Bitdefender®

Conformité avec l'HIPAA : ce qu'il faut savoir sur la sécurité des environnements virtuels et cloud

Bitdefender®

Guide de conformité avec l'HIPAA pour la sécurité de la virtualisation et du cloud : check-list

- **Fonctionne avec toute plate-forme de virtualisation** – pas de dépendance à l'égard d'un fournisseur de virtualisation
- Propose un **contrôle centralisé des postes de travail et serveurs physiques, virtuels et mobiles** - supprime la gestion de différentes solutions dédiées
- Permet une adoption **contrôlée** du BYOD
- Offre une **protection** contre les malwares et maintien de l'intégrité des données médicales sensibles avec une protection antivirus, antimalware et Web
- Conformité **PCI -** DSS

En résumé

Peu de réglementations gouvernementales ou liées à un secteur d'activité ont suscité autant d'intérêt ces dernières années que le Health Insurance Portability and Accountability Act (HIPAA).

Cette loi a eu un impact considérable dans le domaine de la santé et d'autres secteurs apparentés, de même que sur les patients, depuis qu'elle a été votée par le Congrès des États-Unis en 1996. L'HIPAA continuera assurément à affecter les entreprises et les patients pendant de nombreuses années.

L'HIPAA présente des exigences détaillées en matière de protection et de confidentialité des données des patients et a modifié la façon dont les services de santé, les assurances, le secteur des sciences de la vie et d'autres entreprises considèrent et règlent les problèmes de sécurité et de confidentialité.

Du point de vue technologique, l'HIPAA touche un grand nombre de domaines dont les sites web, les appareils médicaux, les dossiers médicaux électroniques et l'imagerie médicale.

Un certain nombre de tendances technologiques récentes, dont le succès de la virtualisation, du cloud computing, des appareils et des applications mobiles ont généré de nouveaux problèmes et défis pour les organismes payeurs et fournisseurs de services de santé devant respecter l'HIPAA.

Des solutions peuvent aider les entreprises à respecter les exigences de l'HIPAA ainsi qu'à améliorer leur situation globale en matière de sécurité et de gestion des risques. Ces solutions fournissent une protection efficace contre les menaces dans les locaux des clients, dans les environnements virtualisés et sur les appareils mobiles.

Ce document propose un aperçu de l'HIPAA et des défis que pose cette loi aux services de santé et à d'autres secteurs qui y sont liés. Il comporte un résumé de son impact sur un certain nombre de secteurs technologiques, ainsi que sur la façon dont des tendances telles que le cloud et la mobilité peuvent affecter les efforts de mise en conformité. Ce rapport décrit également comment les solutions actuelles peuvent accompagner les entreprises dans leurs efforts pour être conformes avec l'HIPAA, aujourd'hui et demain.

Bitdefender®

HIPAA — Présentation et Description

La loi HIPAA a été adoptée par le gouvernement fédéral américain en 1996 afin d'améliorer la portabilité et continuité de la couverture d'assurance maladie dans les marchés de l'assurance individuelle et collective. Les objectifs de cette loi étaient également, entre autres, de lutter contre le gaspillage, la fraude et les abus dans l'assurance maladie et la prestation de services de santé, d'améliorer l'accès aux services de soins de longue durée et leur couverture et de simplifier la gestion des assurances.

Les deux éléments-clés de l'HIPAA sont les suivants : 1) l'HIPAA Privacy Rule (la règle de protection de la vie privée) et 2) l'HIPAA Security Rule (la règle de sécurité). La Privacy Rule, garantie par le Bureau des Droits Civils (OCR) du département américain de la Santé et des Services sociaux (HHS) assure une protection fédérale des données médicales permettant d'identifier personnellement leurs propriétaires, détenues par des organismes soumis à l'HIPAA et leurs associés commerciaux.

Cette règle accorde aux patients un ensemble de droits concernant leurs données confidentielles quel que soit le support de stockage de celles-ci et définit un ensemble de normes nationales pour l'utilisation et la divulgation de données médicales protégées (PHI, Protected Health Information) par les organismes. Ces informations comprennent tout traitement ou problème actuel ou antérieur ainsi que des identifiants courants comme le nom, l'adresse et la date de naissance.

