

DOCUMENTO INFORMATIVO SOBRE CONFIDENCIALIDAD, DEBER DE SECRETO Y USO ADECUADO DE LA INFORMACIÓN

El presente documento tiene por finalidad recordar y reforzar el conocimiento de los derechos y las obligaciones legales y profesionales aplicables al personal al servicio de las instituciones sanitarias del Servicio Madrileño de Salud, sin que implique la creación de nuevas obligaciones distintas de las establecidas por la normativa vigente.

El deber de confidencialidad se enmarca en una responsabilidad compartida entre la organización y las personas que prestan servicios en sus instituciones sanitarias. A tal efecto, el Servicio Madrileño de Salud promoverá las medidas organizativas, formativas y técnicas necesarias para garantizar la adecuada protección de la información y de los datos personales tratados en el ejercicio de la actividad asistencial y administrativa.

Primero. Objeto y ámbito de la información

El personal que preste servicios en el ámbito del Servicio Madrileño de Salud, cualquiera que sea la naturaleza laboral, estatutaria, funcionarial, formativa o de otra índole de su relación con este, está sujeto al deber de confidencialidad y secreto respecto de toda la información a la que acceda con ocasión del desempeño de sus funciones, actividades o tareas.

Estas obligaciones resultan exigibles con independencia del soporte, formato o medio, físico o electrónico, en el que se encuentre la información y de la forma en que se haya tenido acceso a ella.

La presente información se facilita de conformidad con la normativa estatal, europea y autonómica aplicable, incluyendo la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, y demás disposiciones reguladoras de las instituciones sanitarias del Servicio Madrileño de Salud.

Segundo. Acceso y utilización de la información

El acceso a la información, datos, aplicaciones, sistemas y recursos deberá limitarse estrictamente a aquellos que resulten necesarios para el desempeño de las funciones asignadas y realizarse exclusivamente mediante los perfiles, permisos y credenciales autorizados.

La información a la que se tenga acceso únicamente podrá ser utilizada para el cumplimiento de las funciones, actividades o tareas encomendadas y para las finalidades debidamente autorizadas. Queda prohibido todo acceso que no responda a una necesidad funcional debidamente justificada, incluidos los accesos motivados por interés o curiosidad personal o por cualquier finalidad ajena a las funciones asignadas.

Queda expresamente prohibido el acceso a historias clínicas o a cualquier otra información sanitaria cuando no exista una necesidad asistencial, organizativa, de gestión o una habilitación legal que lo justifique. Los accesos a los sistemas de información y a la documentación clínica podrán ser registrados, auditados y verificados conforme a la normativa vigente y a las políticas de seguridad de la información aplicables.

Tercero. *Información protegida*

El deber de confidencialidad y secreto comprende, en particular:

- a) La información clínica y asistencial y los datos personales de pacientes, usuarios, profesionales y cualesquiera otras personas.
- b) La información organizativa, administrativa, económica, contractual, jurídica, técnica, científica, investigadora o de seguridad que no sea de dominio público.
- c) Los procedimientos, protocolos, métodos de trabajo, conocimientos, sistemas, aplicaciones, configuraciones, credenciales y demás recursos de información.
- d) Las obras, contenidos, desarrollos, conocimientos técnicos, resultados de investigación y demás elementos protegidos por derechos de propiedad intelectual o industrial a los que se acceda con carácter reservado, sin perjuicio de la titularidad y del régimen jurídico que en cada caso resulten aplicables.
- e) Cualquier información recibida de otras entidades o personas que esté sujeta a deber de confidencialidad o reserva.

En particular, respecto de la información clínica y asistencial, deberán respetarse los derechos de intimidad y confidencialidad reconocidos en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente.

No tendrá la consideración de información protegida aquella que sea de dominio público por medios legítimos, cuya comunicación haya sido expresamente autorizada por el órgano competente o que deba facilitarse en cumplimiento de una obligación legal o de un requerimiento de autoridad competente.

Asimismo, resultan de obligado cumplimiento las obligaciones de secreto profesional inherentes al ejercicio de las profesiones sanitarias y al desempeño de funciones en instituciones sanitarias del Servicio Madrileño de Salud, de conformidad con la normativa sanitaria vigente.

Cuarto. *Reglas de custodia y seguridad*

En materia de custodia y seguridad de la información deberán observarse, entre otras, las siguientes reglas:

- a) No comunicar, revelar, reproducir, copiar, alterar, extraer o utilizar la información sin autorización o para fines distintos de los funcionalmente necesarios y debidamente autorizados.
- b) No retirar, almacenar ni transmitir información mediante dispositivos, soportes, cuentas de correo, servicios en la nube, aplicaciones o sistemas que no sean corporativos o no estén permitidos por las políticas e instrucciones de seguridad aplicables.

