MANUAL DE USO DE MEDIOS TECNOLÓGICOS Y OBLIGACIONES DEL PERSONAL SANITARIO DE LA FUNDACIÓN PARA LA INVESTIGACIÓN BIOMÉDICA DEL HOSPITAL UNIVERSITARIO DE GETAFE EN MATERIA DE PROTECCIÓN DE DATOS

1. El Delegado de Protección de Datos (DPD) de la Fundación para la Investigación Biomédica del Hospital Universitario de Getafe (en adelante, "FIBHUG") es Alaro Avant [dpo.fibgetafe@alaroavant.com o protecciondedatos@iisgetafe.com].
2. Sólo puedes tener acceso a la información que necesitas para el desarrollo de tu puesto de trabajo.
3. El tratamiento de datos de carácter personal (datos que identifiquen, de forma directa o indirecta, a una persona) únicamente podrá realizarse si se cuenta con una base legal para ello:
    - Consentimiento del interesado
    - Ejecución de un contrato entre FIBHUG y el interesado
    - Interés legítimo de FIBHUG, con la previa ponderación de intereses
    - Interés público
    - Interés vital del interesado
    - Obligación legal (existencia de normativa que respalde el tratamiento)
4. Independientemente de la base legal, se deberá informar al interesado, de forma previa, sobre los siguientes extremos:
    - Identidad y contacto del responsable del tratamiento
    - Base legal del tratamiento
    - Plazos de conservación de los datos
    - Transferencias internacionales de datos (fuera de la UE), en su caso
    - Cesiones o comunicaciones de datos a terceros, en su caso
    - Posibilidad de ejercitar derechos, incluido el de revocación de su consentimiento
    - Derecho a reclamar a una autoridad de control
5. Los proveedores externos que presten servicios a FIBHUG deberán firmar un Contrato de Encargado de Tratamiento donde se establezcan las instrucciones, requisitos, obligaciones y pautas de un determinado tratamiento de datos que se efectuará por el proveedor en nombre de FIBHUG.
6. Únicamente deberán recogerse datos de carácter personal estrictamente necesarios para el cumplimiento de la finalidad del tratamiento. Los datos recogidos que no son necesarios, o aquellos que han dejado de ser necesarios para una determinada finalidad, deberán eliminarse en la mayor brevedad posible.
7. En caso de que algún interesado ejercite un derecho (acceso, oposición, rectificación, supresión, etc.), se deberán dar trámite a su solicitud y responder en un plazo máximo de 30 días desde la recepción de la solicitud.
8. En caso de una brecha de seguridad (destrucción, pérdida o alteración accidental, ilícita o no autorizada de datos de carácter personal), se deberá:
    - Comunicar internamente la incidencia al DPD y Responsable de Sistemas
    - Documentar la brecha en el registro de incidencias
    - Adoptar medidas reactivas para minimizar o corregir la brecha
    - Valorar la incidencia para decidir si es necesaria una comunicación a la Agencia Española de Protección de Datos (en adelante, AEPD) y el interesado

La comunicación a la AEPD, en caso de ser necesaria, deberá realizarse en un plazo máximo de 72 horas desde el conocimiento de la brecha. La comunicación al interesado, en caso de ser necesaria, deberá realizarse sin dilación indebida.

