CODI TIPUS INFORMA **73/13**

RECOMANACIONS SOBRE EL REGISTRE D'ACCESSOS

El marc legal vigent requereix com a mesura de seguretat pel tractament de dades de nivell alt per fitxers i tractaments automatitzats disposar d'un registre d'accessos (veure article 103 del Reial decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desplegament de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal).

La finalitat de disposar un registre d'accessos és en tot cas preventiva amb l'objectiu de poder dur a terme una verificació dels accessos i si són o no els convenients.

És doncs en la seva verificació (revisió com disposa l'article 103.5 del RLOPD) on s'evidencia la dificultat de satisfer el requeriment legal, en aquest sentit exposem tot un seguit de recomanacions adreçades a assolir el compliment de la mesura de seguretat esmentada:

1. Accions i comunicats interns als professionals de l'entitat recordant que les bases de dades de nivell alt disposen d'un registre d'accessos i, a fi i efecte d'acomplir amb el marc normatiu de protecció de dades, els mateixos accessos seran revisats per veure si són o no corresponents, com per detectar incidències.

2. La verificació de tots els accessos resulta una tasca titànica i inassolible i per tant, s'aconsella procedir a la revisió d'una mostra d'accessos, aleatòria i periòdica. Aquesta mostra haurà de realitzar-se de forma mensual i el Responsable de Seguretat elaborarà un informe. Caldria implementar paràmetres en els sistemes d'informació que activessin certes alarmes davant d'accessos irregulars, que posteriorment s'haurien de revisar per si no són adequats a la normativa. Atès però que actualment són pocs els centres que disposen d'una automatització del registre d'accessos, caldria que es procedís manualment i es revisessin els accessos ocorreguts a un nombre d'HC, que no aconsellem que sigui inferior a 20 mensuals.

Alguns criteris que aconsellem per procedir a la selecció d'una part de les Històries Clíniques a revisar:

- Històries Clíniques de personal de l'entitat.
- Històries Clíniques de VIPs, persones notòries o amb rellevància en el territori.
- Històries clíniques de pacients que no hagin estat visitats en un període llarg de temps.
- Accessos efectuats per personal durant el període en què estava de vacances.
- Accessos efectuats per personal durant el període en què estava de baixa.

Existeixen altres opcions que poden ser d'utilitat i que certes organitzacions han adoptat, com ho poden ser per exemple oferir al personal la possibilitat de demanar revisar el registre d'accés a la seva HC.

3. De cada Història Clínica s'haurà d'extreure els accessos esdevinguts i aquests seran revisats i validats. Aquesta tasca recomanem que sigui d'àmbit mixt, en tant que l'extracció sol ser funció d'un perfil més tècnic (Responsable de Sistemes/Informàtica de l'entitat) i la seva revisió de l'àmbit clínico-assistencial i/o de Recursos Humans.

4. Si es detecten accessos no autoritzats sempre serà necessària la presència de l'afectat per justificar o no el que en principi és un accés no autoritzat. Amb tot, si l'accés esdevé com NO autoritzat, caldrà adoptar les mesures disciplinàries convenients d'acord amb allò que estableixi el conveni laboral d'aplicació i en funció de les circumstàncies concurrents a cada cas. El fins fa poc vigent Conveni de la XHUP (el règim disciplinari del qual ha estat assumit per moltes organitzacions del sector dintre dels pactes d'empresa generalment assolits els darrers dos mesos) preveu diversos "tipus" infractors que permetrien qualificar les conductes relacionades com a infracció lleu (article 65.1.e) menys greu (art. 65.2 a i c) greu (article 65.3.g) i molt greu (65.4.a en relació a l'article 54,d de l'Estatut dels Treballadors). Aquesta enumeració és simplement enunciativa i per tant, cal insistir que les circumstàncies del cas i la informació i advertiment previ sobre la improcedència dels accessos indeguts, seran elements determinants. Salvant la llibertat de cada organització en l'orientació de les seves polítiques de RRHH, sí que recomanem que en una primera fase de verificació d'accessos, i sempre que no hi hagin condicions en el cas que agreugin la gravetat del comportament, es tendeixi a aplicar la banda baixa del règim disciplinari laboral d'aplicació. Recordar finalment que determinats comportaments poden tenir rellevància penal i per tant, caldrà estar al cas concret per determinar la intensitat de l'actuació de l'empresa.

5. Per últim, esmentar que el mercat ofereix aïllar aquests registres d'accessos en servidors diferenciats i/o implementar alarmes que s'activin quan els registres d'accessos s'intentin modificar. A més, amb aquestes eines hi hauria capacitat d'utilitzar-les com a prova jurídica. Aquestes serien sens dubte, mesures de seguretat reforçades que mostrarien diligència addicional del responsable del fitxer.

Barcelona, 30 de setembre de 2013.