aperto la via a cure sempre più mirate e a una miglior qualità generale dei percorsi dei pazienti, dove resta comunque fondamentale il ruolo del medico a cui sono richieste nuove competenze e abilità per poter gestire e interpretare la mole di informazioni a disposizione. Anche quando le informazioni sono recuperate con metodi meno tecnologici, sono quasi sempre trattate con sistemi informatici per cui la profilazione del paziente è ormai sostanzialmente digitale.

Il paziente bambino

L'età pediatrica caratterizza un intervallo di tempo della vita di un individuo complesso e variegato che va dalla nascita sino e oltre l'adolescenza, contraddistinto non solo dall'accrescimento fisico e neuromotorio, ma dallo sviluppo di abilità e competenze di tipo emotivo, intellettuale, cognitivo, sociale e relazionale.
L'ambiente stesso all'interno del quale il bambino cresce è complesso ed è caratterizzato da numerosi contesti e attori capaci di influenzarne lo sviluppo e lo stato di salute. Famiglia, scuola, attività educative, ludiche o sportive rappresentano il mondo ordinario del bambino, al quale si affianca quello sanitario con la figura del pediatra, dello specialista e dell'operatore sanitario pediatrico [1].
Per il mantenimento e la promozione dello stato di salute del bambino queste realtà hanno necessità di comunicare tra loro e di scambiare dati, sia quando il minore sta bene, sia quando è affetto da una condizione patologica. In questo i mezzi informatici, intesi come strumenti di registrazione, comunicazione e analisi dei dati, così come dai dispositivi mobili, indossabili o i sistemi di intelligenza artificiale [2], possono essere di grande ausilio. Questo delicato processo tuttavia rende il minore un soggetto peculiare e potenzialmente vulnerabile, che necessita di tutele e garanzie particolari [3; vedi anche **Figura 1**].

Dato digitale	Posizione del dato
File su disco da allegare	hard-disk del mittente, cartella "documenti"
Messaggio di posta con file allegato	hard-disk del mittente, cartella del "client" di posta
Contenuto elaborato da inviare	server di invio (del mittente)
Contenuto elaborato ricevuto	server di ricezione (del destinatario)
Contenuto recapitato	hard-disk del destinatario, cartella del "client" di posta
File su disco dell'allegato	usb-pen del destinatario

Tabella 1. Esempio di possibile proliferazione dei dati con l'invio di un messaggio di posta elettronica con allegato: in particolare dell'allegato si creano più copie in posizioni differenti.

Figura 1. Materiale informativo a cura della Commissione Europea [4]. Il riconoscimento dei diritti del bambino è stato un passaggio fondamentale per lo sviluppo di politiche di tutela dell'infanzia, che si riflettono anche sulla gestione dei dati sensibili e informatizzati di natura sanitaria.

La gestione del dato sensibile in telepediatria

Alla luce di queste considerazioni, si pone il problema di come gestire tali informazioni anche considerando il regolamento europeo noto come GDPR [5]: in particolare esistono prescrizioni molto restrittive per i dati sensibili, in cui ricadono tutti i dati sanitari. Nel caso della branca pediatrica – come evidenziato anche dalle recenti pubblicazioni di istituti sanitari nazionali e internazionali [3,6-9] – la questione diventa ancora più complessa dato che si intrecciano le problematiche dovute alla minore età dei pazienti e alla presenza di soggetti terzi (il/i responsabile/i del minore) che hanno accesso a tali dati.
Per dare un'idea delle difficoltà da affrontare basti considerare che un semplice scambio di email contenente informazioni sanitarie potrebbe facilmente

portare a una violazione della disciplina, considerando che tale canale è tipicamente non protetto e che un semplice invio comporta spesso la generazione di diverse copie del messaggio o di parti di esso [Tabella 1] su cui il mittente ha un controllo limitatissimo.
Una gestione raffinata dei dati non può che valutare un qualche tipo di protezione alla fonte degli stessi, per cui risultano certamente preferibili sistemi che possano utilizzare delle forme di criptazione [10].
Il medico non dovrebbe preoccuparsi della soluzione informatica da un punto di vista tecnologico, ma ha certamente la responsabilità di adottare le dovute cautele nella scelta delle soluzioni (sia hardware che software). Il medico-pediatra deve tener conto ulteriormente della possibilità che i dati digitali siano oltre che ben "custoditi" anche accessibili da parte di tutti gli aventi diritto e in questo caso – come già evidenziato – è sempre presente almeno un responsabile maggiorenne oltre al soggetto minore.
Situazioni più complesse si hanno poi in altri casi, come per esempio per i sensori "wearable" (indossabili) dove la raccolta dei dati avviene solitamente tramite connessioni di rete e con salvataggi locali: risulta evidente che, se i dati fossero raccolti "in chiaro" (salvati su una memoria locale, come per esempio una piccola "card"), una semplice perdita del dispositivo comporterebbe la possibilità di accesso agli stessi a chiunque ne entrasse in possesso con un rischio altissimo di diffusione.