L'un des principaux objectifs de la règle de la vie privée est d'assurer la protection des données médicales des patients tout en permettant la transmission des informations médicales nécessaires pour fournir des soins médicaux de qualité. Cela constitue un compromis autorisant les utilisations indispensables des informations tout en protégeant également la vie privée des patients.

La Privacy Rule s'applique aux assurances de santé individuelles et collectives, aux organismes de centralisation des données du secteur de la santé et à tout prestataire de soins de santé comme les hôpitaux ou les cabinets de médecins transmettant des informations médicales au format électronique relatives à des transactions telles que des indemnisations, demandes d'admissibilité à des prestations, demandes d'autorisation de transfert vers un autre professionnel de la santé, ou d'autres transactions pour lesquelles le département américain de la Santé et des Services sociaux a établi des normes.

Cette réglementation s'applique également aux « associés commerciaux » qui comprennent les individus ou les entreprises réalisant certaines fonctions ou activités au nom d'une entreprise soumise à ces dispositions, ou fournissant certains services à cette entreprise, impliquant l'utilisation ou la divulgation de données médicales permettant d'identifier individuellement des patients. Cela peut comprendre des fonctions telles que le traitement des demandes d'indemnisation, l'analyse de données, le consulting, l'agrégation de données et la facturation.

Lorsqu'une entreprise régie par l'HIPAA a recours aux services d'un travailleur indépendant ou d'une autre personne ne faisant pas partie de son personnel, la Privacy Rule requiert que l'entreprise stipule des mesures de protection des données des patients dans un accord de partenariat commercial. Celui-ci doit spécifier par écrit des mesures de protection précises pour les informations médicales identifiables de façon individuelle utilisées ou divulguées par les associés commerciaux.

Les entreprises régies par la Privacy Rule de l'HIPAA doivent respecter un large éventail d'obligations administratives dont :

- L'élaboration et la mise en place de politiques et procédures écrites de protection de la vie privée
- La désignation d'un responsable officiel chargé d'élaborer et de mettre en place leurs politiques de protection de la vie privée
- La formation des employés aux politiques et procédures de protection de la vie privée
- Le maintien de mesures de protection administratives, techniques et physiques appropriées afin d'empêcher la divulgation intentionnelle ou non de données médicales protégées

De plus, les entreprises doivent conserver certains dossiers liés à la Privacy Rule six ans après leur création.

La Security Rule, également mise en œuvre par l'OCR, définit des normes nationales pour la sécurité des données médicales électroniques. Cette règle spécifie un ensemble de mesures de protection administratives, physiques et techniques pour les entreprises et leurs associés commerciaux à utiliser pour assurer la confidentialité, l'intégrité et la disponibilité des données médicales sensibles.

La Security Rule consiste principalement en une « mise en application » des mesures de protection présentées dans la Privacy Rule respectant les mesures de protection, techniques et non techniques, que les entreprises doivent mettre en place afin de protéger les informations médicales des individus, selon l'HHS. Elle incite également à maintenir l'intégrité et la disponibilité des données médicales sensibles. L'« intégrité » signifie ici que ces données ne peuvent être modifiées ni détruites sans autorisation et la « disponibilité » que ces données sont accessibles et peuvent être utilisées sur demande par une personne autorisée.

Les mesures de protection administratives de la Security Rule requièrent que les entreprises intègrent une analyse des risques à leurs processus de gestion de sécurité. Cela comprend l'évaluation de la probabilité et de l'impact des risques potentiels affectant les données PHI électroniques, la mise en place de mesures de sécurité appropriées pour faire face aux risques identifiés dans l'analyse des risques, la description des mesures de sécurité choisies et le maintien continuel de mesures de sécurité raisonnables et adaptées.

L'analyse des risques doit être un processus continu au cours duquel une entreprise examine régulièrement ses fichiers pour surveiller l'accès aux données médicales électroniques protégées et détecter des incidents de sécurité, évalue régulièrement l'efficacité des mesures de sécurité en place et réévalue régulièrement les risques menaçant ces données.

Les entreprises régies par l'HIPAA doivent également désigner un responsable officiel chargé de concevoir et de mettre en place des politiques et procédures de sécurité, d'implémenter des politiques et des procédures pour autoriser l'accès aux données médicales sensibles et de former l'ensemble des employés en matière de politiques et procédures de sécurité.

