Rev Med Chile 2025; 153(9): 667-669. DOI: 10.4067/s0034-98872025000900667

# *Recomendaciones para el envío de información médica sensible a través de canales seguros*

# *Guidelines for the Transmission of Sensitive Medical Information via Secure Channels*

*Señor Editor:*

Los datos en salud constituyen una herramienta fundamental para la toma de decisiones clínicas y la planificación de tratamientos. La incorporación de la ficha clínica electrónica ha facilitado significativamente el almacenamiento y acceso a esta información; sin embargo, esta mayor accesibilidad también plantea nuevos desafíos en cuanto a la privacidad y la seguridad de los datos sensibles de los pacientes.

En la práctica clínica cotidiana, es común recurrir al envío de datos clínicos a través de correo electrónico o aplicaciones de mensajería instantánea como WhatsApp, debido a su rapidez y eficiencia en la comunicación. Esta tendencia se acentúa especialmente cuando se requiere consultar la opinión de especialistas que se encuentran fuera del centro asistencial o en lugares geográficamente distantes.

El principal problema del uso de canales no oficiales para la comunicación clínica es que los datos sensibles quedan almacenados fuera de la ficha clínica electrónica, lo que puede generar una fragmentación de la información en múltiples plataformas, muchas de ellas carentes de las medidas de seguridad adecuadas[1,2,3]. Esto no solo dificulta la trazabilidad y el acceso integral a la historia del paciente, sino que también expone dichos datos a riesgos de filtración. ¿Qué ocurriría, por ejemplo, si la cuenta de correo electrónico utilizada para compartir información clínica queda expuesta y un tercero accede sin autorización? En tal escenario, la confidencialidad de la información médica se vería comprometida, vulnerando gravemente la privacidad de nuestros pacientes.

La ficha clínica es el único lugar donde deben registrarse y almacenarse los datos de nuestros pacientes, ya que constituye un entorno seguro, diseñado específicamente para proteger su privacidad y garantizar la seguridad de la información. Cualquier dato que deba compartirse debe transmitirse exclusivamente a través de canales seguros, y toda conclusión o decisión clínica derivada de esa comunicación debe ser registrada adecuadamente en la ficha clínica, asegurando así la continuidad y trazabilidad de la atención médica.

Si bien corresponde a las autoridades competentes de cada institución establecer los lineamientos para la comunicación entre profesionales de la salud, a continuación, se proponen algunas recomendaciones orientadas a mitigar el riesgo de filtración de información sensible.

1. *Utilizar plataformas institucionales:* Priorizar el uso de sistemas de mensajería o correo electrónico institucional que cuenten con protocolos de seguridad avalados por la institución de salud.
2. *Evitar el uso de herramientas que no garantizan altos estándares de privacidad:* El uso de correos electrónicos personales o aplicaciones de mensajería instantánea como WhatsApp, aunque resulten prácticas y de uso extendido, no han sido diseñado para el intercambio de información de salud sensible. Estas plataformas suelen carecer de los controles de seguridad adecuados y no aseguran el cumplimiento de los estándares requeridos de confidencialidad y protección de datos. En la tabla 1 se presentan alternativas de comunicación que ofrecen mayores niveles de resguardo.
3. *Proteger la información clínica enviada con una contraseña:* Cuando sea necesario compartir información clínica por medios digitales, esta debe almacenarse en archivos protegidos por contraseña, la cual debe transmitirse por una vía de comunicación distinta a la utilizada para enviar el archivo.
4. *Minimizar los datos personales identificables:*

Al compartir casos clínicos para consulta, incluir solo la información estrictamente necesaria, evitando nombres, RUT u otros identificadores que no sean imprescindibles.

5. *Registrar en la ficha clínica todo intercambio significativo:* Toda opinión o recomendación clínica obtenida a través de una comunicación a distancia debe quedar documentada en la ficha clínica del paciente para asegurar la trazabilidad y continuidad de la atención.

Espero que estas observaciones y recomendaciones contribuyan a fomentar una reflexión crítica sobre las prácticas de comunicación clínica en la era digital y a promover el desarrollo de políticas institucionales que resguarden de forma efectiva la privacidad de los pacientes. Asegurar el adecuado manejo de la información médica no solo responde a una necesidad ética y legal, sino que es también un compromiso fundamental con la calidad y seguridad en la atención de salud.

**Tabla 1.** Comparación de métodos de comunicación alternativos en cuanto a seguridad y posibles limitaciones.

| **Alternativa** | **Características que reducen el riesgo de filtración de información** | **Desventajas** |
|---|---|---|
| Correo electrónico cifrado | - Cifrado de extremo a extremo en el contenido del mensaje (por ejemplo, usando PGP o plataformas como Proton Mail).<br>- Posibilidad de autenticación en dos pasos. | - Requiere configuración técnica específica.<br>- Interoperabilidad limitada con otros sistemas. |
| WhatsApp con contraseña de apertura y mensajes que se autodestruyen | - Cifrado de extremo a extremo<br>- Protección mediante bloqueo por huella digital o contraseña.<br>- Función de mensajes temporales (autodestrucción). | - No es una plataforma institucional.<br>- Almacena datos en dispositivos personales.<br>- Riesgo de copias, capturas de pantalla o reenvío accidental. |
| Telegram | - Cifrado opcional en “chats secretos”.<br>- Posibilidad de autodestrucción de mensajes.<br>- Protección con contraseña para apertura de la app.<br>- Cifrado de extremo a extremo predeterminado en todos los mensajes. | - No es una plataforma institucional.<br>- Pocos usuarios la utilizan. |
| Signal | - Función de mensajes que se autodestruyen.<br>- Sin almacenamiento en la nube.<br>- Código abierto. | - Interfaz menos familiar para algunos usuarios.<br>- Casi ningún usuario la utiliza. |

*Fabián Villena*[1,a,*].

[1]Facultad de Odontología, Universidad San Sebastián, Región Metropolitana, Chile.
[a]Cirujano-Dentista.

**Correspondencia: Fabián Villena / fabian.villena@uss.cl*
*Bellavista 7, Recoleta.*
*Región Metropolitana, Chile.*

*Fuente de apoyo financiero: Beca de doctorado nacional 21220200 de la Asociación Nacional de Investigación y Desarrollo de Chile.*

## Referencias

1. *Mars M, Morris C, Scott RE. WhatsApp guidelines – what guidelines? A literature review. J Telemed Telecare. 2019; 25(9): 524-529.*
2. *Masoni M, Guelfi MR. WhatsApp and other messaging apps in medicine: Opportunities and risks. Intern Emerg Med. 2020; 15(2): 171-173.*
3. *Morris C, Scott RE, Mars M. WhatsApp in Clinical Practice—The Challenges of Record Keeping and Storage. A Scoping Review. Int J Environ Res Public Health. 2021; 18(24): 13426.*