ECIJA
Avenida Escazú, Torre Lexus, Piso 3.
Escazú, San José, Costa Rica, 10203
Tel: +506 4000 1141
www.ecija.com

COVID-19. Consulta médica remota: aspectos legales a considerar

Mauricio París, Socio, ECIJA Costa Rica

Los datos relativos a la salud son datos personales sensibles, de acuerdo con la Ley 8968 de Protección de Datos Personales. Estos datos pueden ser tratados por un profesional de la salud para la prevención o diagnóstico médico (Art. 9.1.d Ley 8968), pero no por esa condición pierden su naturaleza de datos personales.

Las medidas actualmente tomadas por el Gobierno, y las que probablemente se tomen en los próximos días, generan la necesidad de todas las industrias de adaptarse a nuevas formas de prestar sus servicios y comercializar sus productos. La industria médica no es la excepción, y tanto servicios médicos de primera necesidad en una pandemia como la que nos acomete como otros que podríamos considerar accesorios, como la nutrición, la psicología o la dermatología.

Una de las soluciones de la industria médica es la telemedicina, en especial la consulta remota. Implementar esta solución por parte de médicos particulares, clínicas u hospitales no es tan sencillo como habilitar una conexión remota y hablar con el paciente. Si bien la consulta remota no está expresamente regulada en Costa Rica, dado que el médico tiene el compromiso de conocer e implementar todo lo que esté a su alcance para el mantenimiento de la salud individual y colectiva (Art. 12. Código de Ética del Colegio de Médicos), el uso adecuado de los medios tecnológicos a su alcance para la prestación de su servicio resulta un derivado lógico de dicho compromiso.

Pero no toda consulta médica puede ser objeto de consulta remota. En primer término, el profesional en medicina debe tener presente las limitaciones de la telemedicina, que impide que el médico pueda percibir menos elementos del paciente, por ejemplo: no podrá oler, no podrá palpar o auscultar al paciente, no podrá apreciar su lenguaje no verbal, o incluso podría no verlo del todo si la consulta es por teléfono, por mensajería instantánea o si las condiciones de conexión (por ejemplo, el ancho de banda de la conexión) no soportan una conexión por video. También podría haber problemas asociados a la calidad del propio audio. Todas estas condiciones deberán ser tomadas en consideración por el profesional a la hora de determinar si su especialidad permite ofrecer una consulta, si quiera inicial, por medios remotos.

De conformidad con el Código de Ética del Colegio de Médicos, independientemente del lugar donde se lleve a cabo el ejercicio de la profesión, toda consulta por parte del médico debe darse respetando los intereses e integridad del paciente. Derivado de esta disposición, la práctica de cualquier modalidad de telemedicina debe partir del consentimiento del paciente a utilizar medios telemáticos para la prestación del servicio.

Un elemento esencial es la protección de la privacidad y protección de datos del paciente. Los datos relativos a la salud son datos personales sensibles, de acuerdo con la Ley 8968 de Protección de Datos Personales. Estos datos pueden ser tratados por un profesional de la salud para la prevención o diagnóstico médico (Art. 9.1.d Ley 8968), pero no por esa condición pierden su naturaleza de datos personales, y el médico queda obligado no sólo al cumplimiento del secreto profesional, al deber de confidencialidad, sino también a adoptar las medidas técnicas y organizativas para garantizar la seguridad de los datos personales.

En ese sentido, el profesional en medicina debe cumplir **tres recomendaciones principales** en materia de privacidad en aplicación de consulta remota:

1. **Respetar el principio de minimización de datos personales**, es decir, debe recabar exclusivamente aquellos datos que resulten esenciales para la consulta que está realizando. Por ejemplo, si no es necesario grabar una sesión de videoconferencia de un psiquiatra con su paciente, será mejor no grabarla para no exponerse a que la grabación pueda ser accedida por una persona distinta del médico o del paciente, vulnerando así la confidencialidad y la protección de datos personales.

2. **Adoptar medidas de seguridad con respecto a la tecnología utilizada**. El médico no debe utilizar aplicaciones tecnológicas inseguras, que pongan en riesgo la información compartida por el paciente. Cualquier aplicación que utilice debe tener medidas de seguridad indispensables, como el cifrado punto a punto, la encriptación o el uso de redes privadas virtuales (VPN). Adicionalmente, si el médico almacena en su dispositivo, por ejemplo, imágenes corporales que sus pacientes le compartan, tal dispositivo (teléfono, tableta o computador) debe tener medidas de seguridad que eviten el acceso de la información en caso de pérdida o robo del dispositivo. Se debe evitar el almacenamiento de datos personales sensibles en nubes públicas y tomarse en consideración que compartir información médica de un paciente con otro profesional de la medicina requiere el consentimiento del paciente.

3. **Eliminar los datos personales una vez que no sean necesarios**. El médico debe tomar medidas para la eliminación de los datos personales del paciente de sus dispositivos remotos una vez que su utilización no sea necesaria, luego de almacenarlos en el expediente clínico respectivo. La eliminación de imágenes, chats, grabaciones, correos electrónicos, etc. que hayan sido recibidos por el médico una vez que haya finalizado la necesidad de su custodia, por ejemplo, porque el paciente ha sido dado de alta, resulta esencial para evitar pérdida o acceso no autorizado de datos personales.

Por último, cabe mencionar que la prescripción varios medicamentos se realiza hoy día por medio de prescripción electrónica, sistema que presenta múltiples beneficios para el paciente y el médico, incluyendo desde luego el que no resulte necesario retirar presencialmente la prescripción médica.