PROTECCIÓN DE DATOS

POLÍTICA DE SEGURIDAD

El Hospital Guadarrama cuenta con una Política de Seguridad que es actualizada anualmente. Se encuentra en INTRANET: GERENCIA-PROTECCION DE DATOS-Política de Seguridad de la Información y Protección de datos.

Todos los trabajadores están obligados a cumplir las recomendaciones sobre confidencialidad y tratamiento de los datos.

INCIDENCIAS

En el Hospital Guadarrama se ha constituido un Comité de Seguridad de la Informacion y Protección de Datos Personales, que trabaja permanentemente en la seguridad de los datos personales y garantiza su seguridad.

Cualquier incidencia que se observe en materia de datos personales, podemos ponerla en conocimiento del Comité a través del formulario que se encuentra en INTRANET: GERENCIA-PROTECCION DE DATOS-PNT 11 Gestión de Incidencias de Seguridad.

DECALOGO DE BUENAS PRACTICAS EN PROTECCION DE DATOS

1. Trata los datos de las personas como querrías que tratasen los tuyos. Para el uso de datos para una finalidad distinta a la asistencial y grabaciones o utilización de imágenes es obligatorio el consentimiento de la persona o cualquier otro medio que garantice el anonimato en su uso
2. ¿Estás seguro de que tienes que acceder a esa historia clínica? Piénsalo. Sólo debes hacerlo si es necesario para los fines de tu trabajo. Recuerda: los accesos a la documentación clínica quedan registrados en el sistema.
3. Evita informar a terceros sobre la salud de tus pacientes salvo que estos lo hayan consentido o tengas una justificación lícita.
4. Cuando salgas del despacho, asegúrate de cerrar la sesión abierta en tu ordenador, cierra con llave los armarios o archivadores que contengan documentación confidencial. No dejes dicha documentación a la vista sin supervisión.
5. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente contacta con el servicio de informática.
6. No envíes información con datos sensibles por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si tienes que hacerlo, no olvides cifrar los datos.
7. No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro.
8. Vigilar donde se da la información sensible, debe darse en despachos, evitar comentarios en los pasillos o delante de otros.
9. No crees por tu cuenta ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informática. No se pueden crear ficheros paralelos.
10. Está prohibido sacar documentación confidencial mediante soporte informático, salvo autorización previa.