9. Con carácter general, los Medios Tecnológicos de FIBHUG facilitados, tanto al personal de plantilla como al personal externo (en adelante, y de forma conjunta, "empleado" o "empleados"), deben ser considerados herramientas de trabajo de FIBHUG, por lo que el uso de los mismos debe estar destinado exclusivamente a fines profesionales y al cumplimiento de las prestaciones para las que fue contratado el empleado, debiendo utilizarse de forma adecuada a su naturaleza y a sus fines profesionales, quedando totalmente prohibido cualquier uso personal o privado de los Medios Tecnológicos por los empleados de FIBHUG, por lo que no se generará ninguna expectativa de intimidad o privacidad sobre los mismos o sobre el uso que se haga de ellos por parte de los empleados.
10. En consecuencia, todos los Medios Tecnológicos serán accesibles por FIBHUG pudiendo ser en cualquier momento, formateados y/o reseteados. Por lo tanto, el empleado no archivará ni guardará información personal o privada en los Medios Tecnológicos no relacionada con su actividad profesional en FIBHUG.
11. En todo caso, queda prohibida la utilización de los Medios Tecnológicos que suponga la violación del presente manual y/o de la buena fe contractual que debe presidir en todo momento la relación laboral suscrita con los empleados. Dado que los Medios Tecnológicos son herramientas exclusivas de trabajo, los empleados no deberán transmitir, distribuir, almacenar, descargar, instalar, copiar, visualizar o enviar contenidos ajenos al desarrollo de la actividad profesional de FIBHUG.
12. Con relación a las obligaciones, prohibiciones y/o limitaciones sobre la facultad de control de FIBHUG en el uso de los Medios Tecnológicos facilitados por ésta a los empleados para el cumplimiento de las prestaciones para las que fueron contratados, FIBHUG respetará y observará lo dispuesto en la normativa aplicable y vigente en cada momento.
13. Al incorporarte por primera vez a tu puesto, te serán facilitadas las contraseñas informáticas necesarias para el desarrollo de tus funciones:
    - Eres responsable de tu contraseña, no debes de cedérsela a nadie. No debes anotar las contraseñas en lugares visibles o localizables con facilidad.
    - Estás obligado a comunicar al DPD, o al Responsable de Sistemas, la pérdida, olvido o sospecha de que alguien la esté usando.
    - OJO, con las contraseñas: no des a "Recuerda la contraseña en este equipo". Sobre todo, las contraseñas que utilices para entrar en el software y con mayor cuidado de no hacerlo en tu domicilio o algún ordenador de uso público.
14. No está permitida la descarga, instalación, modificación o eliminación de programas o aplicaciones en los equipos salvo que cuentes con autorización expresa del Responsable de Sistemas. No se deben guardar informes, videos o fotos en el escritorio de tu equipo.
15. Cuando te ausentes de tu puesto físico de trabajo, cierra el armario donde guardas datos de carácter personal, en caso de que tuvieras acceso a los mismos, y cierra tu sesión del ordenador. No dejes documentos a la vista y oculta los datos de la pantalla de forma que no se pueda acceder a los ficheros sin introducir la contraseña. Tu ordenador tiene que suspenderse cuando no lo utilices.
16. En relación a los ensayos clínicos, no puedes realizar tratamiento de datos personales identificativos de pacientes. Todos los datos deben haber sido previamente

seudonimizados por parte del investigador principal o de los facultativos del Hospital que no intervengan en el ensayo o estudio clínico.

