



CARTAS A LA DIRECTORA

Registros electrónicos de salud. Nuevas tecnologías para proteger la privacidad del paciente



Electronic health records. New technologies to protect patient privacy

Sra. Directora:

La transformación digital ha supuesto la creación de grandes bases de datos para describir fenómenos biológicos. Los registros electrónicos de salud (EHR), con su capacidad ilimitada para la recuperación e intercambio de información médica, se han convertido en esenciales para validar y entrenar los algoritmos de la inteligencia artificial. La nueva medicina de precisión basada en los datos probablemente transformará la forma en que diagnosticamos, tratamos y nos relacionamos con el paciente. Sin embargo, ¿se acompañan estos avances de nuevos recursos para garantizar la confidencialidad y privacidad del paciente?

En los últimos años, se han descrito métodos basados en el aprendizaje profundo que podrían proporcionar una oportunidad tecnológica para obtener información médica de forma segura. Las redes neuronales han demostrado un potencial prometedor para la detección, clasificación y eliminación automática de información personal. Cada vez son más los estudios que analizan la precisión de estos sistemas para anonimizar los datos de los EHR. En el año 2017, Derroncourt et al. elaboraron un sistema basado en redes neuronales que se mostró superior a los sistemas tradicionales eliminando referencias de identidad de los datos¹. En otro trabajo, los campos aleatorios condicionales y las redes neuronales alcanzaron una precisión del 93% y del 96% respectivamente, superando de nuevo a los métodos de desidentificación convencionales².

Sin embargo, eliminar la información sensible de un EHR no garantiza totalmente la privacidad. A medida que se almacena información biomédica en múltiples categorías, se crea una «huella digital» del sujeto que promueve indirectamente la divulgación deductiva de su identidad^{3,4}. En este sentido, se han propuesto nuevos modelos basados en la privacidad diferencial. Una técnica que consiste en enmascarar información sensible introduciendo nuevos datos («ruido») obtenidos de una distribución de los originales^{5,6}. La incorporación de la privacidad diferencial a los EHR podría garantizar la confidencialidad del paciente, actuando como un filtro que permite obtener datos útiles para una población agregada, pero con demasiado «ruido» como para identificar a un paciente concreto. Es decir, cuanto más específica sea

la pregunta que le hagamos al registro, más inexacta será la respuesta obtenida. Este concepto puede favorecer y a la vez limitar la aplicación de estos modelos a la medicina de precisión, un escenario donde la introducción de grandes cantidades de «ruido» puede alterar considerablemente la calidad de los resultados obtenidos^{5,6}.

Los EHR pueden favorecer el acceso y la participación directa del paciente en la atención médica. Sin embargo, es necesario disponer de recursos adecuados para que los pacientes e investigadores accedan a la información protegidos de ciberataques u otras brechas de seguridad. La tecnología del «Blockchain» –cadena de bloques– podría crear un mecanismo seguro para gestionar el acceso a los EHR almacenados en una nube. Los EHR se convertirían, por tanto, en un registro compartido e inmutable de transacciones verificadas criptográficamente con acceso limitado únicamente a usuarios autorizados. Además, el «Blockchain» podría permitir que los investigadores recopilen información sobre un paciente a través múltiples sistemas independientes, garantizando en todo momento la consistencia e integridad de los datos⁷.

En la era del conocimiento globalizado, no hay duda de que compartir EHR potenciará los resultados de la investigación biomédica. Para disponer de grandes bases de datos, el intercambio de información entre diferentes centros (un proceso casi siempre condicionado por las políticas de acceso, uso e intercambio de datos médicos particulares) se ha convertido en una práctica fundamental. El aprendizaje profundo colaborativo ha surgido como respuesta a esta nueva necesidad, permitiendo entrenar una red neuronal por distintos participantes de forma cooperativa sin compartir los datos necesarios para tal fin⁸. Esta estrategia podría evitar el uso o tratamiento inadecuado de información privada del paciente, al mismo tiempo que proporciona el volumen de datos necesario para obviar los sesgos que genera la aleatoriedad.

Las restricciones y los procesos de acuerdo individuales para la confidencialidad de los datos pueden suponer una desventaja para la adquisición de información médica sensible. En ocasiones, un enfoque completamente ético convierte el diseño y desarrollo de un EHR en un proceso laborioso y costoso que reduce indirectamente el tamaño de la muestra y el poder del estudio. Estos inconvenientes en su mayoría podrían superarse con la aplicación de los modelos generativos, un novedoso sistema para la síntesis automática de información e imágenes médicas. Las redes generativas antagónicas y su propuesta de síntesis competitiva han demostrado su capacidad para generar EHR sintéticos «realistas» de forma precisa a partir de una colección de datos. Enfrentando 2 redes neuronales, estos

sistemas pueden aprender la distribución de las variables de los EHR y generar nuevos datos sintéticos que preserven las propiedades analíticas de los originales^{4,9}. La nueva información generada es una representación precisa, artificial y anónima de la realidad que puede aumentar la disponibilidad de datos y la precisión de las redes neuronales. Aunque no está exenta de limitaciones, esta tecnología revolucionará la investigación biomédica, dotando a los algoritmos de la inteligencia artificial de una mayor evidencia científica sin poner en peligro la privacidad del paciente