Selon le département américain de la Santé et des Services sociaux (HHS) il n'existait pas avant l'HIPAA de normes de sécurité reconnues en matière d'exigences générales pour la protection des informations médicales. Le besoin d'une meilleure sécurité est apparu lorsque le secteur de la santé a délaissé le papier pour recourir de plus en plus à des systèmes électroniques pour verser des indemnités, répondre à des questions relatives à

l'admissibilité, fournir des informations médicales et effectuer d'autres tâches administratives et cliniques.

Un objectif clé de la Security Rule est de protéger la vie privée des informations médicales des individus, tout en autorisant les entreprises à adopter de nouvelles technologies afin d'améliorer la qualité et l'efficacité des soins dispensés aux patients. Ce règlement s'applique aux assurances de santé, aux organismes de centralisation des données et à tout professionnel de la santé transmettant des informations médicales au format électronique relatives à une transaction.

Les entreprises qui ne respectent pas les règles de l'HIPAA encourent des sanctions financières de plus de 50 000 dollars (environ 40 000 euros) par violation de données et peuvent même faire l'objet de poursuites pénales pour certaines violations.

Cependant, les dommages ne se limitent pas forcément aux amendes. La réputation des entreprises ne respectant pas les règles de l'HIPAA peut également être entachée.

Outre l'HIPAA, les entreprises du domaine de la santé et des secteurs connexes doivent respecter la loi HITECH (Health Information Technology for Economic and Clinical Health), qui a modifié et renforcé certaines obligations de l'HIPAA. L'HITECH fait partie du Plan de relance économique des États-Unis de 2009, et est destinée à promouvoir l'adoption et la bonne utilisation de la technologie de l'information dans le domaine de la santé.

La section D de la Loi HITECH règle les problèmes en matière de confidentialité et de sécurité liés à la transmission électronique des données médicales via différentes clauses qui renforcent l'application sur le plan civil et pénal des règles de l'HIPAA.

La loi HITECH requiert que les entreprises soumises à l'HIPAA signalent toute violation de données affectant 500 personnes ou plus au département américain de la Santé et des Services sociaux (HHS) et aux médias, en plus de l'envoi d'une notification aux personnes concernées.

L'impact considérable de ces réglementations

Les obligations stipulées par l'HIPAA/HITECH en matière de confidentialité et de sécurité touchent différents domaines technologiques au sein des entreprises de santé, dont les sites web, les appareils médicaux, les dossiers médicaux électroniques et les systèmes d'archivage et de transmission d'images (PACS). Vous trouverez ci-dessous une brève description des implications de la réglementation dans chacun de ces domaines.

Les sites web. Les entreprises doivent veiller à protéger les données médicales sensibles (PHI) et à les rendre accessibles uniquement par les utilisateurs autorisés. Cela signifie que ces informations doivent être cryptées lorsqu'elles sont transmises sur Internet, stockées ou archivées. Les entreprises doivent également pouvoir sauvegarder efficacement les données afin de les récupérer facilement en cas de besoin. L'accès aux données PHI doit être protégé des utilisateurs non autorisés via des contrôles d'accès efficaces et les entreprises doivent éviter que les données ne soient modifiées en ligne. Enfin, les entreprises doivent également s'assurer que les données sensibles se trouvant sur les serveurs Web de leurs associés commerciaux sont correctement protégées.

