HÃ©bergement de donnÃ©es de santÃ© personnelles : Enjeu stratÃ©gique
Internet
PostÃ© par : JulieM
PubliÃ©e le : 28/4/2016 13:30:00

Les Ã©tablissements de santÃ© ont une mission de service public. Mais au-delÃ de la mission de santÃ© publique, ils endossent, de fait, aussi une mission de protection de leurs patients et en particulier de protection des donnÃ©es sensibles quâ□□ils collectent sur ceux-ci : les donnÃ©es de santÃ© Ã caractÃ¨re personnel.

Parce que lâ□□hÃ´pital est toujours plus numÃ©risÃ©, parce quâ□□il fait appel Ã toujours plus de prestataires externes, les risques existent : risque de perte des donnÃ©es, de fuite de donnÃ©es, de corruption de ces donnÃ©es. Câ□□est toute la confiance dans le secteur de la santÃ© qui est en jeu.

Lâ□□ASIP SantÃ©, agence crÃ©Ã©e en 2009 notamment pour accompagner lâ□□Ã©mergence de technologies numÃ©riques dans le secteur de la santÃ© tout en veillant au respect des droits des patients, a dÃ©fini le rÃ©fÃ©rentiel dâ□□agrÃ©ment des hÃ©bergeurs de donnÃ©es de santÃ© Ã caractÃ¨re personnel (HDS).

Ce rÃ©fÃ©rentiel organise le dÃ©pÃ´t et la conservation des donnÃ©es de santÃ© dans des conditions de nature Ã garantir leur pÃ©rennitÃ© et leur confidentialitÃ©, de les mettre Ã la disposition des personnes autorisÃ©es selon des modalitÃ©s dÃ©finies par contrat, et de les restituer en fin de contrat. Cet hÃ©bergement ne peut avoir lieu qu'avec le consentement exprÃ¨s de la personne concernÃ©e.

Il est donc essentiel pour les candidats Ã lâ□□agrÃ©ment de lâ□□ASIP SantÃ© â□□ dÃ©livrÃ© pour une durÃ©e de 3 ans renouvelable â□□ de clarifier ses exigences et dâ□□identifier les solutions de cyber-sÃ©curitÃ© des donnÃ©es aptes Ã contribuer Ã leur conformitÃ© rÃ©glementaire. Les hÃ©bergeurs doivent donc se conformer Ã de nombreuses exigences et mettre en Å□uvre une sÃ©rie dâ□□actions pour pouvoir obtenir leur agrÃ©ment afin dâ□□hÃ©berger des donnÃ©es de santÃ© Ã caractÃ¨re personnel.

Bien sur, si un Ã©tablissement hÃ©berge lui-mÃªme ses dossiers hospitaliers, il nâ□□a pas besoin dâ□□obtenir un agrÃ©ment. En revanche, si lâ□□Ã©tablissement met son systÃ¨me dâ□□hÃ©bergement au service dâ□□autres Ã©tablissements de santÃ©, il est soumis Ã la procÃ©dure dâ□□agrÃ©ment. Il en est de mÃªme pour les Ã©tablissements de coopÃ©ration sanitaire (groupements de coopÃ©ration sanitaire â□□ GCS -, communautÃ©s hospitaliÃ¨res ...) qui mettent Ã disposition de leurs membres leur systÃ¨me dâ□□hÃ©bergement : ils sont soumis Ã cette procÃ©dure dâ□□agrÃ©ment.

Attention aux aspects liÃ©s Ã la sÃ©curitÃ©

Dans ce contexte, il est nÃ©cessaire de bien penser Ã gÃ©rer le contrÃ´le des accÃ¨s et la traÃ§abilitÃ© des utilisateurs Ã privilÃ¨ges.

Nous pouvons prendre par exemples, la gestion des mots de passe, le contrÃ´le et de traÃ§abilitÃ© des accÃ¨s des prestataires externes, des administrateurs internes Ã lâ□□entreprise et des super-utilisateurs. Cela permet Ã©galement dâ□□enregistrer les sessions dâ□□administration et de les visionner ultÃ©rieurement en cas de besoin (audit, incident,...).

Enfin, les responsables de la sÃ©curitÃ© du systÃ¨me dâ□□information et hÃ©bergeurs peuvent

gÃ©rer facilement le turn-over de leurs Ã©quipes, sans craindre de laisser lâ□□accÃ¨s aux donnÃ©es hÃ©bergÃ©es

Parce quâ□□elle permet de mettre en place une vÃ©ritable politique de sÃ©curitÃ© rÃ©pondant aux exigences technologiques et lÃ©gales, lâ□□approche Â« Privileged Access Management Â» est donc Ã©galement Ã intÃ©grer dans les projets dâ□□hÃ©bergement des donnÃ©es de santÃ© Ã caractÃ¨re personnel. Il ressort donc de lâ□□ensemble de ces Ã©lÃ©ments quâ□□hÃ©berger des donnÃ©es de santÃ© Ã caractÃ¨re personnel nÃ©cessite de mettre en place des dispositifs industriels associant technologies, approche mÃ©tier et contraintes lÃ©gales.