- c) Custodiar adecuadamente los documentos, dispositivos y soportes que contengan información protegida y evitar que puedan acceder a ellos personas no autorizadas.
- d) Mantener bajo control exclusivo las credenciales y medios de autenticación asignados, sin comunicarlos, compartirlos o permitir su utilización por terceras personas.
- e) Cumplir las políticas, instrucciones, protocolos y medidas de seguridad establecidos por el centro y por el Servicio Madrileño de Salud.
- f) Comunicar sin demora indebida, por los canales o unidades habilitadas al efecto, cualquier pérdida, acceso indebido, revelación, alteración, envío erróneo o incidente que pueda comprometer la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información.

Quinto. *Políticas de seguridad y buenas prácticas en el uso de los sistemas de información*

Resultan de aplicación la Política de Seguridad de la Información en el ámbito de la Administración electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid, aprobada por Orden 491/2013, de 27 de junio, el Decálogo de Buenas Prácticas para Usuarios de Sistemas de Información de la Consejería de Sanidad y las demás políticas, normas, instrucciones, protocolos y procedimientos de seguridad que correspondan en cada caso.

Las personas que accedan a los sistemas de información deberán observar dichas disposiciones y buenas prácticas en el acceso, utilización y custodia de la información, sistemas, aplicaciones, equipos, dispositivos, credenciales y demás recursos tecnológicos puestos a su disposición.

Sexto. *Protección de datos personales*

El tratamiento de datos personales queda sometido a las obligaciones derivadas del Reglamento (UE) 2016/679, de la Ley Orgánica 3/2018, de 5 de diciembre, y de las demás disposiciones aplicables en la materia.

El tratamiento de datos personales deberá realizarse exclusivamente para el desempeño de las funciones asignadas, de conformidad con las instrucciones recibidas y con las medidas de seguridad establecidas.

La autorización de acceso a los datos personales queda limitada al desempeño de las funciones asignadas y no permite su utilización, comunicación, copia, extracción o conservación para fines propios, de terceros o distintos de los autorizados.

En particular, los datos relativos a la salud tienen la consideración de categorías especiales de datos personales y estarán sujetos a las medidas reforzadas de protección, confidencialidad y seguridad previstas en el Reglamento (UE) 2016/679, en la Ley Orgánica 3/2018 y en la restante normativa sanitaria aplicable.

Respecto de la información clínica y asistencial, deberán respetarse igualmente los derechos de intimidad, confidencialidad y protección de la documentación clínica reconocidos en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Séptimo. *Comunicaciones legalmente protegidas*

Las obligaciones establecidas en este documento no impedirán ni limitarán:

- a) Las comunicaciones de información comprendidas en el ámbito de aplicación de la Ley 2/2023, de 20 de febrero, y realizadas en los términos previstos en ella, a través del Sistema interno de información o de los canales externos legalmente establecidos.
- b) Las revelaciones públicas realizadas cuando concurren los requisitos previstos en dicha ley.
- c) La puesta en conocimiento de hechos ante autoridades judiciales, fiscales, policiales, administrativas o de control, cuando se realice en el ejercicio legítimo de un derecho, en cumplimiento de un deber o en los demás supuestos previstos por el ordenamiento jurídico.
- d) Las comunicaciones efectuadas en cumplimiento de una obligación legal o de un requerimiento de autoridad competente.

La organización dispone de sistemas y canales habilitados para la comunicación de información prevista en la Ley 2/2023, de 20 de febrero, así como de las garantías de confidencialidad de la identidad de la persona informante, protección de datos personales y protección frente a represalias en los términos legalmente establecidos.

Octavo. *Finalización de la relación*

Cuando finalice la relación con el centro, deberán devolverse los documentos, dispositivos, soportes y demás recursos facilitados, cesar en el acceso a los sistemas y abstenerse de conservar copias de la información fuera de los sistemas corporativos. La devolución, conservación, bloqueo o supresión de la información se realizará conforme a la normativa aplicable y a las instrucciones del órgano competente, sin que las personas sujetas a estas obligaciones puedan destruir por iniciativa propia documentos o información sujetos a deberes de conservación.

Noveno. *Subsistencia del deber de secreto*

El deber de confidencialidad y secreto subsistirá tras la finalización, por cualquier causa, de la relación laboral, estatutaria, funcional, formativa o de otra naturaleza, durante el tiempo establecido en la normativa aplicable y, cuando esta no determine un plazo específico, mientras la información conserve su carácter confidencial o reservado.

Décimo. Responsabilidades

El incumplimiento de las obligaciones contenidas en este documento podrá dar lugar, atendiendo a la naturaleza, gravedad y circunstancias de los hechos, a las responsabilidades disciplinarias, administrativas, patrimoniales, civiles, contractuales o penales que resulten procedentes conforme al régimen jurídico aplicable en cada caso, sin perjuicio de las infracciones o sanciones previstas en la normativa aplicable.

D./D.ª _____,
con DNI/NIE _____, declaro haber recibido el presente documento
informativo en esta fecha.

Y para que conste, firmo el presente recibí.

En _____, a ____ de _____ de _____.

Fdo.: _____