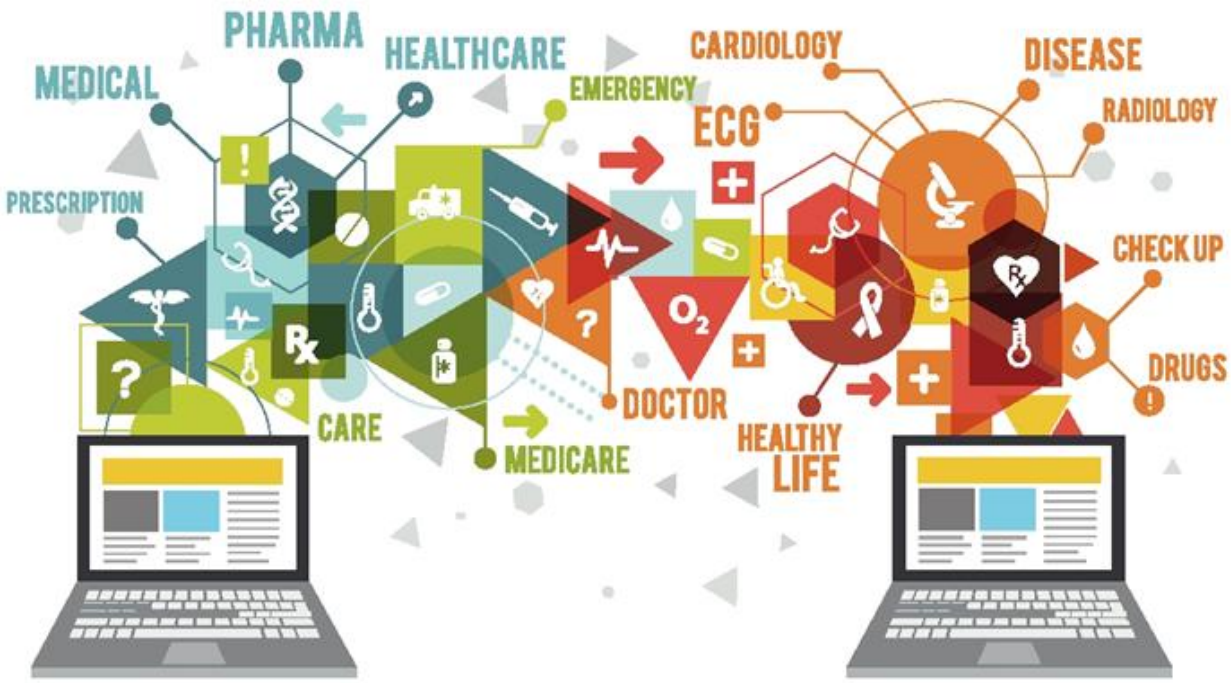
Les appareils médicaux. Les dispositifs utilisés pour différents diagnostics et traitements médicaux peuvent gérer des données de plus en plus nombreuses, de sorte qu'ils sont capables d'enregistrer de nombreuses informations sur l'utilisation d'un appareil médical ainsi que sur les problèmes et les traitements des patients. Certains appareils médicaux peuvent stocker des informations médicales confidentielles sur les patients et les transmettre à d'autres appareils via des dossiers médicaux électroniques. Des organismes comme des hôpitaux et des cliniques doivent veiller à ce que ces appareils soient protégés et conformes aux réglementations HIPAA et HITECH. La sécurité constitue un défi particulier dans le cas des appareils médicaux mobiles, qui peuvent être perdus ou dérobés plus facilement.

Les dossiers médicaux personnels. Le papier est progressivement remplacé car les organismes conservent les dossiers des patients au format électronique. L'apparition des dossiers médicaux électroniques a considérablement changé la façon dont les prestataires de soins accèdent aux données et utilisent des informations pour traiter leurs patients, et peut permettre de réaliser d'importantes économies et d'améliorer la productivité par rapport aux dossiers papier. Les dossiers électroniques sont souvent partagés entre différents organismes de soins et professionnels via des réseaux, et on y accède facilement via des appareils mobiles comme des smartphones ou de tablettes. Les dossiers médicaux électroniques couvrent de nombreuses données : les antécédents médicaux, médicaments et autres traitements, vaccinations, résultats d'analyses médicales, images radiologiques, signes vitaux et toutes sortes de données confidentielles sur les patients. Les dossiers médicaux faisant l'objet de menaces de sécurité telles que l'accès non autorisé, le piratage, le vol ou la perte, les entreprises doivent veiller à la sécurité et à la confidentialité de ces dossiers médicaux électroniques, comme le stipulent l'HIPAA et l'HITECH.

Les systèmes d'archivage et de transmission d'images (PACS). La technologie d'imagerie médicale telle que les systèmes PACS permettent de stocker et d'accéder facilement aux images de différentes sources comme les radiographies, les échographies et IRM (imageries par résonnance magnétique). Les images et comptes-rendus électroniques sont transmis au format numérique via les systèmes PACS, ce qui évite aux professionnels de la santé d'avoir à classer, retrouver manuellement et transporter les clichés. Les données autres que les images comme des documents scannés peuvent également être incluses dans les systèmes PACS. Ces systèmes comprennent des composants comme un système d'imagerie, un réseau pour transmettre des informations, des postes de travail pour interpréter et visualiser les images et des archives pour stocker et retrouver des images et des rapports. L'HIPAA nécessite que des copies de sauvegarde des images des patients soient effectuées en cas de perte. Et ces considérations en matière de sécurité et de confidentialité qui s'appliquent aux appareils médicaux et aux données médicales électroniques s'appliquent également aux PACS.

Les facteurs et tendances affectant les normes HIPAA et HITECH

Un certain nombre de tendances majeures de l'informatique ont un impact sur la capacité des entreprises à respecter les normes de l'HIPAA. Certaines existent depuis quelque temps mais continuent à progresser. D'autres sont devenues des tendances importantes dans les entreprises ces dernières années seulement. Quoi qu'il en soit, elles sont toutes susceptibles d'affecter l'approche par laquelle les entreprises font face aux problèmes de conformité avec l'HIPAA.



La virtualisation est une tendance technologique qui a déjà fait une grande percée dans les stratégies informatiques des entreprises. D'innombrables entreprises ont déployé des machines virtuelles dans leurs datacenters dans le but de réduire leur nombre de serveurs physiques, énergivores et moins agiles, et beaucoup commencent à adopter également la virtualisation des postes de travail.

La technologie de la virtualisation présente des caractéristiques dont la sécurité traditionnelle et les mesures de conformité ne tiennent pas compte, et les entreprises doivent s'assurer que leurs environnements virtuels disposent de mesures pour protéger les données médicales sensibles (PHI). Cela implique de s'assurer que tous les employés et partenaires commerciaux disposent d'un accès adapté aux données PHI, de mettre en place des contrôles d'accès efficaces, de surveiller l'activité liée à l'utilisation de ces données, et d'appliquer des politiques et des procédures afin de protéger les données sensibles contre les violations de sécurité et de confidentialité.

Le cloud computing est étroitement lié à la virtualisation et se fait également une place dans les entreprises. Les services cloud, qu'ils soient proposés dans des cloud privés, publics ou hybrides modifient considérablement la façon dont les entreprises consomment des services informatiques et les fournissent aux utilisateurs finaux.

Les avantages potentiels du cloud sont évidents : des coûts réduits, une plus grande agilité et une extensibilité facilitée, pour n'en citer que quelques-uns. Mais le cloud présente également des défis du point de vue de la conformité à l'HIPAA. Cela est particulièrement vrai dans le cas des clouds publics et hybrides, lorsque des données sont conservées dans des datacenters utilisés par de nombreux clients d'un service cloud. L'une des principales questions et préoccupations est la conformité à l'HIPAA des fournisseurs d'hébergement. Même si un fournisseur de service conserve les données dans son propre datacenter et est responsable de leur sécurité et confidentialité, les institutions médicales doivent s'assurer que les données PHI sont protégées comme le requiert l'HIPAA.

Toute entreprise utilisant un fournisseur cloud devrait vérifier que celui-ci a fait l'objet d'un audit indépendant et que ses employés sont formés aux exigences en matière de sécurité et de confidentialité des données PHI. Les fournisseurs d'hébergement devraient avoir des politiques et procédures écrites et être disposés à conclure un accord de partenariat (BAA, ou Business Associate Agreement), un accord entre une entreprise soumise à l'HIPAA et un partenaire commercial comme un hébergeur.

Ce type d'accord de partenariat, conformément aux directives de l'HIPAA, protège les données PHI et garantit qu'un fournisseur de services cloud utilisera le cryptage pour toutes ses données stockées sur ses serveurs ou transmises. L'HITECH spécifie que la gestion des données PHI par un partenaire commercial doit respecter les règles HIPAA de protection de la sécurité et de la confidentialité des données. Cet accord devrait indiquer clairement comment le fournisseur de services cloud rendra compte et réagira en cas de violation de données.

