25 de mayo de 2016

Iniciativa de Medicina de Precisión: Base y Fundamentos de la Política de Seguridad de la Información

La misión de la Iniciativa de Medicina de Precisión (PMI) del Presidente es crear el nacimiento de una nueva era en la medicina, a través de estudios e investigación, tecnología y políticas que permitan a los pacientes, investigadores y proveedores trabajar juntos para lograr una atención personalizada. Con los Principios de Privacidad y Confianza de la PMI como punto de partida, este documento delinea los principios de la política de seguridad y ofrece un marco que guia decisiones por parte de las organizaciones encargadas de actividades de medicina de precisión o que participan de ellas. Con el objetivo de reconocer que no es posible asegurar la seguridad de la información con solo un enfoque que es igual para cada aplicación, este documento ofrece un marco amplio para la protección de la información y los recursos de los participantes de una manera adecuada y ética, y que además se puede adaptar a los requisitos específicos de cada organización.

Este documento fue creado para que la comunidad del sector de la medicina de precisión lo utilice como base para sus propias necesidades de seguridad de la información. La seguridad de la información es un campo en constante evolución, y todos los días se identifican amenazas y riesgos nuevos. Estos principios y este marco se deberán ir actualizando con el tiempo para responder a nuevas circunstancias y nuevas amenazas. No hay ningún punto en este documento con el objeto de impedir la publicación de la información que le corresponda, siempre que no permita individualizar ni identificar a nadie. Este tipo de información incluye datos acumulados de estudios, hallazgos de investigaciones e información acerca de estudios de investigación en curso. Muchos de los principios a continuación posiblemente ya sean obligatorios por ley para algunas organizaciones de PMI conforme. Las organizaciones de PMI deberán seguir a toda la legislación y normativa vigente que rige la privacidad, seguridad y protección de la información de PMI en cada etapa de la obtención, almacenamiento, análisis, mantenimiento, uso, publicación, intercambio y divulgación de esta información.

Este documento fue elaborado a través de un proceso colaborativo, con la participación de varias agencias, y el aporte de la Oficina para Políticas de Ciencia y Tecnología, el Consejo Nacional de Seguridad, el Servicio Digital de los Estados Unidos, el Instituto Nacional de Normativa y Tecnología, la Comisión Federal de Comercio, el Departamento de Asuntos de los Veteranos, el Departamento de Defensa, y el Departamento de Salud y Servicios Humanos, incluyendo su Oficina de Derechos Civiles, la oficina del Coordinador Nacional de TI aplicada a la Salud, los Institutos Nacionales de la Salud, la Administración de Alimentos y Medicamentos y los Centros de Servicios de Medicare y Medicaid. Estos principios y este marco surgen de las conclusiones de una serie de comités con expertos en seguridad académicos y del sector privado, y una revisión de los recursos de seguridad de la información actuales. Todos los departamentos y agencias del gobierno nacional que participan de la PMI se comprometen a implementar y hacer cumplir los principios y el marco que se describen en este documento, cuando corresponda a sus actividades.

La seguridad exige una serie constante de procesos y controles que adapta y que permitan enfrentar a los riesgos internos y externos y garantizar la confidencialidad,[1] integridad,[2] y disponibilidad[3] de la información generada y aportada durante las actividades de medicina de precisión. Las organizaciones que llevan adelante investigaciones relacionadas con la medicina de precisión deben tomar conciencia de que garantizar la seguridad de la información es un proceso constante y que deben esforzarse por apelar a las mejores prácticas actuales.

Dado que las mejores prácticas en términos de seguridad dependen en gran medida del contexto, cada organización deberá realizar su propia evaluación integral de riesgos para identificar los requisitos específicos de seguridad y generar procesos que permitan revisar y mejorar sus prácticas de manera constante.

La información aportada por los participantes es el recurso fundacional de la PMI, y los participantes merecen que se les garantice que está siendo protegida y utilizada de manera responsable. Para poder generar confianza y fomentar la participación masiva y el aporte de datos de salud, las organizaciones de PMI deben adoptar políticas y prácticas consistentes, ser claras acerca de sus objetivos y expectativas, y transparentes con respecto a los sistemas y uso de la información.

Las siguientes son algunas consideraciones inherentes a la medicina de precisión que orientaron la elaboración de este documento:

- Los tipos de información utilizada para las actividades de PMI pueden incluir, entre otros datos, información de reclamaciones de seguro y clínica; datos demográficos y de encuestas; datos derivados de información genómica y otros especímenes biológicos; y datos de dispositivos u otros equipos móviles, informativos o de otro tipo. Toda esta información se puede guardar en formato electrónico o en papel. A lo largo de este documento, se hará referencia a todos estos datos como "información de PMI". La información de PMI es altamente sensible para los participantes y exige un nivel alto de protección de su seguridad y privacidad.
- El objeto de este documento es que lo usen las organizaciones de PMI como instituciones, prestadores de servicios y otras entidades que obtienen, utilizan, analizan o comparten información de PMI.
- Los principales usuarios de información de PMI incluyen a participantes individuales, investigadores, desarrolladores, científicos civiles,[4] y proveedores de servicios de salud.
- Las organizaciones de PMI tienen la libertad de aprovechar la arquitectura del sistema según lo necesiten, incluyendo los aspectos de seguridad, como metodologías de bases de datos que se guardan en la nube o mecanismos de enclave.