17. Siempre que vayas a desechar o reutilizar cualquier tipo de soporte, debes asegurarte del borrado de la información o de la destrucción total del mismo. Si la información se encuentra impresa en papel, utiliza el contenedor habilitado para este fin ubicado en Secretaria.
18. NO debes extraer información de las instalaciones de FIBHUG, sin la autorización del DPD.
19. No está permitido el uso de equipos, terminales de acceso remoto, ordenadores de sobremesa o portátiles, tablets y/o dispositivos similares o equivalentes particulares propiedad de los empleados de FIBHUG para fines profesionales, sin la previa autorización del DPD y su posterior registro en el Registro de Sistemas. En todo caso, se utilizarán en cumplimiento de las medidas de seguridad e indicaciones de FIBHUG.
20. OJO con la utilización de móviles particulares. Debes tener el móvil con sistema de bloqueo personalizado por si usas el correo electrónico de FIBHUG. NO hagas fotografías ni realices grabaciones de ensayos / estudios clínicos con tu móvil.
21. Si envías datos de carácter personal por el mail, estos documentos deben estar cifrados.
22. Obligatoriamente comunica por email al DPD todas las incidencias que afecten a la integridad de la información, como, por ejemplo: pérdidas o extravíos de información (tanto informática como manual), si encuentras información en una ubicación distinta a la asignada, si tienes problemas en los accesos autorizados, etc.
23. En relación al uso del correo electrónico corporativo, cada empleado accederá únicamente a la dirección que le haya sido facilitada por FIBHUG. El uso correcto del servicio de correo electrónico, supone que el empleado no debe utilizarlo para la comisión de cualquier ilícito contemplado en la normativa vigente. Asimismo, se prohíben las acciones que se muestran a continuación:
    - Vulnerar las normas internas de Seguridad de la Información.
    - Acceder o utilizar la cuenta de correo electrónico de otro empleado o profesional sin autorización.
    - Suplantar -o intentar suplantar- a otros empleados de FIBHUG utilizando este medio.
    - Divulgar información de uso interno, confidencial o sensible de FIBHUG. Con carácter general, no se permite a los empleados redireccionar automáticamente los correos electrónicos recibidos en cuentas de correo corporativas a cuentas de correo no corporativas y viceversa. En el caso de que un empleado necesite redireccionar una cuenta de correo, deberá solicitar autorización motivada y por escrito de FIBHUG, que se ocupará de ejecutar, si finalmente se aprueba, el redireccionamiento.
    - Acceder o utilizar la cuenta de correo electrónico de FIBHUG asignada para fines personales.
24. FIBHUG podrá acceder al correo de los empleados cuando existan indicios suficientes de que un empleado ha incumplido las estipulaciones del presente Manual y/o demás normativa interna existente de FIBHUG.
25. Igualmente, FIBHUG podrá redireccionar el correo de los empleados durante su ausencia temporal (vacaciones, incapacidad temporal, excedencia, etc.) o definitiva, tras su marcha de FIBHUG por extinción de su relación laboral o profesional por cualquier causa. En estos casos de ausencia del empleado, el DPD solicitará al departamento correspondiente que se autorice el redireccionamiento del buzón de correo del empleado o profesional a las cuentas de correo internas que determine FIBHUG.

26. FIBHUG facilita y permite a los empleados el acceso a Internet en función de la necesidad para la correcta prestación de los servicios contratados. En este sentido, el empleado es responsable del material que visualice y descargue de internet. Por tanto, debe realizar un uso responsable y licito de la red desde cualquier medio tecnológico utilizado para el desarrollo de la prestación de sus servicios.
27. El acceso a Internet o a cualquier otra red de ordenadores se deberá realizar a través de las conexiones permitidas, habilitadas y configuradas por FIBHUG. Cualquier otra conexión diferente, pondrá en riesgo la seguridad de los sistemas de información de FIBHUG, y por ello, está terminantemente prohibida.
28. En relación a las conexiones remotas a la red de FIBHUG, solamente se realizarán a través de los medios destinados a tal fin, siendo éstos la única vía permitida de acceso, y siempre previa autorización expresa de FIBHUG. Todos los equipos que pretendan conectarse de forma remota a la red de FIBHUG, deberán tener implantados y correctamente actualizados los controles corporativos de detección, prevención y corrección de código malicioso o virus informático.
29. El quebrantamiento por parte de un empleado de cualquiera de las reglas contempladas en el presente Manual, o cualesquiera otros documentos circulados por FIBHUG, constituirá un incumplimiento por parte del empleado de sus obligaciones, ante lo cual FIBHUG está legitimado tanto para exigir al empleado que cese inmediatamente en sus actuaciones, como para adoptar cualquier otra medida que proceda, incluida la resolución del contrato por incumplimiento, de conformidad a lo establecido en la normativa interna de FIBHUG, así como en la legislación vigente.

El conocimiento, observancia y respeto del presente Manual es vinculante para todos los empleados y profesional externo contratado por FIBHUG, cuando de forma directa o indirecta, accedan o hagan uso de los medios tecnológicos facilitados por FIBHUG.