En plus de la virtualisation et du cloud computing, une autre tendance majeure de l'IT est la progression rapide des appareils et applications mobiles dans les environnements professionnels. L'augmentation du nombre d'appareils, due en grande partie aux programmes de « Bring Your Own Device » (BYOD) a compliqué la gestion des environnements mobiles pour les entreprises.

Du point de vue de la conformité à l'HIPAA, les entreprises doivent veiller à ce que les données PHI se trouvant sur les appareils mobiles sont sûres. De nombreux médecins, infirmières, techniciens et autres professionnels de la santé, ainsi que les bénéficiaires d'assurance maladie, utilisent des appareils portables comme des smartphones et des tablettes dans leur travail au quotidien.

Les entreprises peuvent adopter un certain nombre de mesures pour protéger la sécurité et la confidentialité des données PHI sur les appareils mobiles comme utiliser des mots de passe, des numéros d'identification personnels ou d'autres formes d'authentification des utilisateurs, recourir au cryptage afin de protéger les informations médicales stockées *sur* et envoyées *par* les appareils mobiles, supprimer les données à distance pour les appareils mobiles ayant été perdus ou volés, installer des pare-feux personnels sur les appareils mobiles afin de les protéger contre les connexions non autorisées, déployer des logiciels sur les appareils pour fournir une protection contre les applications malveillantes, les virus, les spywares et autres attaques basées sur des malwares et élaborer une politique complète avec des consignes pour l'utilisation sécurisée des appareils mobiles.

Un défi supplémentaire : celui de la conformité PCI

L'HIPAA et l'HITECH sont loin d'être les seules réglementations que les entreprises du domaine de la santé et leurs partenaires commerciaux doivent connaître et respecter.

La norme en matière de sécurité des données de PCI (PCI DSS 3.0) est une norme de sécurité propriétaire pour les entreprises gérant des données de titulaires de cartes de paiement pour les principales cartes de crédit, de débit et autres. Créée par le Conseil des normes de sécurité PCI, la norme est conçue pour renforcer les contrôles relatifs aux données des détenteurs de cartes afin de réduire les fraudes liées aux cartes de paiement (voir le document Bitdefender : *Conformité à la norme PCI DSS V 3.0*).

La norme PCI spécifie comment les entreprises doivent garantir la sécurité des données des titulaires de cartes de paiement qui sont stockées, traitées ou transmises par des commerçants ou d'autres organismes. Elle exige que les entreprises conçoivent et assurent la maintenance d'un réseau sécurisé en fournissant un antimalware aux postes de travail et serveurs, en installant et en assurant la maintenance d'un pare-feu afin de protéger les données des titulaires de cartes de paiement, en assurant la maintenance d'un programme de gestion des vulnérabilités à l'aide de logiciels ou programmes antivirus régulièrement mis à jour et en adoptant des mesures efficaces de contrôle des accès.

La dernière version (3.0) de la norme PCI, publiée en 2013, comprend les 12 exigences spécifiques suivantes :

- Installer et maintenir une configuration de pare-feu apte à protéger les données des titulaires de cartes
- Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur
- Protéger les données stockées des titulaires de cartes
- Crypter la transmission des données des titulaires de cartes sur les réseaux publics ouverts
- Utiliser des logiciels antivirus et les mettre à jour régulièrement
- Développer et gérer des systèmes et des applications sécurisés
- Restreindre l'accès aux données des titulaires de cartes aux seuls individus qui doivent les connaître
- Affecter un ID unique à chaque utilisateur d'ordinateur
- Restreindre l'accès physique aux données des titulaires de cartes
- Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes
- Tester régulièrement les processus et les systèmes de sécurité
- Gérer une politique de sécurité des informations

La norme PCI est un problème supplémentaire que les fournisseurs de services de santé doivent prendre en compte, avec l'HIPAA/HITECH et l'obligation gouvernementale d'utiliser un système de dossier médical personnel. Toute entreprise du domaine de la santé acceptant les paiements par carte doit obligatoirement respecter la norme PCI. Cela s'applique aux honoraires de services médicaux, aux primes d'assurances médicales et aux achats dans les boutiques des hôpitaux.

De nombreuses entreprises soumises à l'HIPAA/HITECH acceptent également les cartes de paiement, il est donc primordial de déployer une stratégie de sécurité des informations respectant les obligations de toutes ces réglementations.

