HISTORIALES CLÍNICOS ELECTRÓNICOS

Co-funded by the European Union

ESCAPE. *Preparing healthcare professionals for cyberattacks*
Project No.2023-1-ES01-KA220-VET-000151536

Socios

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.

Tabla de Contenidos

1. Definición 1
2. Relevancia general 1
3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados 1
4. ¿Qué puedo hacer como profesional sanitario? 1
5. Más información
    1. Materiales de aprendizaje 2
    2. Vídeos Relacionados 2
    3. Enlaces Relevantes 3
6. Bibliografía 3

Co-funded by the European Union

FACTSHEET – HISTORIALES CLÍNICOS ELECTRÓNICOS

1. Definición

Los historiales clínicos electrónicos son versiones digitales de los expedientes clínicos, los cuales contienen la historia médica, diagnósticos, medicación, tratamientos, e información relacionada. Son frecuentemente objeto de ciberataques1.

2. Relevancia general

El uso de historiales clínicos electrónicos incrementa la coordinación y la seguridad de la atención médica. La información se pone a disposición de manera instantánea para los usuarios autorizados, lo que fomenta una prescripción más segura, disminuye los errores, incrementa la eficiencia y reduce las cargas administrativas basadas en papel2.

La recopilación exhaustiva de las historias clínicas de los pacientes favorece la obtención de diagnósticos y tratamientos más precisos y seguros. Asimismo, se reduce la carga administrativa, se automatizan las derivaciones y se proporcionan recordatorios para el seguimiento de la atención3.

Sin embargo, las demandas excesivas de documentación pueden generar frustración y disminuir el tiempo dedicado a la atención de pacientes, lo que a su vez puede contribuir al agotamiento profesional entre los médicos de mayor edad. Además, si la formación recibida no es la suficiente, puede limitar la efectividad de los sistemas de registro electrónicos4.

3. Importancia en el ámbito de la salud e impacto en la calidad de los cuidados

Las historias clínicas electrónicas (EHRs) son fundamentales para garantizar la implicación del paciente, la exactitud y la continuidad a lo largo de todo su recorrido. Por ejemplo, la capacidad de los profesionales médicos para recuperar de manera ágil historiales médicos completos resulta especialmente útil en situaciones de emergencia5. Además, empoderan a los pacientes al permitirles acceder a información médica, programar citas y gestionar activamente su atención.

No obstante, los profesionales pueden sentirse abrumados por las tareas relacionadas con los EHR, lo que les distrae de la interacción con los pacientes. También puede dar lugar a pruebas mal etiquetadas o errores médicos si hay una deficiente interoperabilidad.

4. ¿Qué puedo hacer como profesional sanitario?

- Seguir las instrucciones y protocolos del proveedor cuando manipules dispositivos médicos.
- Informar de cualquier actividad sospechosa relacionada con estos instrumentos.
- Tener una buena ciberhigiene, utilizar contraseñas seguras y habilitar la autentificación en dos pasos.
- Concienciar a los pacientes del uso seguro de dispositivos médicos en sus hogares.

5. Más información

5.1 Materiales de aprendizaje

- Sequential videos for general topics about cybersecurity (JGT-2)
- Cibersecurity guide for healthcare sector (EU scope) (JGT-7)
- An article exploring the current state of cybersecurity in healthcare. (IST-36)
- An infographic on security and cybersecurity devices used in different healthcare settings. (IST-38)
- An overview of cybersecurity in healthcare, focusing on the role of AI and its regulatory framework. (IST-39)
- Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach (PRAMMER-35)

5.2 Vídeos Relacionados

Este vídeo explica acciones esenciales para garantizar la seguridad del paciente en entornos sanitarios, incluyendo comunicación efectiva, cultura de seguridad y prevención de errores.

Dispositivos médicos
https://youtu.be/qZStO1rWaQQ?si=_FwEhey9Q9KSY9zl

Este vídeo aborda la creciente preocupación por la seguridad de los dispositivos médicos conectados, como marcapasos, bombas de insulina y otros equipos IoMT (Internet de las Cosas Médicas). Estos dispositivos, al estar cada vez más integrados en redes hospitalarias, presentan riesgos significativos si no se gestionan adecuadamente.

Cibserseguridad en Dispositivos Médicos
https://youtu.be/TGNcNvTRgGc?si=T8zvELa9u84qQrGB

5. 3 Enlaces Relevantes

La creciente integración de dispositivos médicos conectados en los sistemas de salud presenta una amenaza significativa para la ciberseguridad, derivada de su susceptibilidad a la explotación por parte de actores maliciosos
https://www.illumio.com/es-mx/blog/connected-medical-devices-healthcare-cybersecurity-vulnerability

La FDA se dedica a ayudar a garantizar que los dispositivos médicos conectados estén protegidos de las amenazas de seguridad cibernética. Si se identifica una vulnerabilidad o deficiencia en el software, hardware u otro factor que pueda suponer un riesgo, la FDA puede emitir lo que se denomina una "comunicación de seguridad".
https://www.fda.gov/consumers/articulos-para-el-consumidor-en-espanol/seguridad-cibernetica-de-dispositivos-medicos-lo-que-necesita-saber

En este artículo, se analizan los nuevos problemas de ciberseguridad del sector, las normativas y los pasos importantes que puede dar para proteger y gestionar sus dispositivos médicos frente a las amenazas actuales y futuras.
https://es.digi.com/blog/post/medical-device-security

6. Bibliografía

Liveri, D., Drougkas, A., & Zisi, A. (2021). Cloud Security for Healthcare Services. ENISA.
https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf

Young, M. (2025, 22 enero). European Commission Publishes Action Plan on Cybersecurity of Hospitals and Healthcare Providers | Covington Digital Health. Covington Digital Health.
https://www.covingtondigitalhealth.com/2025/01/european-commission-publishes-action-plan-on-cybersecurity-of-hospitals-and-healthcare-providers/

Overview. (2025, 26 agosto). Public Health.
https://health.ec.europa.eu/medical-devices-sector/overview_en

World Health Organization: WHO. (2020, 2 julio). Medical devices.
https://www.who.int/health-topics/medical-devices

ESCAPE. Preparing healthcare professionals for cyberattacks
Project No.2023-1-ES01-KA220-VET-000151536

Co-funded by
the European Union

Este proyecto ha sido cofinanciado con el apoyo de la Comisión Europea. Esta publicación [comunicación] refleja únicamente las opiniones del autor, y la Comisión no puede ser considerada responsable del uso que pueda hacerse de la información contenida en la misma.