Cifrar información sanitaria

https://www.ibsalut.es/ibsalut/es/profesionales/seguridad-de-la-informacion/boletines-de-la-oficina-de-seguridad/3071-boletin-n-60-ano-2018

Profesionales. Seguridad de la información. Boletines de la Oficina de Seguridad. Boletín n. 60 año 2018

El correo electrónico es una herramienta indispensable en nuestro día a día y, como para toda herramienta corporativa, es necesario definir un uso correcto y seguro de la misma, ya que, además de abusos y errores no intencionados que puedan causar un perjuicio al Servicio de Salud, el correo electrónico se ha convertido en uno de los medios más utilizado por los ciberdelincuentes para llevar a cabo sus ciberataques.

De hecho, los mensajes de correo electrónico son transmitidos en ocasiones a través de redes públicas no seguras, donde pueden ser capturados, leídos e incluso modificados por terceros tal y como queda de manifiesto en el gráfico ilustrativo de abajo:

En este sentido, el uso adecuado de esta herramienta se ha desarrollado en un capítulo especial del *Código de Buenas Prácticas del Servicio de Salud para el uso de los sistemas de información y en el tratamiento de los datos de carácter personal*, que es de obligado cumplimiento para todos los usuarios de los sistemas de información del Servicio de Salud. Así mismo, tal como se indica en el Código de Buenas Prácticas, el correo electrónico también debe cumplir con las medidas de seguridad de la información de la legislación vigente en materia de protección de datos, así como el resto de leyes sanitarias que le son de aplicación.

Así pues, entre de todas las medidas de seguridad que se aplica al correo electrónico, en este boletín queremos recalcar la correcta protección de la información sensible que enviamos a través de correo electrónico, para evitar que información sensible pueda llegar a manos de terceros no autorizados.

¿Qué entendemos por información sensible y cómo debemos protegerla?

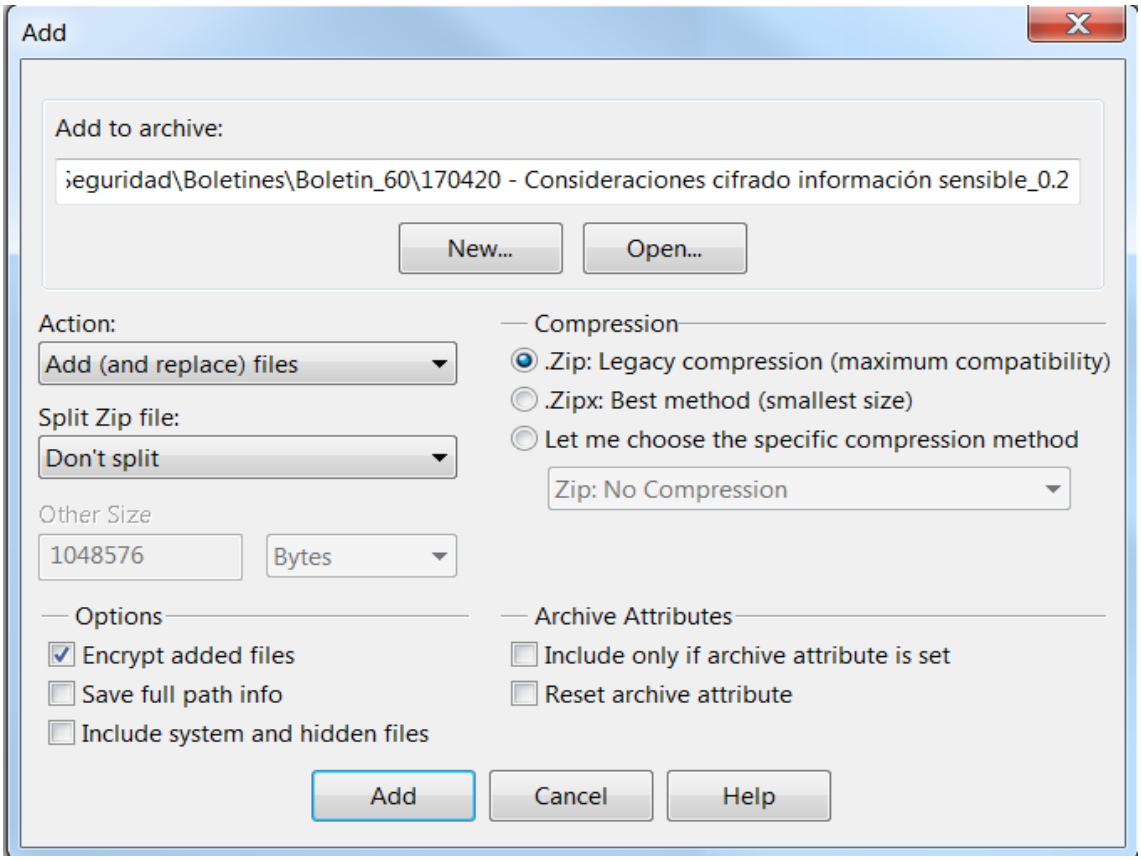
En el Servicio de Salud cuando hablamos de información sensible nos referimos a información de carácter personal con datos de salud de nuestros pacientes, así como a información derivada de actos de violencia de género, religión o creencias; es decir, información que manejamos frecuentemente en nuestra operativa diaria.