Des solutions pour contribuer à la conformité dans les environnements virtuels et cloud

Il est peu probable qu'une solution de technologie unique réponde à l'ensemble des exigences en matière de conformité HIPAA/HITECH. Mais des outils permettent d'aider les entreprises à suivre et se conformer à certaines directives légales sur la sécurité et la protection de la vie privée.

Les parties prenantes devraient rechercher une solution de sécurité basée sur une appliance virtuelle offrant de la sécurité aux postes de travail et serveurs physiques, virtualisés et mobiles.

La solution doit protéger les postes de travail et les serveurs contre les attaques, y compris les malwares, sans entraver les performances des appareils clients. La solution devrait évoluer facilement à l'aide de l'architecture de son environnement virtuel et fonctionner sur toute plateforme de virtualisation, accélérant ainsi le processus de déploiement.

En regroupant le contrôle de la sécurité des postes de travail et serveurs physiques, virtualisés et mobiles via une console d'administration unique, les activités peuvent être simplifiées, en évitant les solutions dédiées à chaque environnement. Le déploiement et la gestion de la protection des postes de travail et serveurs physiques, virtualisés et mobiles devraient être simplifiés via l'intégration à des services essentiels de la virtualisation et de la gestion des répertoires.

La solution devrait satisfaire certaines exigences essentielles des normes HIPAA/HITECH et PCI, avec un pare-feu complet, bidirectionnel, la détection d'intrusion, l'antiphishing, le filtrage web, le contrôle utilisateur et web pour empêcher que des menaces de plus en plus diverses n'infectent les serveurs et les systèmes des utilisateurs finaux.

La solution devrait permettre l'adoption contrôlée des politiques de Bring Your Own Device (BYOD) en appliquant la sécurité uniformément sur tous les appareils des utilisateurs finaux. Les appareils mobiles peuvent ainsi être contrôlés et les informations professionnelles confidentielles qu'ils contiennent sont protégées. Cela est essentiel dans le secteur de la santé, où les prestataires de soins utilisent de plus en plus d'appareils mobiles comme les smartphones et les tablettes.

Enfin, la solution devrait satisfaire aux exigences de l'HIPAA pour assurer une protection contre les malwares et maintenir l'intégrité des données médicales sensibles (PHI) via une protection antivirus, antimalware et Web. Cela permet aux entreprises de respecter la norme en permettant le déploiement et la mise en œuvre de politiques de sécurité au sein de l'entreprise, ainsi que la détection, la surveillance et la correction des incidents de sécurité.

Étant donné l'importance de la sécurité des données, qui va au-delà des exigences de conformité, les entreprises doivent développer une stratégie de sécurité complète et fiable. Ces outils sont essentiels à cette politique.

Conclusion : Prendre ces réglementations à la légère présente des risques

Pour les entreprises du secteur de la santé et toutes celles soumises aux règles de l'HIPAA et de l'HITECH, la conformité avec ces réglementations ne peut pas être considérée comme un « bonus ». C'est un élément important sur le marché actuel de la santé.

Comme nous l'avons déjà signalé, les entreprises s'exposent à d'importantes sanctions financières en cas de non-respect de ces réglementations, ce à quoi il faut ajouter le coût de la correction de la vulnérabilité de sécurité ayant entraîné la faille. Pour de nombreuses entreprises du secteur de la santé, en particulier les plus petites, ce type de coûts peut être dévastateur.

Au-delà des conséquences financières, les entreprises qui ne respectent pas ces réglementations s'exposent à un retour de bâton dans le domaine des relations publiques et à d'éventuelles conséquences sur la réputation de leur entreprise. Aucune société ne souhaite être perçue comme étant non conforme ou négligente en matière de sécurité des données.

Étant donné l'impact considérable de ces réglementations sur différents aspects de l'informatique et les défis que posent des technologies comme le cloud, les appareils mobiles, les médias sociaux et le big data/ l'analytique, la mise en conformité doit être une priorité.

Les cadres des secteurs de l'informatique, de la sécurité et de la gestion des risques travaillant dans des sociétés soumises à l'HIPAA et à d'autres réglementations applicables doivent comprendre clairement ces règles, connaître les solutions existantes et adopter une approche proactive pour être conformes à celles-ci.