Codifica e trasmissione delle informazioni

C'è poi da considerare che la diffusione delle reti in modalità "wireless" richiederebbe di sfruttare comunicazioni ad alta sicurezza, tenendo presente che anche adottando una criptazione del traffico le informazioni possono essere oggetto di ispezioni e analisi malevole [11], per cui una codifica di base dei dati è comunque opportuna.
La criptazione, sfruttando una "chiave di codifica", trasforma un contenuto – per esempio un documento digitale – in una forma tale per cui è possibile risalire alle informazioni originali solo avendo a disposizione una opportuna "chiave di decodifica" (che può essere uguale o diversa dalla precedente a seconda della tecnica di criptazione utilizzata) e limitando quindi i rischi di interazioni indesiderate [12].

Prospettive per una soluzione efficace

La tutela del dato, come previsto dalla normativa nazionale ed europea, deve quindi poter essere garantita, tenendo conto anche degli attori in campo che – come il medico, l'operatore sanitario o l'insegnante – spesso non hanno una formazione puntuale in campo giuridico e nel complesso sottoambito della privacy.
Tenendo conto di tutto quanto detto, è possibile individuare alcuni punti che si ritengono utili per una soluzione efficace:

- adottare un sistema di criptazione a livello di dati e possibilmente anche a livello di trasmissione dei dati stessi (reti);
- avere accesso alle procedure di criptazione/decriptazione in modo molto semplice e il più trasparente possibile;
- far sì che le informazioni possano essere accessibili, eventualmente con differente granularità, da più soggetti;
- adottare una strategia che consenta di poter recuperare l'accesso a dati criptati nel caso che il/i soggetto/i avente/i diritto risultino impossibilitati a farlo: tale recupero deve ovviamente essere attuabile solo da altri soggetti abilitati a subentrare opportunamente.

Conclusioni

L'evoluzione della tecnologia ha aperto nuovi scenari in tutte le discipline coinvolgendo quindi anche la medicina e la pediatria. Il paziente bambino è coinvolto in molteplici realtà che interagiscono tra loro: nel caso dello scambio di informazioni di tipo sanitario si tratta di un soggetto particolarmente esposto a rischi legati alla privacy e per cui sono richieste specifiche garanzie anche a livello normativo. La gestione dei dati sanitari rientra nel più ampio campo dei cosiddetti "dati sensibili" per cui è necessario adottare soluzioni efficaci circa il loro trattamento e la loro trasmissione affinché il tutto avvenga in modo sicuro (funzionale alle necessità e nel rispetto di tutte le normative). Per trattare e comunicare in modo opportuno i dati sensibili con strumenti informatici occorre innanzitutto essere consapevoli di come questi gestiscono i dati stessi e possibilmente adottare tecniche di criptazione adeguate. In prospettiva si ritiene che sarebbe utile poter disporre di alcune funzionalità avanzate: criptazione sia a livello di dati che di comunicazione, procedure semplici e trasparenti che non richiedano competenze informatiche specifiche, accesso differenziato da parte di più soggetti agli stessi dati e possibilità di recupero delle chiavi di accesso da parte di soggetti abilitati in caso di necessità e sotto opportune condizioni. ■

Bibliografia

1. Capello F, Naimoli A E, Pili Giuseppe. Telemedicine for Children's Health. Springer, 2014.
2. Li-Qi Shu, Sun Yi-Kan, Tan Lin-Hua, et al. Application of artificial intelligence in pediatrics: past, present and future. World J Pediatr. 2019 Apr;15(2):105-108.
3. Gabbrielli F, Capello F, Tozzi AE, et al. Indicazioni ad interim per servizi sanitari di telemedicina in pediatria durante e oltre la pandemia COVID-19. Rapporto ISS COVID-19 n. 60/2020. Versione del 10 ottobre 2020.
4. European Commission. The European Union's Plan for Children's Rights. European Union editor, 2021.
5. REGULATION (EU) 2016/679: General Data Protection Regulation (GDPR), European Parliament and Council.
6. World Health Organization. From innovation to implementation: eHealth in the WHO European region: World Health Organization. Regional Office for Europe, 2016.
7. World Health Organization. How to plan and conduct telehealth consultations with children and adolescents and their families. 2021.
8. Curfman A, McSwain S D, Chuo J, et al. Pediatric Telehealth in the COVID-19 Pandemic Era and Beyond. Pediatrics. 2021 Sep;148(3):e2020047795.
9. Capello F. La telepediatria: prime indicazioni operative dagli USA. Quaderni acp. 2018;25:30-32.
10. Abbas A, Khan SU. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J Biomed Health Inform. 2014 Jul;18(4):1431-1441.
11. Papadogiannaki E, Ioannidis S. A survey on encrypted network traffic analysis applications, techniques, and countermeasures. ACM Computing Surveys (CSUR). 2021;54:1-35.
12. Oleiwi ZC, Alawsi WA, Alisawi WC, et al. Overview and Performance Analysis of Encryption Algorithms. Journal of Physics: Conference Series; 2020: IOP Publishing.

andrea.naimoli@unitn.it