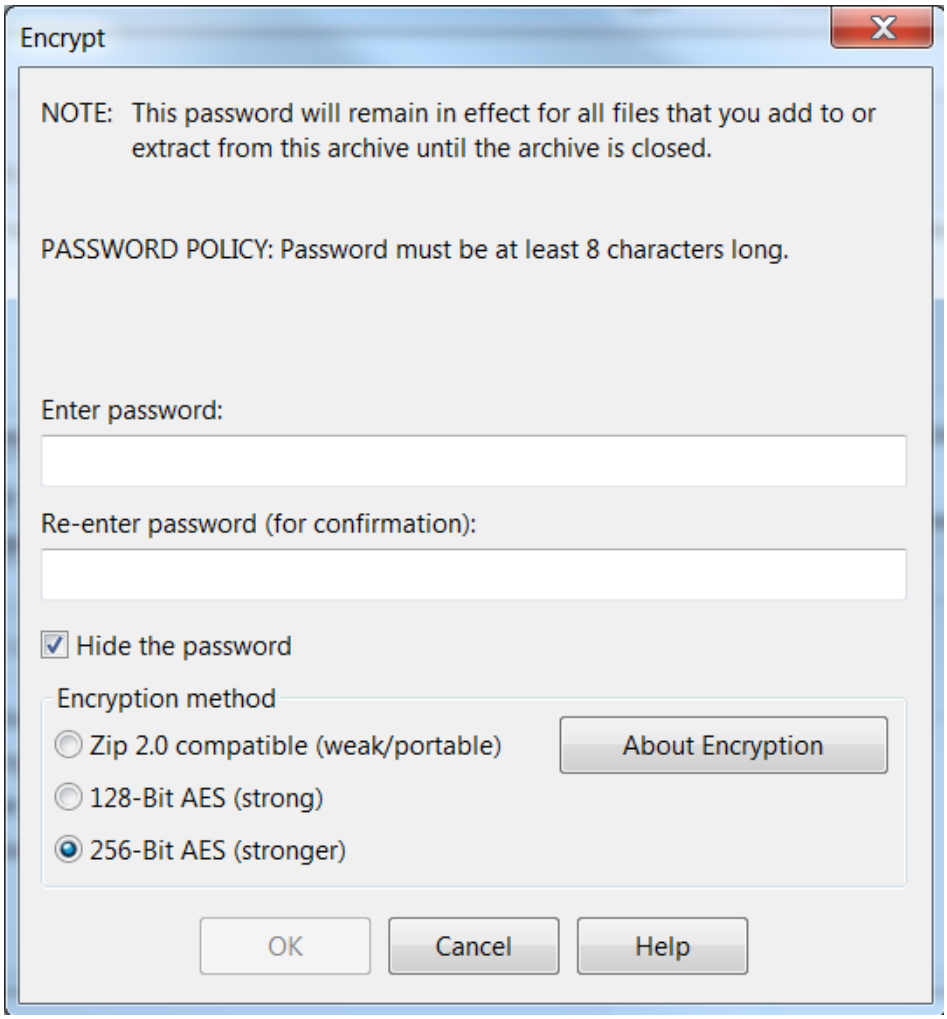
A la hora de manejar y tratar este tipo de información se deben aplicar medidas de seguridad más robustas y restrictivas de lo habitual, de modo que garanticen la integridad y confidencialidad y que cumplan con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de Abril de 2016, relativo a la protección de las personas físicas respecto al tratamiento de datos personales.

