Lo que se puede medir se puede mejorar

Brechas de seguridad

1.- ¿Qué es una brecha de seguridad?

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal (datos que hayan sido comprometidos o puedan ser comprometidos).

Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. **En general, una BRECHA DE SEGURIDAD, se trata de sucesos que ocasionan destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.**

Actualmente existe un reglamento que regula dicha situación. Este **Reglamento (UE) 2016/679 General de Protección de Datos**, establece en sus artículos 33 y 34 la obligación para las organizaciones (tanto privadas como públicas), que actúen como responsable del tratamiento, de notificar a la Autoridad de Control competente las brechas de seguridad que puedan ocasionar daños y perjuicios sobre las personas y, si esos daños son graves, comunicar la brecha a las personas cuyos datos se han visto afectados para que puedan tomar sus propias medidas.

2.- Brechas de seguridad en el hospital.

En el hospital a lo largo del presente año se han producido diferentes brechas de seguridad. A continuación queremos ejemplificar algunos casos concretos para trasladaros a todos (tanto personal asistencial como no asistencial) la importancia de cuidar y asegurar la privacidad de los datos de nuestros pacientes (no solo los concernientes a la Historia Clinica, también, todos aquellos documentos, en uno u otro formato, que manejamos de manera diaria y que contienen información de la medicación de nuestros pacientes, la habitación que ocupan, la consulta que tienen citada, etc, es decir, datos de carácter personal que no deben llegar a terceros y que no podemos dejar a la vista de terceras personas, ya que son datos sensibles y privados que tenemos la obligación de custodiar y/o destruir siguiendo los circuitos establecidos, una vez utilizados.

I. **Ejemplo de Brecha de Seguridad en Quirófano**. La brecha de seguridad se produjo cuando una vez finalizadas las intervenciones a las que fueron sometidos ambos pacientes y antes de que estos abandonasen el hospital se les entregó:

o Paciente A, informe de alta y pruebas preoperatorias del paciente B.
o Paciente B, informe de alta.

Al día siguiente de abandonar el hospital, el Paciente A se puso en contacto con el hospital vía telefónica para hacernos saber que tenía información de otro paciente que no era él. Ante esta situación, el hospital habló con el Paciente A para gestionar la recogida de las pruebas preoperatorias del Paciente B, ofreciendo como alternativas que trajese la documentación al hospital (a lo cual se negó) o que entregase ésta a un mensajero que el hospital enviaría específicamente a su casa para ello (a lo cual también se negó).

A día de hoy el Paciente A ha enviado en formato electrónico (email) la información del Paciente B, pero estamos pendientes de que nos pueda traer la documentación original una vez que acuda a una visita a las Consultas Externas del centro.

II. **Ejemplo de Brecha de Seguridad en Hospitalización**. La brecha de seguridad se produjo cuando al Paciente A, en el momento del alta se le entregó la Historia Clinica de otro paciente (Paciente B).

En este caso, un familiar del Paciente A, al que habíamos entregado la Historia Clínica del Paciente B, acudió al día siguiente del hecho al hospital y después de identificarse correctamente entregó en el servicio de Atención al Paciente la Historia Clínica del Paciente B, formulando 2 preguntas concretas:

o ¿Cómo es posible que se pudiese producir una situación de estas características? ¿Nadie comprueba la información que se entrega? ¿No existe verificación?
o ¿Si la información de su familiar (Paciente A) había sido entregada a otro paciente?

Además de preguntar, solicitaba que le fuese entregada la información de su familiar (Paciente A) para poder llevársela en el momento.

En este caso, la brecha de seguridad se pudo cerrar puesto que el servicio de Atención al Paciente contactó rápidamente con la planta de hospitalización correspondiente para poner en su conocimiento la situación y averiguar dónde se encontraba la información del Paciente A. Después de una rápida gestión de todas las áreas implicadas, se pudo comprobar que dicha información se encontraba en planta y se procedió a entregar la documentación correspondiente del Paciente A y recoger la información que se le había entregado incorrectamente del Paciente B.

3.- Cómo debemos proceder en caso de detectar una brecha de seguridad.

Las palabras que definen cómo debemos proceder cuando identificamos o nos comunican una brecha de seguridad son:

- **Comunicación**: poner en conocimiento de nuestros responsables el hecho para valorarlo y poner en marcha los mecanismos necesarios para su inmediata subsanación.
- **Rapidez**: es fundamental dar rápida respuesta a la brecha de seguridad, contactando con las partes implicadas.
- **Análisis y aprendizaje**: análisis concreto de los motivos o situación que ha generado la brecha de seguridad con el fin de poder establecer protocolos, circuitos de mejora que nos permitan seguir mejorando.

Pero sin duda, las acciones más efectivas que podemos poner en marcha cada día, cada uno de nosotros son, en primer lugar, ser conscientes (más aun si cabe) de la sensibilidad y privacidad de la información que manejamos en el hospital. En segundo lugar, establecer acciones o comportamientos diarios orientados a garantizar y asegurar la privacidad de dicha información (comprobar/verificar que la documentación que entregamos es de y para el paciente correcto; y destrucción de información sensible una vez utilizada).