La innovación en salud exige que la tecnología que diseñamos mejore el valor de la asistencia que prestamos. Los EHR nos permitirán progresar en el diagnóstico y tratamiento de las enfermedades, siempre y cuando seamos capaces de abordar los problemas éticos relacionados con su aplicación. La privacidad y la confidencialidad en la medicina son valores centrales que requieren de una aplicación e interpretación continua en el contexto de una práctica clínica cambiante¹⁰. La investigación médica debe continuar descubriendo fuentes de datos y técnicas analíticas que contribuyan al conocimiento, al mismo tiempo que mantiene un compromiso con el uso ético de los datos³. Es el momento para que las nuevas tecnologías generen la confianza necesaria y nos permitan superar estas barreras con enfoques innovadores.

Fuentes de financiación

No

Conflictos de interés

Los autores declaran no tener ningún conflicto de intereses.

Bibliografía

1. Dernoncourt F, Lee JY, Uzuner O, Szolovits P. De-identification of patient notes with recurrent neural networks. *J Am Med Inform Assoc.* 2017;24:596–606.
2. Richter-Pechanski P, Amr A, Katus HA, Dieterich C. Deep learning approaches outperform conventional strategies in De-identification of German medical reports. *Stud Health Technol Inform.* 2019;267:101–9.
3. Mooney SJ, Pejaver V. Big data in public health: Terminology, machine learning, and privacy. *Annu Rev Public Health.* 2018;39:95–112.
4. Xiao C, Choi E, Sun J. Opportunities and challenges in developing deep learning models using electronic health records data: A systematic review. *J Am Med Inform Assoc.* 2018;25:1419–28.
5. Mao C, Zhao Y, Sun M, Luo Y. Are my EHRs private enough? Event-level privacy protection. *IEEE/ACM Trans Comput Biol Bioinform.* 2019;16:103–12.
6. Azencott CA. Machine learning and genomics: Precision medicine versus patient privacy. *Philos Trans A Math Phys Eng Sci.* 2018:376.
7. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing blockchains for efficient health care: Systematic review. *J Med Internet Res.* 2019;21:e12439.
8. Gong M, Feng J, Xie Y. Privacy-enhanced multi-party deep learning. *Neural Netw.* 2020;121:484–96.
9. Lee SH. Natural language generation for electronic health records. *NPJ Digit Med.* 2018;1:63.
10. McCoy TH Jr, Hughes MC. Preserving patient confidentiality as data grow: Implications of the ability to reidentify physical activity data. *JAMA Netw Open.* 2018;1:e186029.

Á. Iglesias-Puzas^{a,*}, A. Conde-Taboada^a, P. Boixeda^b y E. López-Bran^a

^a Servicio de Dermatología, Hospital Universitario Clínico San Carlos, Madrid, España

^b Servicio de Dermatología, Hospital Universitario Ramón y Cajal, Madrid, España

* Autor para correspondencia.

Correo electrónico: alvaroigpu@gmail.com

(Á. Iglesias-Puzas).

Disponible en Internet el 30 de marzo de 2020

<https://doi.org/10.1016/j.jhqr.2020.01.004>

2603-6479/ © 2020 FECA. Publicado por Elsevier España, S.L.U.

Todos los derechos reservados.

Cambios en los mecanismos de lesión en el traumatismo craneoencefálico en la población de edad avanzada



Changes in the mechanisms of injury in traumatic brain injury in the elderly

Sra. Directora:

La población geriátrica está aumentando de manera constante en los últimos años en los países desarrollados, estimándose que en España el número de personas con una edad igual o mayor de 65 años crecerá hasta los 14 millones de individuos en 50 años¹.

Unido a ello, esta franja poblacional presenta, a pesar de una mayor fragilidad biológica, una mayor actividad, con un alto grado de independencia funcional, por lo que están más expuestas a sufrir enfermedad traumática^{2,3}.

La enfermedad traumática representa un problema sanitario debido a su alta morbimortalidad, además de su asociación con grandes costes sanitarios⁴. Dentro de ella, el traumatismo craneoencefálico (TCE) representa el trauma más frecuente⁵.

Por todo lo anteriormente expuesto, el estudio del TCE está tomando una importancia creciente en nuestro medio^{5,6}, y los autores decidimos estudiar los cambios en el mecanismo de lesión y la presencia de trauma asociado al TCE en la población > 64 años ingresada en cuidados intensivos.