Con carácter general, **NO** debemos enviar información de carácter personal con datos de salud por medio del correo electrónico. Y en el supuesto de que sea estrictamente necesario hacer un envío de ese tipo, mediante la presente publicación queremos poner de manifiesto la necesidad de cifrar dichos correos o, en su defecto, cifrar el contenido de la información que se envía para garantizar un nivel de seguridad apropiado.

¿Cómo podemos cifrar la información?

El Servicio de Salud dispone de un paquete de programas ya instalado en todos los equipos que permite cifrar la información de manera segura. Estamos hablando de la aplicación **WinZip**, mediante la cual podremos cifrar la información utilizando una contraseña que cumpla la política del Servicio de Salud y un algoritmo de cifrado robusto (i.e. AES-256) que garantice la confidencialidad de los datos que se quieran enviar.


Add
Add to archive:
eguridad\Boletines\Boletin_60\170420 - Consideraciones cifrado información sensible_0.2
New...
Open...
Action:
Add (and replace) files
Split Zip file:
Don't split
Other Size
1048576
Bytes
Compression
.Zip: Legacy compression (maximum compatibility)
.Zipx: Best method (smallest size)
Let me choose the specific compression method
Zip: No Compression
Options
Encrypt added files
Save full path info
Include system and hidden files
Archive Attributes
Include only if archive attribute is set
Reset archive attribute
Add
Cancel
Help


Encrypt
NOTE: This password will remain in effect for all files that you add to or extract from this archive until the archive is closed.
PASSWORD POLICY: Password must be at least 8 characters long.
Enter password:
Re-enter password (for confirmation):
Hide the password
Encryption method
Zip 2.0 compatible (weak/portable)
About Encryption
128-Bit AES (strong)
256-Bit AES (stronger)
OK
Cancel
Help

La contraseña deberá ser notificada al destinatario telefónicamente o a través de otra vía que se considere segura (i.e. SMS) diferente a la utilizada para enviar la información, de modo que alguien que intercepte el correo no tenga conocimiento de la contraseña.

La distribución de información sensible requiere, además, haber recabado correctamente el consentimiento previo por parte del propietario de los datos.

Uso inadecuado del servicio de correo electrónico y posibles consecuencias

Nuestra obligación, como profesionales del Servicio de Salud, es proteger la información a la que tenemos acceso cumpliendo con las medidas de seguridad de la información y evitando que terceros no autorizados puedan acceder a ella. El tratamiento incorrecto o uso indebido de la información puede suponer sanciones económicas muy elevadas para el Servicio de Salud, así como un severo impacto en su reputación.

De hecho, a menudo podemos leer o escuchar noticias de ciberataques relacionados con centros de salud que han vulnerado la seguridad de los datos sensibles de sus pacientes, publicando o comercializando con dicha información de forma no autorizada, como consecuencia de no aplicar buenas prácticas de seguridad.

Así pues, a modo de recordatorio, a continuación se enumeran algunos ejemplos de malas prácticas de seguridad de la información que todos debemos intentar evitar:

- Propagar contenido de carácter racista, xenófobo, pornográfico, sexual, de apología del terrorismo o que atente contra los derechos humanos, que actúe en perjuicio de los derechos a la intimidad, el honor y la imagen propia o contra la dignidad de las personas.
- Divulgar información sensible sin la autorización previa correspondiente.
- Difundir mensajes de correo electrónico sin identificar plenamente al remitente. Si la cuenta de correo es usada por grupos de usuarios, hay que identificar al autor.
- Hacer circular cartas encadenadas y participar en esquemas piramidales o en actividades similares.
- Enviar masivamente mensajes o información que consuman injustificadamente recursos tecnológicos.
- Instalar o emplear servidores o servicios de correo que no tengan la autorización previa correspondiente.