---

[1] Se considera pérdida de confidencialidad el uso o divulgación no autorizados de información.
[2] Se considera pérdida de integridad la modificación no autorizada o destrucción de información.
[3] Se considera pérdida de disponibilidad la interrupción del acceso autorizado a o uso de la información o de un sistema de información.
[4] En ciencia civil, el público participa de manera voluntaria del proceso científico, abordando problemas del mundo real de maneras que pueden incluir formular preguntas de investigación, llevar adelante experimentos científicos, obtener y analizar datos, interpretar resultados, hacer descubrimientos nuevos, desarrollar tecnologías y aplicaciones, y resolver problemas complejos.

- Este documento aborda las medidas de seguridad para proteger la información de PMI, que incluye datos y metadatos asociados a especímenes biológicos recogidos como parte de las actividades de PMI. Existen otros requisitos relacionados con la seguridad física, que las organizaciones de PMI deben respetar y que se encuentran fuera del alcance de este documento.
- Convertir la información en anónima consiste en eliminar cualquier información que permita identificar a una persona (como nombre, fecha de nacimiento, dirección, número de seguro social) de un juego de datos, para que la información no se pueda

vincular a ninguna persona en particular, ni de manera directa ni de manera indirecta. La eliminación de la identificación es un control técnico importante que las organizaciones de PMI deben emplear cuando corresponda, y que puede ayudar a proteger la privacidad de un participante. Sin embargo, no hay ningún proceso de eliminación de la identificación que garantice que no resulte posible volver a identificar a las personas. En consecuencia, las organizaciones no deben apoyarse en la eliminación de la identificación como única medida de seguridad o técnica de protección de la privacidad.

Base de la Política de Seguridad

Los siguientes son los principios dominantes que deberían orientar a las organizaciones al elaborar e implementar un plan de seguridad adecuado. Las organizaciones de PMI deben, como mínimo:

- Esforzarse por crear un sistema que genere la confianza de los participantes. Esto implica adoptar un enfoque en el que la prioridad es el participante al momento de identificar y enfrentar riesgos de seguridad de la información. Los participantes son componentes fundamentales de todas las actividades de investigación.
- Reconocer que la seguridad, la medicina y la tecnología evolucionan rápidamente. En consecuencia, las organizaciones deben considerar la seguridad uno de los componentes centrales de su cultura y servicios, y garantizar que los procesos y controles de seguridad se puedan adaptar y actualizar.
- Procurar preservar la integridad de la información, de manera que esta resulte confiable para los participantes, investigadores y médicos y otros proveedores de servicios de salud.
- Identificar los riesgos clave y elaborar planes de evaluación y gestión que enfrentan dichos riesgos, al tiempo que proveen el avance de las investigaciones y de la ciencia.
- Proveer a los participantes y a otras partes relevante expectativas claras y procesos de seguridad transparentes.
- Usar prácticas y controles de seguridad para proteger la información, pero no como motivo para denegar a un participante el acceso a su información ni como una

excusa para limitar los usos adecuados de la información con fines de investigación.

- Actuar de manera responsable. Procurar reducir al mínimo la exposición de la información de los participantes y mantener a los participantes e investigadores al tanto si se produce algún tipo de intrusión, para sostener la relación de confianza a lo largo del tiempo.
- Compartir sus experiencias y retos, para que las organizaciones puedan aprender unas de otras.

Lograr los Principios a través de los Fundamentos de la Política de Seguridad de la Información de la Iniciativa de Medicina de Precisión

Hay varios marcos en los que las organizaciones de PMI pueden basar la organización de sus programas de seguridad de la información. Esta sección se basa en un marco elaborado por el Instituto Nacional de Normas y Tecnología (NIST). El NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (Marco del NIST para Mejorar la Seguridad de la Información de Infraestructura Crítica, versión 1.0) define una serie de actividades, resultados y referencias que permiten a las organizaciones habilitar cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder y recuperar, como herramientas para evaluar el desempeño de los procesos de seguridad informática y de la información, además de los controles físicos y ambientales.[5] Las organizaciones deben elegir el marco de seguridad que aborde de manera correcta los riesgos de seguridad que enfrentan, y que esté en línea con las Bases y Fundamentos de la Política de Seguridad de la Información de la PMI.

---

[5] NIST Framework for Improving Critical Infrastructure Cybersecurity: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf