La gestion juridique des données de santé en termes de partenariat entre les hôpitaux et les services de solutions digitales de suivi médical : une analyse comparée du droit européen et du droit fédéral américain

Carte de visite

Rédigé par Tiphaine Charlotte DUMONT

Enseignant référent : Monsieur Nicolas COURTIER

Remerciement

A Maître Nicolas Courtier, Avocat au barreau de Marseille, pour avoir accepté de diriger cette carte de visite, qui clôture mes années d'études universitaires au sein de la Faculté de droit et de sciences politiques d'Aix-en -Provence. Je le remercie pour sa bienveillance, son accompagnement, sa disponibilité, ses précieux conseils, ainsi que pour la qualité de son enseignement tout au long de l'année.

A Madame Valérie-Laure Benabou, Professeur agrégée et Directrice du Master 2 PINTA, pour m'avoir accueilli au sein dans son master, pour ses conseils et enseignements, sa bienveillance et sa générosité.

A ma famille, pour leur soutien et joie de vivre illimitée.

A mes amis et camarades, pour tout ce qu'ils m'ont apporté.

SOMMAIRE

Abréviation

CEPD : Comité européen de la protection des données

CLOUD Act : Loi sur la clarification de l'utilisation légale des données à l'étranger ou Clarifying Lawful Overseas Use of Data Act

CMS : Centers for Medicare & Medicaid Services

CNIL : Commission nationale de l'informatique et libertés

CSP : fournisseur de services dans les nuages

DoT : Ministère américain des transports ou pour U.S Department of Transportation

DPD ou DPO : Délégué à la protection des données ou Data protection officer

GAFAM : Google, Apple, Facebook, Amazon et Microsoft

GINA : loi sur la non-discrimination en matière d'information génétique ou Genetic Information Non-discrimination Act

FDA : Administration des aliments et des médicaments

FTC : Commission fédérale du commerce des États-Unis

e-PHI ou PHI : informations de santé protégées ou electronic protected health information

United States : États-Unis

UE : Union européenne

HIPPA : Loi sur la portabilité et la responsabilité de l'assurance maladie ou Health Insurance Portability and Accountability Act

HITECH : loi sur les technologies de l'information en matière de santé pour la santé économique et clinique ou Health Information Technology for Economic and Clinical Health Act

HMO : organismes de maintien de la santé ou Health Maintenance Organizations

Iaas : l'infrastructure en tant que service

ITA : l'Administration du commerce international ou l'International Trade Administration

Loi FD&C : Lois fédérales sur les aliments, les médicaments et les cosmétiques ou Federal Food, Drug and Cosmetics Acts

MLAT : Traité d’entraide judiciaire ou Mutual Legal Assistance Treaty

NIST : Institut national des normes et de la technologie ou National Institutes of Standards and Technology

NTIA : Administration nationale des télécommunications et de l'information ou National Telecommunications and Information Administration
NIST : Institut national des normes et de la technologie ou National Institutes of Standards and Technology

NPP : avis de politique de confidentialité ou Notice of Privacy Pratices

ONC : bureau du coordinateur national des technologies de l'information en matière de santé ou Office of the National Coordinator for Health Information Technology

OCR : Bureau des droits civils ou Office for Civil Rights

Paas : plate-forme en tant que service

PHI : informations sanitaires protégées

RGPD : Règlement général sur la protection des données

Saas : le logiciel en tant que service

U.S.C : Code des États-Unis ou United States Code

INTRODUCTION

Dans un contexte de commerce mondial, où les entreprises créent de nombreuses filiales dans plusieurs pays, où il existe aujourd'hui une externalisation du transfert des données collectées d'un pays, il est conseillé d'examiner la législation des différents territoires avant toute mise en œuvre. Notre étude portera donc sur deux d'entre eux qui ont été soumis à une réglementation stricte dans ce domaine, à savoir les États-Unis et l'Europe. Il aurait peut-être été également opportun de s'intéresser à la Chine, qui a mis en place un système de protection de la sécurité et de la confidentialité des données personnelles, avec une forte limitation créant des politiques de cybersécurité. Par ailleurs, le Japon aurait pu faire l'objet d'un développement, ayant mis en place une législation à la fois générale et sectorielle, mélange de la politique législative mise en œuvre aux États-Unis et de celle de l'Union européenne. Cependant, la volonté de cette carte de visite étant de clarifier certains points importants concernant la réglementation de certains pays ayant le plus haut taux de données en transit et bénéficiant d'une législation étendue, nous avons choisi de nous concentrer sur le droit américain et européen. En effet, tout au long de cette étude, nous tenterons d'exposer les règles générales sur la protection des données de santé dans le cadre du droit fédéral américain et du droit européen.

Le droit américain se compose de plusieurs lois nationales sur la protection de la vie privée et la sécurité des données, spécifiques à un secteur ou à un domaine. Il existe une centaine de réglementations relatives à la vie privée et à la sécurité parmi les 50 États qui composent son territoire. En ce qui concerne les données relatives à la santé, il s'agit de la loi sur la Portabilité et Responsabilité de l'assurance maladie (informations personnelles sur la santé) nommée HIPPA (Health Insurance Portability and Accountability Act). En outre, la Commission fédérale du commerce des États-Unis (FTC), un organisme indépendant du gouvernement américain dont la mission principale est l'application du droit de la consommation et le contrôle des pratiques commerciales anticoncurrentielles, s'occupe des pratiques déloyales en matière de vie privée et de sécurité des données.

En Europe, le Règlement général sur la protection des données (RGPD), entré en vigueur en 2016, est une législation unifiée au sein des pays membres de l'Union européenne. Ainsi, il est directement applicable aux États membres (certains articles de la directive peuvent être adaptés par les États membres afin d'avoir des règles plus strictes) concernant une cinquantaine de domaines.

L'objectif de cette carte de visite sera de traiter plus spécifiquement des partenariats existants entre les établissements de santé et les solutions digitales de suivi médical à travers une étude comparative franco-américaine. Cette étude permettra d'appréhender les étapes à devoir respecter dans la pratique ainsi que les questionnements théoriques ayant des incidences directes sur la création d'un projet e-santé. Le choix lors de cette étude est de traiter séparément les deux législations, comprenant des spécificités pouvant difficilement faire l'objet d'une conciliation au sein de mêmes parties. L'ensemble des ressources permettant la gestion des données personnelles par le biais d'utilisation d'équipements informatiques ainsi que de moyens d'hébergement et de communication

devront être prise en considération afin d'acquérir des réflexes juridiques précis, cohérents et suffisants en matière de conformité dans le cadre d'un traitement de données de santé.

Comme l'énoncent Madame Malafosse et Madame Bandon-Tourret : « la notion d'e-santé, ou santé numérique, désigne l'utilisation de technologies de l'information et de la télécommunication au service de la santé telles que les logiciels utilisés par les professionnels de santé dans le cadre de leur activité, la télémédecine et les applications mobiles relatives à la santé »[1]. Ce type d'application offre un suivi administratif et médical connecté afin de développer une gestion optimale des patients quelles que soient leurs pathologies, interventions ou traitements. Ces applications d'e-fitback sont le plus souvent des solutions de type *Software as a Service* (Saas), qui est un concept basé sur le cloud. [2] Ce type d'application permet la fourniture d'un service délivré via Internet qui ne nécessite aucune installation sur les services de l'établissement de santé. Le fournisseur de l'application est donc un hôte tiers. Ce type de service est en plein essor en raison de son faible coût au fil du temps. En effet, l'établissement de santé n'a plus besoin d'investir régulièrement dans de nouveaux logiciels, le fournisseur de Saas effectuant des mises à jour régulières. Un autre avantage du Saas dans le domaine du suivi médical est qu'il permet de désencombrer les hôpitaux et de suivre les patients à moindre coût.

Le terme « Cloud computing » est apparu dans les années 90. Le professeur Ramnath CHELLAPA – doyen associé et directeur académique du Master of Science in Business Analytics – utilisa ce terme pour la première fois en 1997 afin de désigner un paradigme informatique dont les limites ne seraient plus techniques mais économiques. Ce terme fut transformé en concept en 1999 par l'entreprise Salesforces, proposant un logiciel de gestion, et est devenu aujourd'hui un secteur de sous-traitance informatique. Le Cloud revêtant différentes définitions en fonction des organes et acteurs peut toutefois se caractériser par son extériorité et sa flexibilité. Il se distingue traditionnellement entre celui d'« infrastructure » et celui de « service » ainsi que par son offre pouvant être décliné en un Cloud privé, public ou mixte comme la présente étude tentera de l'expliquer. Malgré les différentes définitions existantes et la remise en question même de l'utilisation du terme Cloud concernant des solutions simples d'hébergement de données par certains professeurs [3], la Commission nationale de l'informatique et des libertés (CNIL) [4] le définit comme « le déport vers " le nuage Internet "[5] de données et d'applications qui auparavant étaient situées sur les serveurs et ordinateurs des sociétés, des organisations ou des particuliers. Le modèle économique associé s'apparente à la location de ressources informatiques avec une facturation en fonction de la consommation »[6]. Cette étude comparative sera envisagée sous le spectre de cette définition. Comme l'énonce le Département de la Santé et des Services sociaux des États-Unis, il existe plusieurs formes

---

[1] MALAFOSSE Jeanne Bossi, BANDON-TOURRET Diane, *Lancer un projet e-santé*, Editions Législatives, 2020, p.14.
[2] Société nouveal e-santé, « Les parcours de soins connectés avec e-fitback » [en ligne], [consulté le 25 juillet 2020]
[3] Cabinet Alain Bensoussan Avocats Lexing, « Cloud computing et droit, retour sur une année de grands changements », *Revue Lamy Droit de l'Immatériel, Nº 138*., [en ligne] 1er juin 2017, p. 2 [consulté le 25 juillet 2020]
[4] La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité de contrôle française en matière de données, il s'agit du régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.
[5] Bien avant qu'apparaisse l'expression " Cloud Computing ", les architectes réseau schématisaient Internet par un nuage. En anglais, le terme « the Cloud », était couramment utilisé pour désigner Internet.
[6] COMMISSION NATIONALE INFORMATIQUE ET LIBERTES, "Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services", publié le 25 juin 2012 [en ligne], [consulté le 12 juin 2020], sur https://www.cnil.fr/

de cloud computing. En effet, comme le défini l'Institut National des Standards et Technologie du Département du Commerce américain, le cloud computing est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un *pool* partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement approvisionnées et libérées avec un minimum d'effort de gestion ou d'interaction avec le fournisseur de services pouvant aboutir à trois types de service : SaaS, PaaS et IaaS[7].

Le PaaS (*Platform as a service*) est une solution généralement utilisée afin de fournir un cadre sur lequel les développeurs peuvent s'appuyer. Il est défini par le Département du Commerce américain comme étant « la capacité fournie au consommateur de déployer sur le cloud des applications créées ou acquises par les consommateurs, utilisant des langages de programmation, des bibliothèques, des services et des outils pris en charge par le fournisseur. Le consommateur ne peut gérer ou contrôler l'infrastructure en nuage sous-jacente, y compris le réseau et les serveurs, systèmes d'exploitation ou de stockage, mais a le contrôle des applications déployées et éventuellement les paramètres de configuration de l'environnement d'hébergement des applications »[8].

Quant au IaaS (*Infrastructure as a service*), il s'agit d'un nouveau modèle économique consistant à proposer des machines virtuelles ainsi qu'une puissance de traitement via une architecture cloud. Il sera fourni des ressources de traitement, de stockage, de réseaux et d'autres ressources informatiques fondamentales où le consommateur est capable de déployer et d'exécuter des logiciels arbitraires, qui peuvent inclure des systèmes d'exploitation et des applications. Le consommateur ne gère ni ne contrôle l'infrastructure en nuage sous-jacente, mais il a le contrôle des systèmes d'exploitation, du stockage et des applications déployées, et éventuellement un contrôle limité de certains composants de réseau (par exemple, les pares-feux des hôtes). Ainsi, au lieu d'acheter une infrastructure physique, les gens ne peuvent acheter que les ressources dont ils ont besoin.

Il convient de distinguer l'entreprise proposant un Saas de la société hébergeant les données qui fournira un service IaaS.

Hébergeant des données de santé lors du suivi administratif et médical, le prestataire de services a l'obligation de mettre en place, tout comme l'établissement de soins, des procédures de sécurité et de confidentialité des données personnelles du type « données de santé » dans les pays qui ont mis en place une protection de la vie privée dans le secteur de la santé. Tout acteur de projet e-santé devra contribuer à la sécurisation en respectant certains enjeux similaires en droit fédéral américain et en droit européen : disponibilité, intégrité, confidentialité et auditabilité.

Les données relatives à la santé peuvent être définies comme « les données relatives à la santé physique ou mentale passée, présente ou future d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne »[9].

Aux États-Unis, les lois sont spécifiques à un secteur, de sorte que toute entreprise souhaitant s'y installer devra en tenir compte. En effet, il n'existe ni de loi fédérale, ni d'autorité indépendante régissant la collecte et le traitement des données des utilisateurs. Les autorités déjà existantes telles

[7] MELL Peter, GRANCE Tomothy, « Recommendations of the National Institute of Standards and Technology : The NIST Definition of Cloud Computing », *NIST Special Publication 800-14* [en ligne], septembre 2011, p. 2 [consulté le 25 juillet 2020]

[8] Ibid.

[9] Art. 4, 15 du règlement (UE) 2016/679

que le Département de la santé ou la Commission fédérale du commerce (FTC) ont ainsi vu une extension de leur rôle respectif, devant aujourd'hui prendre en compte le respect de la protection des données personnelles. Par exemple, la FTC ayant pour finalité de protéger le consommateur aura un rôle de contrôle en matière de protection des données personnelles des consommateurs. Dans le secteur de la santé, la loi la plus emblématique est la loi portabilité et responsabilité en matière d'assurance maladie. Cette loi doit être traitée en priorité, en établissant la base commune de la législation sur les données de santé à prendre en considération par les différents acteurs du secteur de la santé. Toutefois, ce n'est pas la seule loi applicable, notamment en matière d'applications de suivi médical. Selon le type d'application, les lois à respecter pouvant différer (Chapitre 1).

En Europe, comme indiqué précédemment, il existe un texte unifié sur la protection et la confidentialité des données personnelles. L'étude ne devrait donc pas se concentrer sur le type de législation applicable mais sur le type d'acteur qui, concernant le RGPD, entre dans le partenariat. Cette considération nous permettra d'identifier le type de responsabilités que les différents acteurs doivent assumer, et par conséquent le type de contrat et de procédures à mettre en œuvre. Cependant, le RGPD pouvant être complété par le droit national des Etats membres dans le domaine des données de santé - ce qui fut particulièrement le cas en France – l'étude de la conformité supplémentaire afin de répondre aux exigences posées par le droit français est nécessaire. (Chapitre 2).

En outre, il est essentiel de traiter des transferts internationaux de données. Cela permettra d'examiner dans quelles conditions le transfert de données à caractère personnel est possible, quels pays devraient être favorisés en cas d'établissement aux États-Unis ou en Europe, ou de volonté de transfert, et, enfin, s'il existe ou non des dérogations à la politique de circulation transfrontalière des données dans ces pays. Promulguée par le Congrès américain, la loi fédérale américaine, dite Cloud Act, est venue clarifier l'utilisation légale des données situées à l'étranger par les autorités américaines. Cette loi promulguée en 2018 engendre un large débat depuis plusieurs années quant aux effets pouvant en découler en matière de protection des données personnelles en cas de transfert. Afin de prendre en considération l'ensemble des problématiques pouvant être rencontrées en matière de transfert international de données, il est plus que primordiale de prendre de la hauteur afin de traiter de l'impact du Cloud Act sur le traitement des données de santé. En effet, la contractualisation avec un hébergeur américain peut entraîner des conséquences devant être prises en considération par les différents acteurs du secteur. (Chapitre préliminaire).

CHAPITRE PRÉLIMINAIRE : DES DIFFÉRENCES D'APPROCHES ENTRE LES LÉGISLATIONS EN MATIÈRE DE TRANSFERTS INTERNATIONAUX DE DONNÉES À CARACTÈRE PERSONNEL

Se référant à la circulation ou au transfert d'informations entre serveurs informatiques par-delà les frontières nationales, les flux de données transfrontaliers permettent aux personnes de transmettre des informations par-delà les frontières. D'un pays à l'autre, les politiques et les lois relatives aux données varient. Pendant que le règlement général sur la protection des données de l'Union Européenne (RGPD) est motivé par des préoccupations liées à la protection de la vie privée, l'objectif de la politique commerciale internationale des États-Unis est de garantir l'ouverture des flux de données transfrontaliers. Comme l'indique le Congressional Research Service[10] dans un rapport de mars 2019[11]: « Il n'existe pas de norme ou de définition mondialement acceptée de la confidentialité des données dans le monde en ligne, et il n'existe pas de règles multilatérales contraignantes complètes concernant spécifiquement les flux transfrontaliers de données et la confidentialité ». Même s'il n'existe pas de règles multilatérales complètes concernant spécifiquement la vie privée ou les flux de données transfrontaliers, il existe des négociations sur de nouveaux accords commerciaux et des règles qui ont promulgué des codes de conduite recommandés [12]. Toutefois, il convient de noter que la convention 108 du Conseil de l'Europe constitue l'instrument juridique internationale de prédilection, étant le plus large à ce sujet. Il s'agit du premier instrument international contraignant dans le domaine de la protection des données. Comme l'énonce le Conseil de l'Europe, « les parties doivent prendre les mesures nécessaires en droit interne pour en appliquer les principes afin d'assurer, sur leur territoire, le respect des droits fondamentaux de la personne humaine au regard de l'application de la protection des données ».

Au sein de cette étude – d'autant plus que les Etats-Unis ne sont pas parties à la Convention 108 – la question des flux de données transfrontaliers doit être examinée à la lumière des législations américaine et européenne. En effet, il existe un souci croissant de garantir la continuité du régime de protection mis en place à l'intérieur de chaque pays, même au-delà de leurs frontières. Cette préoccupation se manifeste face à l'intensification des échanges électroniques rendant impossible le confinement du partage des données sur le territoire de chaque pays.

Promulguée par le Congrès américain, la loi fédérale américaine dite Cloud Act, est venue clarifier l'utilisation légale des données situées à l'étranger par les autorités américaines. Ainsi, l'accès aux preuves électroniques stockées à l'étranger dans le cadre de procédures pénales est aujourd'hui encadré en raison de la demande croissante aussi bien des forces de l'ordre américaines que des grandes entreprises technologiques (principalement les GAFAM). En effet, comme il fut constaté, une enquête pénale sur deux nécessite la saisie de preuves électroniques stockées sur les

[10] Le Congressional Research Service, une composante de la Bibliothèque du Congrès, effectue des recherches et des analyses pour le Congrès sur un large éventail de questions de politique nationale.

[11] F. FEFER Rachel, « Data Flows, Online Privacy, and Trade Policy », *Congressional Research Service Report* [en ligne], mars 2019, sommaire, [consulté le 25 juillet 2020]

[12] Accord général sur le commerce des services de l'OMC, Effort plurilatéral de l'OMC, Lignes directrices de l'OCDE sur la protection de la vie privée, Déclaration ministérielle sur l'économie numérique du G-20 de 2018, Cadre de protection de la vie privée de l'APEC de 2005 ou Règles transfrontalières de l'APEC sur la protection de la vie privée.

serveurs localisés hors du territoire américain[13]. Ce texte fait suite aux entraves rencontrées par les forces de l'ordre américaines et vient renforcer les pouvoirs étendus par le USA Patriot Act de 2001 – remplacé ainsi que modifié par le USA Freedom ACT en 2015 – d'obtention des preuves des banques, des fournisseurs de services dans le nuage et d'autres entreprises dans un objectif d'application de la loi de protection contre le terrorisme, le soutien matériel et le blanchiment d'argent. L'application de la loi permet aux enquêteurs de mettre en œuvre les outils classiques de procédure pénale à des fins probatoires mais aussi punitives : citations à comparaître devant un grand jury, mandats de perquisition, écoutes téléphoniques, ordonnances, registres, etc. Le Cloud Act a pour objectif de rationaliser certains de ces pouvoirs d'investigation au vu de la nécessité d'éventuels accords bilatéraux afin de procurer aux États des droits réciproques concernant les données électroniques des entreprises stockant à l'étranger. Il s'agit d'une conséquence directe de l'affaire opposant l'entreprise Microsoft aux États-Unis : sur le fondement du Stored Communications Act[14], la société Microsoft exécutait le mandat en fournissant les données visées situées sur le sol américain mais refusa de divulguer celles stockées sur des serveurs localisés à l'étranger dans son data center en Irlande, devant obligatoirement être fondé sur le Traité d'entraide judiciaire (Mutual Legal Assistance Treaty ou MLAT) seul apte à « permettre, d'une manière générale, l'échange de preuves et d'informations en matière pénale et dans des domaines connexes »[15].

Cependant, l'accueil de l'autre côté de l'Atlantique fut hostile à l'arrivée de cette nouvelle loi. En effet, le règlement général sur la protection des données adopté par l'Union européenne engendre un débat bien plus pratique que théorique autour d'un possible conflit de loi.

Il conviendra donc lors de notre étude sur le transfert international de données personnelles de passer en revue l'étendue des obligations résultant du Cloud Act dans un premier temps. Et, dans un second temps, de clarifier les articles du RGPD afin d'identifier si ledit texte américain contredit réellement les règles européennes en matière de protection des données, et, si, il n'existe pas dans la pratique des moyens de pallier aux effets négatifs pouvant être engendrés par ce texte lorsque ceux-ci sont avérés.

I- L'approche américaine

En matière de droit américain, il n'existe pas de textes permettant le transfert de données avec des pays tiers. Cependant, le Stored Communication Act adopté en 1986 vient fixer un principe de confidentialité et de protection des données de communications stockées sur le sol américain, à l'exception notamment de toutes requêtes américaines en matière de procédures répressives. Ainsi, par ce texte, les États-Unis avaient la possibilité de transférer des données par le biais de traités bilatéraux. Ces derniers furent remplacés en 2003 par des traités d'assistance judiciaire mutuelle ou dit MLAT. Il existe aujourd'hui de nombreux traités mais aussi, des mécanismes de certifications qui

[13] Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontalier aux preuves électroniques aux fins de la coopération judiciaire en matière pénale, COM, 70 final, 2019, p. 1.

[14] Il s'agit d'un ancien texte adopté en 1986 permettant les communications de données électroniques sur le sol américain. Ce texte n'envisageait pas à l'époque la situation où les données électroniques sont accessibles depuis les États-Unis mais stockées sur des serveurs à l'étranger.

[15] Treaties and Agreements, sur U.S Department of State Archive, [en ligne] publié le 7 mars 2012, [consulté le 25 juillet 2020]

furent favorisés par l'entrée en vigueur du RGPD. Toutefois, le fameux « Privacy Shield » est aujourd'hui remise en question par la Cour de Justice de l'Union Européenne. En outre, il existe aujourd'hui un autre débat qu'il convient de traiter : les effets du Cloud Act.

A- Les règles générales en matière de transfert

Comme il peut être constater à travers les accords ou les rapports du gouvernement américain, les États-Unis préconisent une politique d'un Internet libre et ouvert, qui se traduit par la liberté de circulation. Dans de nombreux engagements internationaux de libre-échange, la volonté politique de rendre obligatoire le fait que les gouvernements « ne peuvent pas mettre en œuvre des mesures commerciales qui entraveraient le commerce numérique des biens et des services, restreignent les flux de données transfrontaliers ou exigent le stockage ou le traitement local des données » peut être perçue[16]. Toutefois, la nature sectorielle des lois du pays et le fait que les États légifèrent également, rendent difficile pour les autorités – notamment la FTC – l'application des mesures générales de protection des données personnelles. Ainsi, à travers des traités bilatéraux ou multilatéraux, les États-Unis tentent de négocier dans ce domaine afin d'obtenir des autorisations pour le transfert transfrontalier d'informations. Il s'agit notamment de certains accords tels que l'Accord États-Unis-Mexique-Canada pour la révision de l'Accord de libre-échange nord-américain, qui comprend un chapitre 19 sur le commerce numérique, ou l'Accord global et progressif pour le partenariat transpacifique négocié par l'administration Obama traitant spécifiquement de la question des flux transfrontaliers de données[17]. Enfin, l'administration Trump prépare des travaux visant à établir une politique américaine globale de protection des données dans un avenir proche grâce notamment aux National Institutes of Standards and Technology (le NIST élabore un cadre de protection de la vie privée), aux National Telecommunications (le NTIA élabore un ensemble de principes de protection de la vie privée) et à l'International Trade Administration qui collabore avec des gouvernements étrangers et des organisations internationales (le rôle de l'ITA est de veiller à ce que les approches du NIST et du NTIA soient conformes aux objectifs de la politique internationale des États-Unis).

Malgré les différences d'approche en matière de protection et de confidentialité des données personnelles, les États-Unis et l'Europe avaient convenu d'un mécanisme d'auto-certification depuis 2016, appelé « Privacy Shield ». Il s'agissait de l'un des seuls cas de véritable accord de conformité visant à garantir le transfert international sécurisé de données à caractère personnel entre les États-Unis et un pays tiers.

Ce programme volontaire par lequel les entreprises établies aux États-Unis étaient reconnues comme offrant un niveau de protection adéquat en vertu de la législation européenne pour le transfert de données par une entité européenne à des entreprises établies aux États-Unis. Cette auto-certification comprenait des engagements et des obligations ainsi que des limitations d'accès par les autorités répressives et des exigences de transparence. En effet, cette exigence résulte des habitudes américaines en matière de surveillance massive des responsables de traitement par les pouvoirs

[16] CONGRES AMERICAIN, Public Law 114-26, titre I, Sect. 102 (b)(6)(C), 9 juin 2015, 129 STAT. 319
[17] L'administration Trump a retiré les États-Unis de l'accord en janvier 2017. Toutefois, l'accord reflète la politique américaine en matière de données personnelles, qui était encore similaire sous l'administration Trump.

publics [18]. Les entreprises éligibles à ce mécanisme d'auto-certification devaient relever de la compétence de la Federal Trade Commission (FTC) ou du ministère américain des transports (DoT pour U.S Department of Transportation). Pour cela, l'entreprise en question devait disposer d'une certification active dans le domaine des données personnelles spécifiques. En effet, la loi américaine étant spécifique à un secteur, il ne s'agissait pas d'une certification pour toutes les données. Un site web permettait[19] de vérifier si l'organisation en question figure sur la liste du Privacy Shield.

En outre, comme l'indiquait le gouvernement américain sur son site : « Les responsables du traitement des données dans l'Union Européenne (UE) et en Suisse sont tenus de conclure un contrat lorsqu'un transfert est effectué à des fins de traitement uniquement, que le destinataire soit ou non un participant au programme Privacy Shield. Dans le cadre du Privacy Shield, ce contrat ne nécessite pas d'approbation préalable et ne doit pas inclure de clauses contractuelles types ». En effet, le principe supplémentaire 10 portant sur les contrats obligatoires pour les transferts ultérieurs, énonçait l'obligation d'un contrat afin d'apprécier le respect du RGPD par le sous-traitant[20]. En cas de transfert de données à une société agissant en tant que responsable du traitement, la base juridique du transfert doit être vérifiée au préalable à la lumière de l'exigence de consentement prévue aux articles 7 et 8 du RGPD. Enfin, il appartient au responsable du traitement des données de la société européenne de se conformer ce règlement. En particulier, les personnes concernées doivent être informées du transfert de données (la finalité du transfert, les destinataires de leurs données et le fait que les données sont protégées par le bouclier de protection des données).

C'est dans ce cadre qu'aujourd'hui cette auto-certification ne peut plus constituer une base légale. En effet, le Comité européen de la protection des données (CEPD) a précisé lors d'une Foire Aux Questions[21] publiée le 24 juillet sur son site que les « transferts effectués sur la base de ce cadre juridique sont illégaux » en raison d'une décision de la Cour de justice de l'Union européenne (CJUE) invalidant, le 16 juillet 2020, le Privacy Shield dû au risque que font peser les programmes de surveillance américains sur la protection des données. Ainsi, les entreprises ne pourront à partir d'aujourd'hui, aucun délai de grâce n'étant accordé, que faire appel à des clauses contractuelles types par le biais de modèles de contrats de transfert de données personnelles ayant fait l'objet préalablement d'une approbation de la part de la Commission européenne comme le prévoit le RGPD et l'a approuvé la CJUE. Cependant, au regard de la décision de la CJUE, l'annulation de la Privacy Shield résultant de la surveillance des autorités américaines, ainsi comme l'a rappelé la Cour, le seul fait que les autorités publiques américaine ne soient liées par aucune clause type contractuelles, bien que ne remettant pas en cause la validité des transferts fondées sur ce type de clauses, entraînent une obligation pour les entreprises d'adopter des mesures complémentaire dans le seul but d'assurer un niveau de protection adéquat au regard de la réglementation européenne. En effet, la volonté des

[18] Cette exigence s'inscrit à la suite de l'arrêt de la CJUE dit « Schrems I », du 6 octobre 2015 dans l'affaire C-362/14 Maximillian Schrems / Data Protection Commissioner antérieur à l'arrêt du 16 juillet 2020 dit « Schrems II » invalidant le Privacy Shield.

[19] INTERNATIONAL TRADE ADMINISTRATION, European Businesses, sur *Privacy Shield Framework* [en ligne], [consulté le 10 février 2020 et 20 aout 2020]

[20] INTERNATIONAL TRADE ADMINISTRATION, « Obligatory Contracts for Onward Transfers », sur *Privacy Shield Framework* [en ligne], [consulté le 10 février 2020 et 20 aout 2020]

[21] JELINEK Andrea, « Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems », sur le site du Comité européen de la protection des données [en ligne], adopté le 23 juillet 2020 [consulté le 25 juillet 2020]

entreprises de commercialiser des services Cloud en adéquation avec le RGPD pose problème au regard de la réglementation américaine applicable aux entreprises américaines même lorsque les datacenters se trouvent sur le sol européen et qu'il s'agit de données de résidents européens. Par l'invalidité du Privacy Shield, les entreprises se retrouvent dans l'obligation de recourir aux autres outils de transfert sous peines d'amendes s'élevant jusqu'à 4% du chiffre d'affaires annuel mondial ou 20 millions d'euros. Cependant, l'énonciation par la CJUE de la mise en place de mesures complémentaires ne précise pas lesquelles. Une précision de la part des autorités de contrôle est fortement attendue. En outre, cet arrêt a une portée générale. Tout État tiers non amène d'assurer un niveau de protection adéquat pourra voir la décision d'adéquation conclue invalidée. Une vigilance quant aux décisions futures de la CJUE dans ce domaine est nécessaire au regard notamment du système de surveillance intrusif mise en place par des pays tels que la Russie ou la Chine jouissant à l'heure actuelle d'une décision d'adéquation.

Afin de mieux appréhender l'impact de la réglementation américaine en matière de transferts de données, il convient de se référer notamment aux règles mise en place par la Loi sur la clarification de l'utilisation légale des données à l'étranger (Clarifying Lawful Overseas Use of Data Act).

B- Une complémentarité de règles en matière d'enquête : l'avènement du Cloud Act

Dès lors que des données sont stockées dans le Cloud[22], la protection des données à caractère personnel est soumise à la législation du pays où le fournisseur du service choisi réside. Chaque pays ayant ses propres particularités juridiques, la prise en compte de la législation applicable revêt un caractère essentiel dans le choix d'un hébergeur. Cette vigilance doit notamment conduire les entreprises à étudier la législation en vigueur mais aussi le contrat devant découler de cette relation.

Dans le cadre d'une étude comparative droit américain fédéral/droit européen, mais aussi dans le cadre d'une étude globale internationale, l'entrée en vigueur du Clarifying Lawful Overseas Use of Data Act, promulguée le 23 mars 2018, entraîne des effets sur lesquels il convient de se pencher.

Dans une lettre adressée au vice-président Joseph Biden en sa qualité de président du Sénat américain, le procureur général adjoint Peter J. Kadzik avait décrit la future loi clarifiant l'utilisation légale des données à l'étranger comme nécessaire à la sécurité des échanges et respectueux de la vie privée aux fins de lutte contre les crimes graves, y compris le terrorisme[23]. Celui-ci avait notamment perçu la difficulté auxquelles faisaient face les entreprises, confrontées à des obligations juridiques contradictoires venant des gouvernements, entraînant une insécurité juridique. En outre, il fit remarquer la difficulté ressortant du processus du MLAT. En effet, les traités d'entraide judiciaire constituent un mécanisme jugé trop laborieux en raison de la demande exponentielle d'assistance adressée aux États-Unis à l'ère du numérique. Un même prestataire détient généralement plusieurs data centers et, ainsi, l'ensemble des données d'un même individu n'est pas automatiquement stocké au même endroit[24]. L'État qui souhaiterait avoir accès, dans le cadre d'une enquête, à l'ensemble de

[22] Il sera détaillé l'importance du choix d'un service d'hébergement et les règles afférentes au sein des chapitres suivants.
[23] KADZIK Peter, Lettre de l'assistant du général de division au vice-président Joseph R. Biden, président du Sénat des États-Unis [courriel], 15 juillet 2016.
[24] Ibid.

ces preuves électroniques se retrouverait dans l'obligation d'engranger plusieurs procédures MLAT simultanément sans pouvoir être certain d'avoir un retour positif pour l'ensemble des demandes de divulgation. En outre, tout pays n'ayant pas conclu de traité avec les États-Unis devra passer par une commission rogatoire, ne pouvant être émise pendant la phase d'enquête d'une procédure pénale. Ces procédures MLAT étant longues et manquant de souplesse, l'application du Cloud Act permet aujourd'hui de contourner cette procédure. Pour démontrer la complexité de cette procédure il est intéressant notamment de se référer à l'exemple donné par CALLAWAY David et DETERMANN Lothar au sein de l'article « The New US Cloud Act – History, Rules, and Effects »[25].

En réponse aux demandes provenant des services répressifs américains, les fournisseurs de communication électronique[26] et de services informatiques à distance[27] ont l'obligation de divulguer le contenu d'un fil ou d'une communication électronique qui seraient en leur possession, sous leur garde ou sous leur contrôle. Il importe peu que cette communication soit située à l'intérieur ou à l'extérieur des États-Unis en vertu de l'article 2713 du Titre 18 du Code des États-Unis (appelé aussi 18 U.S.C.) suite à la codification du H.R 4943 §103(a) du Cloud Act en son sein [28]. Toutefois, la loi met à la disposition des fournisseurs [29] une base légale leur permettant de contourner le mandat de divulgation des données. En effet, l'article 2703(h)(2)(A) 18 U.S.C. permet de déposer une motion de modification ou d'annulation [30] de la citation à comparaître ou de tout autre processus juridique nul et non avenu, en raison d'une conviction raisonnable provenant du fournisseur selon laquelle la divulgation d'un client ou d'un abonné, étranger et résidant à l'étranger (le terme étranger vise toute personne non américaine et ne résidant pas sur le territoire américain), « créerait un risque important que le fournisseur viole les lois d'un gouvernement étranger admissible ». Il convient toutefois de faire remarquer que la loi Cloud ne modifie en rien les normes préexistantes de common law et de courtoisie internationale [31].

Comme il a été énoncé précédemment, la loi mentionne qu'il doit s'agir d'un risque violant les lois d'un « gouvernement étranger admissible » (*qualifying foreign government*). Le Cloud Act le définit comme un gouvernement ayant conclu un accord intergouvernemental (appelé aussi *executive agreement*) avec le procureur général des États-Unis non formellement désapprouvé par le Congrès

---

[25] CALLAWAY David et DETERMANN, « The New US Cloud Act – History, Rules, and Effects », The Computer & Internet Lawyer, Vol. 35, n°8, 2018, §III.

[26] Titre 18 du Code des États-Unis, Chap. 119 - Interception des communications filaires et électroniques et interception des communications orales, §2510(15) [en ligne] : « tout service qui fournit [...] aux utilisateurs [...] la possibilité d'envoyer ou de recevoir des communications par fil ou par voie électronique »))

[27] Titre 18 du Code des États-Unis, Chap. 121 – Accès aux communications électroniques et aux documents transactionnels stockés, § 2711(2) [en ligne] : l'expression "service informatique à distance" désigne la fourniture au public de services de stockage ou de traitement informatique au moyen d'un système de communications électroniques

[28] Titre 18 du Code des États-Unis, Chap. 121, § 2711 [en ligne]

[29] Le fournisseur, « y compris un service de communication électronique étranger ou tout service information à distance.

[30] Il convient de noter qu'une requête en annulation nécessite qu'un tribunal américain procède à une analyse de courtoisie. Nous étudierons dans notre seconde partie les conséquences de cette analyse en matière de choix d'hébergeur pour une entreprise ou un hôpital français.

[31] La courtoisie internationale est à distinguer notamment du droit international public. Il s'agit d'un ensemble d'usage suivis à titre de simples convenances et pour des raisons de commodité pratique. Dans le contexte de l'internationalisation, la courtoisie constitue une coopération fortement utilisée supposant qu'un pays examine la demande que lui adresse un autre pays en vue d'engager ou d'élargir une procédure d'application de ses réglementations afin de mettre un terme à une pratique gravement préjudiciable aux intérêts du pays requérant.

américain[32]. Ainsi, le procureur général devra obtenir au préalable l'autorisation du secrétaire d'État et du Congrès par le biais de la démonstration suivante : le droit interne étranger et sa mise en œuvre doivent être en capacité de fournir une protection suffisante de fond et de procédure en matière de vie privée, de libertés civiles et de protection des données à la lumière des activités et collectes de données opérées par le gouvernement étranger. En effet, devra être garantie la mise à disposition de lois adéquates en matière de cybercriminalité et de preuve électronique. De plus, l'État en question doit adhérer au préalable à l'ensemble des obligations et engagements internationaux applicables en matière des droits de l'Homme ou faire preuve de respect pour les droits de l'Homme universels par le biais notamment d'une protection contre toute atteinte, détention ou arrestation arbitraire envers un justiciable, la garantie du droit à un procès équitable et enfin, l'interdiction de la torture et des peines ou traitements considérés comme cruels, inhumains ou dégradants. Enfin, pour être considéré comme admissible, le gouvernement doit adopter des procédures appropriées afin de réduire au minimum l'acquisition, la conservation et la diffusion d'informations concernant les ressortissants des États-Unis visés par l'accord au regard de l'article 2523(b)(2) U.S.C 18. In fine, le fait d'être reconnu comme un gouvernement admissible entraînera la possibilité de contester toute divulgation violant une loi, par exemple le RGPD mais permettrait aussi au dit gouvernement de demander des informations à un fournisseur américain sans avoir à passer par le processus du traité d'entraide judiciaire sous réserve d'un accord intergouvernemental. L'ensemble des dispositions devant être incluses dans l'accord sont précisées au sein du Cloud Act.[33]

Parmi les problématiques qui ont justifié les travaux afin d'édicter de nouvelles réglementations dans ce domaine, la question de la nationalisation des flux de données s'est transformée, à l'ère numérique, en une internationalisation due à l'intensification des échanges électroniques. Ainsi, la question du contrôle des transferts internationaux de données et des paradis de données a été débattue en Europe. Afin de protéger les citoyens européens contre l'exploitation de leurs données dans des pays extérieurs à l'Union européenne - où les règles européennes ne sont pas applicables – de nouvelles réglementations ont dû être mises en place.

II- L'approche européenne

En droit européen, il existe un principe de garantie de conformité en matière de transferts des données vers des pays tiers. Ainsi, il convient d'étudier les règles générales en matière de transfert de données. L'arrivée du Cloud act étant considéré comme contrevenant aux règles imposées par le RGPD son étude est primordiale.

A- Les règles générales en matière de transfert

Les transferts internationaux de données au regard du RGPD consistent à envoyer des données en dehors de l'Union Européenne ou à accéder à des données sur un autre territoire[34]. Le RGPD

[32] Titre 18 du Code des États-Unis, Chap. 121 §2523(b)(1) [en ligne]
[33] Annexe 1
[34] Considérant 101 du Règlement (UE) 2016/679

considère que les transferts de données au sein de l'UE sont garantis. En effet, il existe un principe de libre circulation des données sur le sol européen en raison des règles unifiées en Europe. En outre, ce principe implique l'interdiction d'envoyer des données en dehors du territoire européen en raison d'un manque de protection au sein de l'État tiers. Le caractère adéquat s'apprécie au regard de l'ensemble des circonstances relatives au transfert ou à une catégorie de transfert de données : la nature des données, la finalité du traitement, la durée du traitement, le pays d'origine. Si les données proviennent d'un pays tiers et sont traitées dans l'UE, la règle est celle de la protection en vertu de la législation du pays d'accueil.

Il existe des exceptions à ces principes. En effet, en raison de l'intensification de l'externalisation des flux, des solutions doivent être envisagées afin de préserver un minimum de garanties pour les personnes concernées. Des garanties supplémentaires devraient ensuite être prévues pour les État tiers afin d'assurer la protection de la vie privée. Cela peut être considéré comme une similitude avec les États-Unis qui imposent leurs propres normes généralement à d'autres pays par le biais d'un accord. Dans tous les cas, la dérogation est subordonnée au respect de garanties adéquates pour la protection de la vie privée et des libertés et droits fondamentaux (y compris les recours juridiques). En plus des décisions d'adéquations, il existe trois types d'exceptions devant faire l'objet d'un développement.

On peut rappeler que le régime de protection établi par le RGPD prévoit, à la lumière de l'article 44, que tout transfert de données vers un État tiers fondé sur une décision d'adéquation entre le droit applicable dans un État tiers et un État membre entraîne un niveau de protection adéquat[35]. C'était notamment le cas pour une décision d'adéquation entre le Japon et l'UE du 23 janvier 2019.[36] Ces décisions d'adéquation sont progressivement adoptées par la Commission européenne. Il s'agit donc d'une sorte d'accord internationale répertorié sur le site de la Commission européenne.

L'une des exceptions la plus importante est l'établissement de garanties contractuelles solides. L'absence de protection juridique sera donc remplacée par une protection contractuelle.

L'une des clauses essentielles pour garantir le respect de l'accord de transfert de données à caractère personnel est la clause dite « tiers bénéficiaire ». Ainsi, les personnes concernées par le traitement pourront intenter une action en justice en invoquant cet accord afin de justifier l'absence de protection des données. En outre, l'autorité nationale est compétente pour veiller au respect de ces clauses et vérifier leur signature.

Enfin, il existe des règles d'entreprise contraignantes similaires au système des clauses contractuelles mais s'appliquant au sein des groupes de sociétés qui, uniquement dans ce cas précis, doivent être autorisées avant tout transfert par l'autorité nationale.

En outre, certains cas particuliers autorisent les transferts internationaux de données, notamment en cas de force majeure. Cette règle est énoncée à l'article 26 du RGPD, qui permet aux États membres de prévoir qu'un transfert de données à caractère personnel sera possible vers un pays ne disposant pas d'un niveau de protection adéquat. Il s'agit d'une dérogation en raison de la forte

[35] CNIL, « La protection des données dans le monde, sur le site de la CNIL » [en ligne], publié le 19 novembre 2019, [consulté le 20 mars et 25 août 2020]

[36] La compatibilité avec le RGPD a été exigée en ce qui concerne les règles d'accès aux données à des fins de procédures pénales et de sécurité nationale et ses conditions juridiques spécifiques permettant aux européens de porter plainte contre des entreprises japonaises.

suspicion que ce niveau de protection n'est pas atteint. Ce sera le cas une fois que le consentement préalable de la personne concernée aura été donné, dans le cas où le transfert de données est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou si cela est nécessaire à la conclusion ou à l'exécution d'un contrat entre le responsable du traitement et un tiers. Une autorité, y compris un tribunal, doit avoir demandé un tel transfert. Ou, lorsque le transfert est nécessaire à la protection des intérêts vitaux de la personne concernée, le transfert de données vers un État tiers dans le domaine de la santé.

Il convient de rappeler que ces exceptions ne peuvent s'appliquer à des traitements massifs, récurrents ou structurels.

Au regard de l'expansion toujours plus massive chaque année des solutions offertes par les fournisseurs de solutions cloud, la question du transfert des données revêt un caractère fondamental. En effet, depuis quelques années est née une doctrine portant sur la volonté de créer un Cloud « souverain » c'est-à-dire de restreindre le recours à seulement certains fournisseurs situés sur le sol national en matière de certaines données. L'une des idées qui en est à l'origine est celle de faire face à la volonté croissante d'autres pays, selon cette doctrine, de « capter » par la donnée des informations stratégiques, quand bien-même le fondement de cette captation paraîtrait légitime.[37] Il convient alors à la lumière de l'entrée en vigueur du Cloud act en 2018 et l'annulation de la Privacy Shield d'étudier le point de vue des auteurs européens concernant les effets du Cloud act.

B- La critique européenne du Cloud Act : aspect théorique et pratique

Comme il a été affirmé précédemment en vigueur du Cloud act résulte d'une volonté politique des forces de l'ordre et mais aussi des entreprises d'alléger et de clarifier les procédures de divulgation. Cependant, l'adoption du Cloud Act trouve avant tout sa source au sein de l'affaire Microsoft vs. United States. En effet, la Cour d'appel des États-Unis du deuxième circuit a déclaré comme application extraterritoriale illégale un mandat exigeant d'une société que celle-ci procède à la récupération de données stockées sur des serveurs à l'étranger. Cette loi avait ainsi pour première nécessité de rendre sans objet l'affaire en instance devant la Cour suprême. Comme Peter J. Kadzik en avait fait mention au sein de sa lettre, il s'agissait d'un « ajout nécessaire » afin de résoudre les litiges en cours devant la Cour suprême.

De part la naissance de ces litiges, s'est posée la question de savoir si le règlement général sur la protection des données empêcherait la mise en œuvre du Cloud Act. Autrement dit, le Cloud Act, autorisant des injonctions indépendamment du lieu de détention des données crée-t-il un conflit de loi ? Il convient ainsi de se placer à travers le spectre d'une entreprise soumise à la compétence juridictionnelle américaine, ayant des données stockées sur des datas center en Europe et, faisant l'objet d'une injonction de divulgation de données par les autorités américaines. En effet, une connaissance pointue du sujet permettra aux acteurs du secteur des données de santé de connaître l'ensemble des conséquences pouvant découler de la conclusion d'un contrat d'hébergement avec une entreprise soumise à la compétence américaine.

[37] BOURGEOIS Mattieu, « CLOUD COMPUTING - Notions et enjeux», *JurisClasseur Communication* [en ligne], mai 2020, [consulté le 27 juillet 2020]

Il existe aujourd'hui deux situations pouvant justifier une opposition de la part d'un prestataire de service à l'encontre d'une demande de divulgation de données dans un délai de 14 jours suivant la demande[38] : celle fondée sur un accord intergouvernemental (*executive agreement*) et celle basée sur le fondement d'une exception de courtoisie (appelée *comity*) à l'égard d'une réglementation étrangère applicable (dans le cas présent, le RGPD).

Dans le cas d'un accord intergouvernemental, la législation énumère trois conditions devant être prises en considération par le juge afin d'identifier si le risque de violation est suffisamment avéré pour annuler le mandat : l'intérêt de la justice exigeant d'annuler ou de modifier la demande des autorités américaine, des données concernant un justiciable de l'état étranger ne résidant pas sur le sol américain et une violation du droit étranger [39].

Afin d'effectuer une balance entre les intérêts des juridictions étrangères et ceux de l'état américain, huit intérêts doivent être pris en considération : les intérêts des États-Unis, y compris ceux de l'autorité américaine sollicitant l'information ; les intérêts de l'État étranger au non-dévoilement de l'information ; la probabilité, l'ampleur et la nature des sanctions auxquelles s'exposent les prestataires ou leurs employés ; la localisation et la nationalité de la personne dont les données sont sollicitées ainsi que l'ampleur et la nature de ses liens avec les États-Unis et l'État étranger ; l'ampleur et la nature des liens et de la présence du prestataire avec les États-Unis ; l'importance de l'information sollicitée pour les investigations ; la possibilité d'obtenir l'information par des moyens qui seraient moins dommageables, et, cas plus particulier, les intérêts de l'autorité d'un État tiers qui a sollicité les informations auprès des États-Unis dans le cadre de la coopération internationale en matière pénale.

En matière de *comity*, le professeur Régis Bismuth – se fondant lui-même sur un article[40] – estime qu'en « l'absence d'*executive agreement* conclu entre les États-Unis et l'État étranger, l'analyse des juridictions américaines ne serait pas fondamentalement différente »[41]. Cependant, bien que le Cloud Act exprime, en l'absence d'un accord conclu entre l'Union Européenne et les États-Unis, que « les normes de droit commun [régissent] la disponibilité ou l'application de l'analyse de la courtoisie internationale »[42], l'application des critères est extrêmement incertaine, ne se basant que sur la jurisprudence américaine. En effet, l'analyse de la courtoisie internationale ne constitue pas un principe de procédure destiné à trancher un conflit de loi mais bien une doctrine de simple diplomatie judiciaire relevant de la souveraineté du pays ayant compétence juridictionnelle, dans le cas présent, il s'agit donc de la souveraineté juridictionnelle américaine. Il est ainsi possible d'estimer que contrairement à l'analyse du professeur Regis Bismuth, cette situation est vectrice d'une réelle insécurité juridique. En effet, comme le souligne Madame Augagneur[43], il ne s'agit que d'une analyse fondée sur une volonté de « relations cordiales de collaboration » (*amicable working relationship*).

---

[38] Titre 18 du Code des États-Unis, Chap. 121, §2703(h)(1)(A)(i)
[39] Titre 18 du Code des États-Unis, Chap. 121, § 2703(h)(2)(B)
[40] JACOB Patrick, « Quand les nuages ne s'arrêtent pas aux frontières, Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », *Cahier de droit de l'entreprise*, n° 4, dossier 28, Juillet 2018 -Lexis 360® [consulté le 14 juillet 2020]
[41] BISMUTH Régis, « Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ? », *Revue critique de droit international privé*, [en ligne] 2019, p.681, [consulté le 12 août 2020]
[42] Cloud Act, H.R. 4943 § 103(c)
[43] AUGAGNEUR Luc-Marie, Héberger ses données chez les GAFAM : quel discours croire sur le Cloud Act ?, Revue Lamy Droit de l'Immatériel, Nº 162, [en ligne] 1er août 2019, [consulté le 12 août 2020]

L'appréhension des règles de droit de l'Union Européenne nous permet notamment d'identifier le conflit pouvant se dresser. En effet, bien plus que de « pencher dans la balance de son pays » au regard de l'intérêt de la justice, la reconnaissance même d'un conflit de lois est en jeu le souligne le mémoire initialement soumis à la Cour suprême par le gouvernement américain et le professeur Théodore Christakis[44]. Ce texte concernait le caractère selon eux purement hypothétique d'un conflit de lois au regard des article 49(1)(d) et (e) du RGPD autorisant tout transfert de données personnelles nécessaires pour des raisons « importantes d'intérêt public » ou à la constatation, l'exercice ou défense de droits en justice.

Bien que la majorité des pays européens perçoivent le Cloud Act comme ne permettant pas d'assurer une protection suffisante au regard des conditions fixées bien trop souple, l'interprétation des dispositions du RGPD, notamment l'une, qui aurait permis de limiter le transfert des données dans un cadre plus légitime pour l'ensemble des gouvernements européens est aujourd'hui encore trop floue et in fine, incertaine.

Le RGPD a dressé une liste limitative de situations dans lesquelles des données à caractère personnel peuvent faire l'objet d'un transfert vers un pays tiers[45]. Il existe précisément cinq situations : une décision d'adéquation adoptée par la Commission qui constate que le pays tiers assure un niveau adéquat de protection[46], l'existence de garanties appropriées et la mise à disposition de droits opposables et de voies de droit effectives pour les personnes concernées par le traitement[47], l'existence d'une reconnaissance par l'autorité nationale de contrôle de règles d'entreprise contraignantes[48], un transfert fondé sur un accord international tel qu'un traité d'entraide judiciaire[49], et, enfin, toute série de dérogations spécifiques au regard d'un transfert justifié par des « motifs importants d'intérêt public ».

Au regard de l'article 45 du RGPD, le gouvernement américain lors de son contre-mémoire dans le cas de l'affaire Microsoft Incorp vs. United States (soumis ultérieurement au mémoire de la Commission européenne), a souhaité mettre en exergue l'exigence d'une décision d'adéquation en matière de transferts de données de certains fournisseurs et, en outre, son inclinaison à la conclusion d'un accord dans le cas d'enquêtes. Cependant, au vu de la dernière décision datant du 16 juillet 2020 de la Cour de Justice de l'Union Européenne[50], il est possible de douter de l'arrivée prochaine d'un tel accord. La seule hypothèse pouvant être la plus à même de s'appliquer se trouve prévue par l'article 49 du RGPD. En effet, l'article 49(1) énonce la possibilité d'un transfert dès lors que celui-

[44] CHRISTAKIS Théodore, « a communication aux autorités américaines de données sur la base du Cloud Act est-elle en conflit avec le règlement général sur la protection des données ? », *Revue critique de droit international privé* 2019/3 (N° 3), pages 695 à 707, [en ligne], [consulté le 11 août 2020].

[45] Comme l'énonce le professeur Régis Bismuth : « Le RGPD peut avoir une portée extraterritoriale car il a ainsi vocation à s'appliquer dans la situation où les données d'un américain vivant aux États-Unis et qui n'a jamais été en Europe sont stockées dans un serveur situé dans l'UE. Même dans ce cas, un prestataire tel que Facebook, Google ou Microsoft ne pourrait accéder à la demande des autorités américaines de transférer directement ces données sans contrevenir aux dispositions du RGPD. » Ainsi, un réel conflit de lois peut être envisageable dès lors que l'interprétation du RGPD fait l'objet de plus de clarté. En effet, même en cas d'un futur accord intergouvernemental avec les États-Unis, le manque de clarté notamment de l'article 49 du RGPD posera toujours problème.

[46] Article 45 du Règlement (UE) 2016/679

[47] Article 46 du Règlement (UE) 2016/679

[48] Article 47 du Règlement (UE) 2016/679

[49] Article 48 du Règlement (UE) 2016/679

[50] Cette décision a remis en cause la décision d'adéquation existant entre l'Union Européenne et les États-Unis

ci est « nécessaire pour des motifs importants d'intérêt public ». Cependant, la détermination de motifs importants d'intérêt public ne peut être établie de façon unilatérale par les autorités et juridictions américaines. En effet, il est précisé à l'article 49(4) du RGPD que le motif d'intérêt public doit être « reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis » c'est-à-dire au regard de l'intérêt public de l'Union européenne ou d'un État membre, non celui d'un pays tiers. Suite à l'interprétation faite par un groupe de travail sur l'article 29, le Comité européen de protection des données a notamment rappelé[51] que la dérogation d'intérêt public n'est pas soumise à la seule présence d'une enquête pénale en cours en vue de servir un intérêt public d'un pays tiers[52]. En outre, comme l'a rappelée la Commission Européenne, une priorité est accordée aux accords internationaux de coopération, d'entraide judiciaire et d'assistance mutuelle.

Malgré les tensions existantes entres les interprétations de la Commission européenne et du Comité européen et le manque d'une interprétation précise et claire de leurs parts des dispositions précitées, il peut être estimé, sans trop s'avancer, que le transfert de données personnelles à partir de l'Union européenne vers les États-Unis est impossible en cas de situations ne constituant pas un crime grave ou, en cas d'enquête pénale dont le critère de gravité du fait juridique reproché n'est pas reconnu en droit européen ou de l'État membre dont il est question.

En l'état actuel des choses, bien que le Cloud Act semble garantir la non-divulgation arbitraire de données personnelles depuis sa promulgation, l'absence d'interprétation claire du RGPD et d'une relation équilibrée entre les États-Unis et l'Union Européenne pose des difficultés pour conclure un accord intergouvernemental équitable.

Ainsi, il serait recommandé pour tout entreprise ou organisme français de recourir à un prestataire européen ou au moins, comme le recommande Stephan Hadinger, directeur des technologies chez Amazon web services[53], ainsi que le RGPD, de recourir à un chiffrement des données hébergées et de s'assurer, pour l'entreprise ou l'organisme prestataire, d'être le seul à détenir la clé de sécurité. En effet, le prestataire ne pourrait alors remettre au juge américain que des données chiffrées[54]. Dans le cas de la conclusion d'un contrat avec une entreprise américaine –notamment en raison du fait qu'il s'agirait du seul prestataire fournissant un service pleinement effectif et suffisant – il s'agit de l'unique « garde de fou » réel aux effets négatifs de Cloud Act. En effet, une clause introduite dans le contrat afin d'exiger du prestataire de garantir qu'il agirait systématiquement pour s'opposer à la communication des données, qu'il en assumerait l'entière charge procédurale et les entières conséquences, y compris à l'égard du RGPD, serait insuffisante pour prévenir toute possibilité de transférer les données ou de retour sur investissement en raison des conséquences que pourraient engendrer ledit transfert ordonné par les juridictions américaines.

[51] Lignes directrices 2/2018 sur les dérogations à l'article 49 du 2016/679, p. 5.
[52] Il s'agit d'un ancien groupe de travail
[53] Il s'agit d'un service notamment d'hébergement des données de santé ayant obtenu en janvier 2019 en France la certification HDS.
[54] MERCIER Anne-Laure, « Stephan Hadinger (AWS France) : "Un client optant pour un stockage en France a l'assurance que ses données y restent bien" », sur mindhealth [en ligne], publié le 28 mai 2019, [consulté le 31 juillet 2020].

Enfin, il est maintenant nécessaire de traiter de l'application de la législation américaine et européenne sur les données de santé. En effet, la politique de protection des données personnelles, bien que similaire sous certains aspects, soulève des questions différentes.

CHAPITRE I - LES ÉTATS-UNIS ET LA LOI HIPAA

Comme l'énonce l'HIPAA, les professionnels de la santé et leurs partenaires commerciaux ont le devoir de prendre des mesures raisonnables pour assurer la sécurité et la confidentialité des informations personnelles sur la santé. Cette loi sectorielle est la principale qui puisse s'appliquer aux partenariats entre les établissements de soins de santé et les prestataires de services de santé. Toutefois, avant de déterminer si cette loi est applicable à l'un ou aux deux acteurs susmentionnés, il est nécessaire d'identifier précisément si ces acteurs correspondent aux définitions des protagonistes sous l'égide de cette législation. En outre, les développeurs et éditeurs d'applications mobiles liées à la santé doivent prendre en considération, avant de commencer à distribuer leur application, la nécessité d'assurer une conformité aux lois en vigueur by design.

Enfin, d'autres lois et règlements fédéraux peuvent être applicables. Il est donc nécessaire de savoir laquelle ou lesquelles le sont.

Section 1- Une obligation de conformité générale en matière de données de santé

Visant à protéger la confidentialité des données de santé, la loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) ne s'applique qu'à certaines informations de santé détenues par certains types d'organisations. En effet, toutes les données de santé ne sont pas protégées par cette loi. L'HIPAA concerne les informations spécifiques sur la santé « qu'elles soient orales ou enregistrées sous quelque forme ou support que ce soit, qui [...] concernent la santé ou l'état physique ou mental passé, présent ou futur d'un individu »[55]. Ainsi, deux aspects principaux doivent être abordés : le champ d'application de la loi HIPAA et la manière de s'y conformer. Toute personne travaillant dans des domaines liés aux soins doit avoir une compréhension pratique du champ d'application de la loi HIPAA et de la manière dont celle-ci les affecte.

La première question que tout responsable de données et, d'une manière générale, tout professionnel de la conformité doit se poser est la suivante : « Cette loi s'applique-t-elle à nous ? » et, si c'est le cas, « Quelles sont les diverses étapes et exigences à respecter ? »

I- Les règles générales

Il convient ainsi d'étudier en profondeur les exigences imposées par la loi HIPPA c'est-à-dire le cadre législatif de cette loi, ainsi que les exigences de conformité principales à mettre en œuvre.

[55] CONGRES AMERICAIN, Loi sur la portabilité et la responsabilité de l'assurance maladie (Health Insurance Portability and Accountability Act), 1996

A. Le cadre législatif

L'HIPAA regroupe les organisations responsables de la protection des données de santé en trois catégories : les entités couvertes (*covered entities*), les associés (*business associates*) et les sous-traitants (*subcontractors*).[56]

L'HIPAA définit les données de santé (information de santé protégée ou *protected health information*) comme toute donnée sur la santé d'une personne, ses soins de santé et aussi le paiement qui est collectée et créée par une entité déterminée.[57] Elle s'applique à toute entité qui est un prestataire de soins de santé, un centre d'échange d'informations sur les soins de santé ou un régime d'assurance santé. Centers for Medicare & Medicaid Services (CMS)[58] fournit sur son site web un outil d'orientation sur les entités couvertes afin d'identifier plus facilement les personnes devant se conformer à l'HIPPA.

Premièrement, l'HIPAA réglemente l'activité des prestataires de soins de santé, mais uniquement ceux qui facturent par voie électronique certaines transactions administratives et financières comme les médecins, les psychologues, les maisons de retraite, les cliniques et les pharmacies. Plus précisément, la loi fédérale fait références aux prestataires de soins de santé et aux entités qui transmettent des transactions de couverture sous forme électronique. Étant donné que seules les entités couvertes qui facturent par voie électronique entrent dans le champ d'application de la loi HIPAA, il est nécessaire d'identifier plus précisément ce qu'une entité couverte n'est pas afin de déterminer lesquelles sont incluses.

Nous pouvons voir que, généralement, les prestataires de soins de santé offrant des services gratuits, tels que les cliniques gratuites, ou continuant à facturer en utilisant des dossiers papier, des fax et des envois postaux, ne seront pas soumis à l'HIPAA. Il doit s'agir d'une personne, d'une entreprise ou d'une agence qui fournit, facture ou reçoit un paiement pour des soins de santé dans le cours normal de ses activités et qui transmet ou envoie toute transaction couverte par voie électronique. En effet, le système de soins de santé des États-Unis diffère du système français. Comme le système américain n'est pas un système de santé publique, il n'existe pas de système d'assurance maladie général, c'est-à-dire de système de santé universel. Centrées sur la notion de « service », les entités publiques ou privées « achètent » des services de santé à des « prestataires ». Comme l'indique le Bureau pour la Science et la Technologie de l'Ambassade de France aux États-Unis : « Aux fins de la réglementation fédérale, un prestataire de soins de santé est défini comme un médecin ou un prestataire de services de santé (comme détaillé dans la section 1861(s) de la loi sur la sécurité sociale[59]) ou toute autre personne ou organisation qui fournit, facture ou est rémunérée pour une procédure de santé. Cette définition inclut, par exemple, les médecins, les pédiatres, les infirmières et les hôpitaux. » À cet égard, il existe un processus en huit étapes appelé processus de facturation médicale. Ce processus est utilisé pour s'assurer que le patient est éligible pour recevoir

[56] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, « HIPAA Administrative Simplification» [en ligne], mars 2013, p. 11-12.
[57] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, Texte du règlement de simplification administrative de l'HIPAA, mars 2013, p. 14.
[58] Un site web du gouvernement fédéral géré et payé par les centres américains pour les services Medicare et Medicaid.
[59] ADMINISTRATION DE LA SÉCURITÉ SOCIALE AMÉRICAINE, Title 18 U.S.C, Sect. 1861, Part. E, Sec. 1861, Compilation des lois sur la sécurité sociale [en ligne].

des services de la part du prestataire. Le processus de facturation médicale passe par l'enregistrement, l'établissement de la responsabilité financière pour la visite, l'enregistrement et le départ du patient, la vérification de la conformité du codage et de la facturation, la préparation et la transmission des demandes de remboursement, le suivi du payeur, la génération des déclarations ou des factures du patient, l'affectation des paiements du patient et l'organisation du recouvrement. Au cours du processus, certaines données personnelles seront transmises à différentes personnes : notamment l'émetteur de factures médicales, le codeur médical et le prestataire de soins de santé. Ensuite, toutes les entités couvertes doivent s'assurer que la facture est conforme aux normes de l'HIPPA qui établissent les normes de conformité de la facturation. En effet, sauf dans certaines circonstances, l'HIPPA exige que les entités couvertes soumettent leurs demandes de remboursement par voie électronique.[60]

Deuxièmement, l'HIPAA réglemente les centres d'échange d'informations sur les soins de santé. C'est le cas lorsque l'entreprise ou l'agence traite, ou facilite le traitement, des informations sur la santé d'un format ou d'un contenu non standard à un format ou un contenu standard, ou d'un format ou d'un contenu standard à un format ou un contenu non standard. De plus, l'entreprise ou l'agence doit remplir cette fonction pour une autre entité juridique. Plus précisément, elle exige que le destinataire du dossier personnel ne puisse pas être lié par les lois sur la protection de la vie privée à l'expéditeur grâce à un consentement conforme du patient. Ainsi, si un patient autorise un hôpital à partager ses dossiers médicaux personnels avec son employeur, celui-ci ne sera pas concerné par l'HIPAA car la loi ne couvre que les activités des entités visées. A contrario, les exigences de l'HIPAA s'appliquent aux partenaires commerciaux de la société de diffusion des dossiers ou de la société de logiciels de dossiers médicaux qui ont reçu des dossiers médicaux par une entité couverte. Au regard de l'HIPAA, un associé commercial est une personne ou une entreprise qui accède à des informations de santé protégées (PHI) dans le cadre de sa collaboration avec une entité couverte ou de la fourniture de services à celle-ci. Les associés commerciaux d'une entité peuvent inclure un transcripteur médical, un consultant qui effectue une révision de l'utilisation pour un hôpital ou un cabinet comptable qui vérifie le plan de santé d'une entreprise. En effet, si « une entité couverte engage un associé pour l'aider à mener à bien ses activités et fonctions de soins de santé », l'HIPAA exige un contrat écrit « qui établit spécifiquement ce que l'associé a été engagé pour faire et exige que l'associé se conforme à l'HIPAA ».[61]

En outre, le sous-traitant, c'est-à-dire une personne ou une entreprise qui a accès aux données de santé tout en travaillant avec le *business associate* ou lui fournissant des services, est soumis à la loi HIPAA. Il s'agit par exemple, d'une société locale de services informatiques d'un transcripteur médical. A contrario, un cabinet d'experts-comptables, business associate d'une covered entity, louent des services de stockage de données à un tiers, le sous-traitant. [62]

Enfin, l'HIPAA réglemente les plans de santé ou exactement, les plans de prestations privées et certains programmes financés par le gouvernement. On parle de régime privé de prestations lorsque le régime est un régime de santé individuel ou collectif, ou une combinaison des deux, qui fournit ou

[60] HigherEducation, « The Medical Billing Process », sur MB&CC [en ligne], [consulté le 20 juillet 2020].

[61] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « Covered Entities and Business Associates », [en ligne], publié le 16 juin 2017, [consulté le 27 août 2020]

[62] Un expert-comptable (CPA) est un professionnel de la comptabilité qui a réussi l'examen uniforme de CPA. La désignation CPA est une certification d'expertise dans le domaine de la comptabilité.

paie le coût des soins médicaux. Les plans de santé comprennent : les compagnies d'assurance maladie, les organismes de maintien de la santé (Health Maintenance Organizations ou HMO), les plans de santé financés par l'employeur et les programmes gouvernementaux qui paient les soins de santé, comme Medicare, Medicaid, ainsi que les programmes de santé des militaires et des vétérans. Afin de déterminer plus facilement si un plan de santé est considéré comme une entité couverte, il convient de se référer aux diagrammes de l'annexe 3.[6364]

Lorsqu'une entité couverte (dans notre cas l'établissement de santé) engage les services d'un fournisseur de services dans le nuage (cloud services provider ou CSP) pour créer, recevoir, maintenir ou transmettre des ePHI (comme pour traiter et/ou stocker des ePHI) en son nom, le CSP est un *business associate* au sens de l'HIPAA[65].

Une fois que l'organisation sait que l'HIPAA s'applique à elle, la question suivante peut se poser : « La loi établit-elle des règles clés qui doivent être suivies en premier lieu ? ». L'HIPPA a établi trois règles principales qui protègent la vie privée et la sécurité des PHI : Privacy Rule en décembre 2000 et modifiée en août 2002, Security Rule en février 2003 et Enforcement Rule en avril 2003 et octobre 2009.

L'HIPAA Privacy Rule établit des normes nationales afin de donner des droits spécifiques concernant la protection des informations de santé identifiables individuellement et concerne spécifiquement la confidentialité des données. Elle réglemente également les personnes qui peuvent avoir accès à ces informations de santé - les trois types d'entités couvertes déjà vues précédemment - et oblige les entités couvertes et leurs associés à se conformer à la protection de leurs informations.

L'HIPPA Security Rule fixe les normes nationales de protection des informations de santé transmises ou stockées sous forme électronique, plus précisément, la confidentialité, l'intégrité et la disponibilité des informations de santé électroniques afin de garantir la sécurité.

L'HIPPA Enforcement Rule quant à elle fournit des normes pour toutes les règles de simplification administrative au regard de l'Administrative Simplification Rules. Elle met en place des procédures d'enquête sur toute violation potentielle détectée, des procédures d'audition et l'imposition de sanctions pour aider à faire respecter les règles.

Afin de compléter ces règles, l'HIPPA est suivie par des lois qui se rapportent à la règle de confidentialité et de sécurité. Il s'agit de la loi sur les technologies de l'information en matière de santé pour la santé économique et clinique (Health Information Technology for Economic and Clinical Health Act ou HITECH) de 2009 qui étend la responsabilité des partenaires commerciaux et qui a révisé les sanctions pour violation des règlements de l'HIPPA, ainsi que la loi sur la non-discrimination en matière d'information génétique (Genetic Information Non-discrimination Act ou GINA) de 21 mai 2008 se concentrant sur l'information génétique des personnes afin de les protéger contre la discrimination fondée sur leur information génétique spécifiquement dans l'emploi et la

[63] Il s'agit d'un résumé schématique des "Directives sur les entités couvertes" établi pour cette carte de visite.
[64] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « Guide de normes de simplification administrative adoptées par le HHS en vertu de la loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) », [en ligne], [consulté le 20 février 2020].
[65] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « May a HIPAA covered entity or business associate use a cloud service to store or process ePHI? », [en ligne], publié le 6 octobre 2016 sur hhs.gov, [consulté le 25 juin 2020].

couverture santé. Enfin, la règle omnibus a mis en œuvre un certain nombre de dispositions de la réglementation de l'HIPAA sur la vie privée et la sécurité par l'intégration de HITECH et a créé des changements pour la GINA.

La règle de notification des violations de l'HIPAA établit une obligation pour les entités couvertes et leurs associés commerciaux de fournir une notification à la suite d'une violation d'informations médicales protégées non sécurisées.

Le maintien de ces règles est la première étape pour toute organisation qui souhaite adopter des processus et des procédures visant à garantir le plus haut degré de confidentialité et de sécurité des dossiers médicaux des personnes.

B. Les exigences de conformité principales : sécurité et confidentialité

Comme cela a été affirmé précédemment, le respect des règles principales susvisées est la première étape pour toute organisation qui souhaite adopter des processus et des procédures visant à garantir le plus haut degré de confidentialité et de sécurité des dossiers médicaux des patients. Par conséquent, il convient de se pencher sur les principales normes de sécurité de l'HIPAA qui doivent être mises en œuvre par les entités visées au sein de cette étude.

La règle de sécurité intitulée "Security Standards for the Protection of Electronic Protected Health Information" énonce, au 45 CFR Part 160 et Part 164, sous-parties A, C et E, les dispositions de l'HIPAA concernant les normes de sécurité. Avant l'entrée en vigueur de l'HIPAA, aucun ensemble de normes de sécurité ou d'exigences générales pour la protection des informations de santé n'existait dans le secteur des soins de santé. Cela fut rendu indispensables compte tenu de toutes les nouvelles applications basées sur le web et autres "portails" qui donnent aux médecins, aux infirmières, au personnel médical ainsi qu'aux employés administratifs un accès plus large aux informations de santé électroniques. En effet, permettant au personnel médical une plus grande mobilité et efficacité dans le traitement des soins (ainsi, les médecins peuvent vérifier les dossiers des patients et les résultats des tests où qu'ils se trouvent), l'augmentation du taux d'adoption de ces technologies créée une augmentation des risques potentiels pour la sécurité. Outre, la règle de sécurité, celle de confidentialité exige des garanties administratives, physiques et techniques appropriées. Il existe une complémentarité entre les deux règles, mais aussi des distinctions primaires. Lorsque la règle de sécurité (HIPPA Security Rule) ne couvre que les informations personnelles sous forme électronique, la règle de confidentialité (HIPPA Confidentiality Rule) s'applique à toutes les formes d'informations personnelles. Il faut donc se concentrer, au sein de cette étude, sur les normes imposées par la règle de sécurité.

En premier lieu, chaque entité doit tenir compte de l'importance des garanties **administratives** afin d'établir une protection adéquate des données relatives à la santé. En effet, le respect de la règle de sécurité doit primer sur toute autre mesure par la mise en place de garanties administratives raisonnables et appropriées afin d'établir les bases du programme de sécurité de chaque *covered entity*. Ces garanties administratives sont notamment inscrites au §164.308. Dans un premier temps, il est nécessaire d'établir plus précisément ce qui constitue une mesure de protection administrative : il

s'agit de "mesures, politiques et procédures administratives visant à gérer la sélection, l'élaboration, la mise en œuvre et le maintien de mesures de sécurité pour protéger les informations de santé électroniques protégées et à gérer la conduite du personnel de la *covered entity* en ce qui concerne la protection de ces informations". Ainsi, au vu de cette définition, il est possible de déduire à juste titre qu'il est essentiel de procéder à une évaluation du contrôle de sécurité déjà en place afin d'établir, dans un deuxième temps, une analyse des risques potentiels, par type de gravité et, enfin, une série de solutions documentées en ce qui concerne les différents facteurs et risques de l'entité spécifique. En effet, il est primordial d'établir une protection adéquate by design mais aussi périodiquement afin de garantir l'efficacité des environnements opérationnels. En outre, en ce qui concerne le §164.308(a)(2), il est nécessaire de désigner une personne responsable de l'élaboration et de la mise en œuvre des politiques et des procédures requises par la règle de sécurité[66]. De plus, l'entité doit établir une liste des personnes et entités ayant accès aux systèmes. Plus précisément, l'entité doit mettre en place des politiques et des procédures appropriées pour garantir un accès approprié aux membres du personnel. Cette norme, appelée "sécurité du personnel", est directement liée à la "norme de gestion de l'accès aux données" qui exige la mise en œuvre d'un accès restreint aux seules personnes et entités qui ont besoin d'un accès. Comme l'explique le CMS : "En mettant en œuvre cette norme, le risque de divulgation, d'altération ou de destruction inappropriée de l'e-PHI est minimisé[67]". Ainsi, en ce qui concerne le 45 CFR §§ 164.308(a)(1)(ii)(A), avant que les services de cloud computing - dans le cas d'une application de "fourniture de services SaaS" - puissent être utilisés par les établissements de santé, les *covered entity* doivent s'assurer que les services sont sécurisés. Pour ce faire, il est obligatoire de réaliser une analyse d'impact. Enfin, la règle de sécurité prévoit d'autres types de garanties nécessaires, telles que l'administration des contrats d'associés, le plan d'urgence [68] [69] [70], la sensibilisation et la formation à la sécurité [71] [72] ou les procédures en cas d'incident de sécurité.

Deuxièmement, il est nécessaire de mettre en œuvre des systèmes, des équipements et des installations afin de garantir la sécurité. Ensuite, comme l'indique le 45 C.F.R, §164.304 de l'HIPPA Security Rule, il s'agit de "toutes les mesures physiques, politiques et procédures visant à protéger les systèmes d'information électroniques d'une *covered entity*, ainsi que les bâtiments et équipements connexes, contre les risques naturels et environnementaux et les intrusions non autorisées". Il existe quatre normes dans le cadre des garanties **physiques** : les contrôles d'accès aux installations, l'utilisation des postes de travail, la sécurité des postes de travail et les contrôles des dispositifs et des supports. Tout d'abord, le § 164.310(a)(1) de l'HIPAA Security Rule exige des entités visées qu'elles "mettent en œuvre des politiques et des procédures pour limiter l'accès physique à leurs systèmes d'information électroniques [...] (et s'assurent) que [...] l'accès autorisé est autorisé. Les normes de contrôle d'accès aux installations demandent une phase de mise en œuvre spécifique : des opérations d'urgence avec des entités de mesures de sécurité physique, un plan de sécurité des installations afin de documenter et de définir les garanties utilisées, un contrôle d'accès et des procédures de validation

[66] Il s'agit de la norme d'évaluation du paragraphe §164.308(a)(8) de la règle de sécurité
[67] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « Security Standards: Administrative Safeguards Security », *HIPAA Security SERIES* [en ligne], 2005, Vol. 2, p. 11, [consulté le 20 février 2020].
[68] Security Rule, §164.308(b)(1)
[69] Nous apporterons plus de précisions à ce sujet
[70] Security Rule, §164.308(a)(7)
[71] Security Rule, §164.308(a)(5)
[72] Security Rule, §164.308(a)(6)

et enfin, des registres de maintenance afin de "documenter les réparations et les modifications des composants physiques d'une installation qui sont liés à la sécurité (par exemple, le matériel, les murs, les portes et les serrures)". Ensuite, le §164.310(b) exige l'utilisation des postes de travail. Un poste de travail est défini comme "un dispositif informatique électronique, par exemple, un ordinateur portable ou de bureau, ou tout autre dispositif qui remplit des fonctions similaires, et des supports électroniques stockés dans son environnement immédiat". En outre, le §164.310(c) exige la sécurité du poste de travail. Il est nécessaire de "mettre en œuvre des mesures de protection physique pour tous les postes de travail qui accèdent à des informations de santé protégées électroniquement, afin de limiter l'accès aux utilisateurs autorisés". Enfin, le §164.310(d)(1) exige le contrôle des dispositifs et des supports : "mettre en œuvre des politiques et des procédures qui régissent la réception et le retrait du matériel et des supports électroniques qui contiennent des informations de santé protégées électroniquement, à l'entrée et à la sortie d'un établissement, ainsi que le déplacement de ces éléments à l'intérieur de l'établissement". Lorsque les entités couvertes se débarrassent de tout stockage électronique contenant l'e-PHI, elles doivent s'assurer qu'il est inutilisable et si possible inaccessible et, au lieu de se débarrasser des dispositifs médicaux électroniques, les entités couvertes qui le réutilisent ont l'obligation de retirer préalablement les e-PHI des supports électroniques.

Enfin, en raison des progrès technologiques dans le secteur des soins de santé, les risques internes et externes sont accrus en ce qui concerne la protection des PHI. Des garanties **techniques sont** donc nécessaires. Le 45 CFR §164.306(b) exige une approche flexible et neutre dans la sélection des solutions technologiques et autres mesures de sécurité. En effet, l'analyse et la gestion des risques doivent prendre en considération tous les facteurs et particularités du traitement afin de sélectionner des technologies et mesures raisonnables et appropriées. C'est précisément la raison pour laquelle la règle de sécurité n'exige pas de solutions technologiques spécifiques. Les mesures de sécurité doivent inclure un contrôle d'accès par "des systèmes d'information électroniques qui conservent des informations médicales protégées électroniquement afin de ne permettre l'accès qu'aux personnes ou aux logiciels auxquels ont été accordés des droits d'accès tels que spécifiés au §164.308(a)(4)"[73]. Il s'agit du principe du "minimum nécessaire" : les utilisateurs autorisés n'auront accès qu'aux informations minimales nécessaires à l'exercice de leurs fonctions. Cela exige une identification unique de l'utilisateur[74][75] et, une procédure d'accès d'urgence. En outre, les garanties techniques impliquent des contrôles d'audit, précisément, il s'agit de "matériel, logiciel et/ou mécanismes procéduraux qui enregistrent et examinent l'activité dans les systèmes d'information qui contiennent ou utilisent des informations de santé électroniques protégées"[76] et que "la propriété de ces données ou informations n'a pas été altérée ou détruite de manière non autorisée" au §164.304.[77] Enfin, la norme de sécurité de transmission exige que l'entité couverte "mette en œuvre des mesures de sécurité techniques pour se prémunir contre l'accès non autorisé à des informations de santé électroniques protégées qui sont transmises sur un réseau de communications électroniques" (§164.312(e)(1) et, la norme d'authentification de la personne ou de l'entité, nécessite la mise en œuvre de procédures pour

[73] Security rule §164.312(a)(1)
[74] Security rule §164.312(a)(2)(i)
[75] Security rule §164.312(a)(2)(ii)
[76] Security rule §164.312(b)
[77] Security rule §164.312(c)(1)

vérifier "qu'une personne ou une entité cherchant à accéder à des informations de santé électroniques protégées est bien celle qui demande l'accès" (§164.312(d)).

Il est maintenant nécessaire de répondre à quelques questions clés : Les *covered entity* doivent-elles conclure des accords spéciaux avant de partager les informations sur les patients ? Quels renseignements médicaux personnels les entités couvertes peuvent-elles partager sans le consentement du patient ? Quels sont les droits des patients en ce qui concerne leurs renseignements médicaux personnels ? Cette argumentation sera abordée à travers le champ d'application de l'HIPPA Confidentiality Rule. En effet, la règle de confidentialité créée des normes spécifiques pour protéger les informations des patients et, parce que les informations des patients continuent à évoluer, les entités couvertes doivent suivre des directives strictes afin de protéger la réputation de l'établissement de santé et les informations des patients.

Afin de se conformer à l'HIPPA Confidentiality Rule, les praticiens doivent avoir des procédures et des politiques internes spécifiques pour contrôler, protéger et divulguer correctement les PHI. La règle de confidentialité exige que les entités couvertes élaborent et distribuent un avis spécifique appelé "avis de politique de confidentialité" (Notice of Privacy Practices ou NPP). En effet, en vertu d'un principe clé d'équité dans l'information, toute personne a le droit de savoir quelles informations personnelles sont collectées, partagées et protégées, la raison de ce traitement et par qui. L'avis doit décrire comment les informations sur la santé peuvent être utilisées et divulguées. En règle générale, le patient doit autoriser toute divulgation de ses PHI, y compris les informations de santé identifiables individuellement. Il doit également rappeler le droit d'une personne à la portabilité de ses données de santé et son droit de se plaindre si elle estime que son droit à la vie privée a été violé et comment contacter l'entité couverte pour obtenir plus d'informations et déposer une plainte. Toutefois, il n'est pas conçu pour interférer avec le traitement des patients et toutes les informations relatives au traitement, au paiement et aux opérations de soins de santé (to treatment, payment and healthcare operations ou TPO) peuvent être discutées et partagées librement pour traiter le patient, se faire payer et effectuer des opérations de soins de santé de routine. L'exigence de notification de l'HIPPA couvre toutes les diligences imposées par l'HIPAA que les entités couvertes doivent respecter. Plus de 20 éléments requis doivent figurer dans une notice de confidentialité.

Le département de la santé et des services sociaux, l'Office des droits civils (Office for Civil Rights ou OCR) et le bureau du coordinateur national des technologies de l'information en matière de santé (Office of the National Coordinator for Health Information Technology ou ONC) ont élaboré des modèles de NPP pour aider à améliorer l'expérience et la compréhension des patients[78]. Afin de faciliter la compréhension pratique, il convient de se concentrer sur l'aspect pratique de la mise en œuvre de l'avis. Les principaux droits à la vie privée des patients que toute entité couverte doit connaître sont résumés à l'annexe 2.[79]

[78] BUREAU DES DROITS CIVILS, DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN « MODEL NOTICES OF PRIVACY PRACTICES QUESTIONS AND INSTRUCTIONS », [en ligne], 2014 , [consulté le 20 février 2020] et « MODEL : Your Information. Your Rights. Our Responsibilities », [en ligne], 2014, [consulté le 20 février 2020].

[79] BUREAU DES DROITS CIVILS, DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « OCR PRIVACY BRIEF, SUMMARY OF THE HIPAA PRIVACY RULE », [en ligne], 2003, p. 11-13, [consulté le 20 février 2020].

L'HIPPA exige que le NPP soit mis à la disposition des patients sur le lieu de prestation de services, sur demande, et qu'il soit affiché sur un tableau d'affichage où les patients peuvent le voir. En outre, les établissements de santé fournissent généralement leur NPP aux patients lors de leur première visite et les patients sont alors tenus de signer un accusé de réception de l'avis comme preuve qu'il a été fourni. S'ils refusent de signer, la *covered entity* doit consigner ce refus dans le dossier du patient. Si l'entité couverte gère un site web qui décrit ses services, l'HIPPA exige qu'elle affiche l'avis. Enfin, pour les payeurs, il est essentiel d'envoyer un courriel tous les trois ans afin de diffuser l'avis.

Au-delà des règles générales en matière de données de santé, comme il a été vu précédemment, la loi HIPAA s'applique aux *covered entities* et *business associates*. Dans le cas d'un partenariat entre un établissement de santé et un éditeur de solution digitale de suivi médical, la question de l'hébergement de ces données par le *business associate* se pose. Autrement dit, que celui-ci les héberge sur ses propres serveurs ou recours à un fournisseur, quelles sont les exigences américaines en cas d'hébergement de donnés de santé au regard de la loi HIPAA ?

II- L'application de la loi HIPAA en matière d'hébergement de données de santé

Les prestataires d'hébergement ont l'obligation se conformer aussi bien à la loi HIPAA qu'à la loi HITECH. Ensemble, ces deux textes énoncent l'ensemble des exigences en matière de protection des données de santé. Ainsi toute entité soumise à ces textes a l'obligation de prendre en considération l'utilisation qu'il compte faire d'un cloud dès lors qu'un tel service sera souscrit.

Les lois HIPPA et HITECH sanctionnent sévèrement tout défaut de conformité en matière notamment de partage des dossiers médicaux électroniques. En effet, sous peine de subir une amende pouvant s'élever jusqu'à 1,5 millions de dollars et le risque d'être considéré comme responsable civilement, il convient de s'assurer de la protection des données et de la sécurité du service proposé.

La loi HIPAA considère les prestataires d'hébergement comme des partenaires commerciaux. Ainsi, il revient aux fournisseurs de service d'hébergement de données de fournir des solutions prenant en considération au sein de leur mise en conformité la loi HIPAA bien que celle-ci ne prévoit pas d'exigences spécifiques. En effet, chaque fournisseur de service d'hébergement est considéré comme responsable de la conformité des prestations proposés et doit rendre tout compte de celle-ci auprès du Département de la Santé et des Services sociaux des États-Unis. Ainsi, le département a mis en place un système d'audit concernant certains de ces fournisseurs et, garanti au regard de la loi HITECH une indemnisation en cas de démonstration de pratiques suffisantes concernant la protection des données des dossiers de santé électroniques.

Avant le choix du prestataire, il convient avant tout de choisir le type de d'hébergement. En effet, il existe plusieurs formes d'hébergement. Une distinction doit dans un premier temps être opéré entre l'hébergement locale et l'hébergement cloud.

L'hébergement locale consiste à ce que l'ensemble des données soient hébergées au sein de l'entreprise même, permettant un meilleur contrôle d'accès aux données et la possibilité de mettre en

place un système de protection interne confidentiel. Toutefois, ce type d'hébergement ne convient pas toujours à l'ensemble des finalités que demande cet hébergement. En effet, les données ne peuvent être ici qu'uniquement accessibles au sein de l'entreprise et peut, en cas de sinistre, entraîner une perte totale de l'ensemble des données pour un coût d'investissements de départ mais aussi de maintenance importante.

A l'inverse, l'hébergement Cloud consiste à ce que l'ensemble des données soient hébergées sur le datacenter du prestataire. Ainsi, les données sont accessibles depuis n'importe quel terminal via une connexion internet, offrant ainsi une possibilité de partage. Dans le cas présent, ce type d'hébergement est requis.

Malgré que la loi HIPAA ne prévoit aucune exigence supplémentaire en matière d'hébergement, un guide est mis à la disposition des justiciables afin d'appréhender le rôle et les responsabilités de chacun. En effet, face à la prolifération et adoption massive par les entreprises de solutions de cloud computing[80], les *covered entities* ainsi que les *business associates* ont questionné le Département de la Santé et des Services sociaux en matière de conformités dans le cadre de données de santé. Au regard de la présente étude, l'intérêt se portant sur les ressources cloud offertes par un fournisseur de prestation cloud en tant qu'entité juridiquement distincte de la *covered entity* ou de *business associate* envisageant l'utilisation de ses services, ce guide[81] est d'une utilité première. En effet, le Département par celui-ci a cherché à répondre aux différentes interrogations pouvant être posées par les *covered entities* et les partenaires commerciaux. Étant des hébergeurs, les prestataires de solutions de cloud computing sont considérés comme des partenaires commerciaux dès lors qu'un partenaire commercial lié à une *covered entity* ou que la *covered entity* elle-même fait appel à ses services pour créer, recevoir, maintenir ou transmettre les données de santé en son nom. Étant alors considéré comme un *business associate*, le prestataire a l'obligation de conclure un accord de partenariat commercial conformément à la loi HIPAA. Dans ce sens, le Département de la Santé et des Services sociaux rappelle que le chiffrement des données de santé et l'absence de détention de la clé de chiffrement par le prestataire ne peuvent l'exempter de ses obligations. Ainsi, le fournisseur de service est à la fois contractuellement responsable du respect des termes de l'accord et directement responsable du respect des exigences applicables en vertu de la loi HIPAA et HITECH.

Ainsi, l'accord d'association d'entreprises doit permettre d'établir l'ensemble des utilisations et divulgations des données de santé que pourra exercer en vertu du contrat mais aussi requis par la loi, le partenaire commercial/prestataire de solutions cloud pour le compte du partenaire commercial ou de la *covered entity*. En outre, il devra être prévu l'ensemble des exigences revenant à la charge du fournisseur du service cloud en matière de sécurité : plus précisément les mesures de protection appropriées afin d'empêcher toute utilisation ou divulgation non autorisée et d'en communiquer auprès des autres parties y compris les incidents constituant une violation de données de santé n'ayant pas fait l'objet d'une procédure de sécurité. De plus, celui-ci devra respecter toute communication auprès d'une personne concernée par le traitement en raison de l'obligation revenant au partenaire commercial et à la *covered entity*, de répondre aux demandes des personnes concernées en vertu des

[80] Il s'agit d'une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée.
[81] DEPARTEMENT DE LA SANTÉ ET DES SERVICES SOCIAUX AMÉRICAIN, « Guidance on HIPAA & Cloud Computing », sur HHS.gov [en ligne], publié le 16 juin 2017, [consulté le 7 mars 2020].

droits qu'ils leur sont reconnus[82]. Dès lors qu'une demande émanera du Département de la Santé et des Services sociaux des États-Unis, le partenaire commercial devra mettre à disposition l'ensemble des documents permettant de démontrer la conformité du traitement. En cas de résiliation, le fournisseur de solutions cloud aura l'obligation de retourner ou de détruire les données ayant fait l'objet de l'hébergement. Enfin, tout contrat de sous-traitance devra être conclu sous les mêmes restrictions et conditions que le contrat de sous-traitance.

Au-delà des obligations incombant au prestataire de solution cloud en vertu de ses relations contractuelles avec un partenaire commercial ou une *covered entity*, celui-ci devra respecter les obligations mises à sa charge au regard de la loi HIPAA et de la loi HITECH. Ainsi, celui-ci devra mener sa propre analyse des risques et établir ses propres politiques de gestion des risques en vertu des articles suivants : 45 CFR §§ 164.308 (a) (1) (ii) (A), 164,308 (a) (1) (ii) (B) et 164.502. Après avoir étudié de façon succincte les exigences devant être intégrées au sein de l'accord, une question fondamentale en termes de stratégie doit être posée : en cas de défaut de résolution d'un accord entre la *covered entity*/*business associate* et le prestataire de solutions cloud, bien qu'il s'agisse d'un défaut d'application de la loi HIPAA, existe-il des remèdes afin de contre carrer toutes sanctions futures ? En effet, le bureau des droits civils américains prévoit qu'en cas d'infraction des article 45 CFR §164.308(b)(1) et §164.502(e) un accord de résolution et un plan de mesures correctives peut être conclu. Cependant, il convient de rappeler que sa propre dénonciation n'entraînera pas une annulation de l'ensemble des sommes devant être réglées auprès du ministère, mais aura pour finalité de les « limiter ». Cette constatation peut notamment être fait au regard de nombreuses enquêtes du bureau des droits civils ayant constatés des violations affectant des milliers de personnes au sein de plusieurs entreprises. On peut le constater par le biais de l'Université de santé et de science de l'Oregon (OHSU) ayant fait l'objet d'une enquête révélant en 2016 des preuves de vulnérabilités généralisées au sein du programme de conformité HIPAA, « y compris le stockage des informations de santé électroniques protégées (ePHI) de plus de 3000 personnes sur un serveur cloud sans accord d'associé commercial ». L'OCR avait « constaté un risque important de préjudice pour 1 361 de ces personnes en raison de la nature sensible de leurs diagnostics ».[83]

En outre, comme le recommande le ministère de la Santé et des Services sociaux, un accord de niveau de service peut être opportun au regard des attentes commerciales des parties mais aussi d'une conformité pertinente avec la loi HIPAA et l'accord d'association d'entreprise. Notamment, au regard des articles 45 CFR §§ 164.308 (b) (3), 164.502 (e) (2) et 164.504 (e) (1), les termes fixés par le contrat SLA ne doivent pas aboutir à une impossibilité pour la *covered entity* ou le *business associate* d'accéder aux données de santé. Les exigences contractuelles en matière de SLA étant similaires en droit américain et en droit français, il conviendra pour des raisons de cohérence de traiter en détail ces exigences au sein de la partie « droit français » afin de nous focaliser sur d'autres aspects pratiques au sein de la partie « droit américain ».

Enfin, au regard des obligations lui incombant, il est recommandé aux *covered entities et business associates* de rendre les informations de santé protégées non sécurisées inutilisables, illisibles ou

[82] 45 CFR § 164.504 (e) (2) (ii) (E) - (G)

[83] Se référer notamment à l'accord de résolution conclut avec le Département de santé et services sociaux des États-Unis ainsi qu'au communiqué de presse du gouvernement.

indéchiffrables pour des personnes non habilitées. Au regard de l'article 45 CFR 164.304, l'Institut national des normes et de la technologie (NIST) a identifié comme conforme deux processus répondant à la règle de sécurité de la loi HIPAA par « l'utilisation d'un processus algorithmique pour transformer les données en une forme dans laquelle il y a une faible probabilité d'attribuer un sens sans l'utilisation d'un processus ou d'une clé confidentiels » c'est-à-dire un cryptage. Il s'agit donc de tout processus s'inscrivant dans la norme SP 800-111 (Guide des technologies de chiffrement du stockage pour les périphériques des utilisateurs finaux[84]) ou SP 800-52 en matière de données en mouvement et de normes fédérales FIPS 140-2.

Enfin, la loi HIPPA autorise tout *covered entity* ou *business associate* d'utiliser une solution de cloud computing d'un prestataire stockant les données de santé en dehors des États-Unis cela sous conditions de conclusion d'un accord d'association d'entreprise et du respect des règles de la loi HIPAA.

Ainsi, après avoir détaillé l'ensemble des règles devant être prise en compte au regard de la loi HIPPA lors de la conclusion d'un partenariat entre un hôpital et un service de solution digitale de suivi médical, il convient d'en étudier leur application à notre cas spécifique.

Section 2- L'application de la réglementation en matière de partenariats entre hôpitaux et service de solution digitale de suivi médical

Au sein des partenariats entres les établissements de santé et les éditeurs de solutions digitales, l'éditeur peut être envisagé comme un partenaire commercial. Toutefois, selon la loi HIPAA, ce partenaire est-il considéré comme un partenaire commercial, un tiers ou une entité couverte ? Deuxièmement, quelles sont les lois et lesquelles s'appliquent à cette application mobile de santé spécifique ?

En effet, il convient d'énoncer de façon exhaustives les différentes législations afférentes aux applications mobiles dans le secteur des données de santé et, in fine, d'identifier lesquelles sont applicables afin d'en tirer les conséquences pratiques à mettre en place telles que les mesures de confidentialité et de sécurité ou les obligations de contractualisation et le formalisme contractuel dans le cadre de ce type de partenariat. La rédaction d'un accord d'association d'entreprise mais aussi la souscription d'un contrat cloud computing d'hébergements privé des données sont nécessaires.

I- Les exigences de conformité principales en matière d'applications de données de santé

Les développeurs d'applications mobiles liées à la santé doivent prendre en considération, pour commencer à distribuer leur application, la nécessité d'intégrer la conformité dès la conception. En effet, des lois et règlements fédéraux pourraient s'appliquer à eux. Tout d'abord, il est nécessaire de déterminer laquelle ou lesquelles sont applicables : la loi FTC, la règle de notification des violations de la santé édictée par la FTC (Federal Trade Commission ou Commission fédérale du commerce),

[84] SCARFORNE Karen, SOUPPAYA Murugiah, SEXTON Matthew, « Guide to Storage Encryption Technologies for End User Devices », sur CSRC [en ligne], publié en novembre 2007, [consulté le 25 mars 2020].

la loi sur la portabilité et/ou la responsabilité de l'assurance maladie et les lois fédérales sur les aliments, les médicaments et les cosmétiques (Federal Food, Drug and Cosmetics Acts ou FD&C Act). Tout d'abord, la FDA applique la loi FD&C, qui réglemente la sécurité et l'efficacité des dispositifs médicaux, y compris certaines applications médicales mobiles. La FDA concentre sa surveillance réglementaire sur un petit sous-ensemble d'applications médicales qui présentent un risque plus élevé si elles ne fonctionnent pas comme prévu. Deuxièmement, la Commission fédérale du commerce applique la loi FTC, qui interdit les actes ou pratiques trompeurs ou déloyaux dans ou affectant le commerce, y compris ceux relatifs à la vie privée et à la sécurité des données, et ceux impliquant des allégations fausses ou trompeuses sur la sécurité ou les performances des applications. Enfin, la règle de notification des violations de la santé de la loi FTC exige de certaines entreprises qu'elles fournissent des notifications à la suite de violations des informations contenues dans les dossiers médicaux personnels.

En particulier, il est important de noter que plusieurs réglementations peuvent être applicables et, par conséquent, l'étude des données de santé des partenariats ne peut pas couvrir uniquement le spectre de l'HIPPA. En raison de la complexité de ces lois et règlements fédéraux, la Commission fédérale du commerce a créé un nouvel outil en ligne pour rassembler les différentes caractéristiques transcendantes de chacun d'entre eux. En collaboration avec l'OCR, le Bureau du coordinateur national des technologies de l'information sur la santé (ONC) du HHS et la Food and Drug Administration (FDA), l'outil d'orientation a été créé afin de prendre en compte les réponses des développeurs aux questions et leur indiquera des informations détaillées sur certaines lois fédérales qui pourraient s'appliquer à la demande. Les juristes, les responsables des données et les professionnels de la conformité doivent recueillir avec soin des informations suffisantes sur la nature de l'application, notamment sur sa fonction, les données qu'elle collecte et les services qu'elle fournit aux utilisateurs, afin de pouvoir répondre avec précision aux différentes questions. Ces informations permettront d'établir le scénario, le profil type de l'application et donc la nature de l'entité, le type de risques et la responsabilité.

A) Les applications de suivi médical au titre de l'HIPAA

La confidentialité des informations sur la santé et, en fin de compte, des données sur la santé est établie par l'**HIPAA**. Précisément, la loi fait référence aux informations « orales ou enregistrées sous quelque forme ou support que ce soit, qui [...] concernent la santé ou l'état physique ou mental passé, présent ou futur d'un individu », c'est-à-dire les informations de santé identifiables. Il peut s'agir d'informations relatives à la santé, par exemple, des données démographiques, du paiement pour la fourniture de soins de santé, de l'adresse IP du consommateur ou, d'une manière générale, de toute information/donnée dont on peut raisonnablement penser qu'elle peut être utilisée pour identifier le consommateur. Ainsi, il est d'abord nécessaire de connaître la nature de ces données de santé. Pour ce faire, il faut rappeler plus précisément quel type de service offre la société qui développe l'application, et, à qui. Comme indiqué dans l'introduction, il s'agit d'une solution numérique pour le suivi médical. Cela permet d'individualiser les soins de manière plus opérationnelle. Elle permet aux établissements de santé de superviser une multitude de parcours de patients, que les soins soient médicaux, chirurgicaux ou obstétricaux. À tout moment, les patients et les professionnels de la santé

peuvent échanger pour des besoins spécifiques, envoyer des documents, des photos ou des vidéos via un système de messagerie sécurisé. Toutes les données relatives à la santé sont hébergées. En outre, selon les choix de l'éditeur, l'application santé peut avoir une multitude de fonctionnalités : questionnaires de suivi, conseils personnalisés, questionnaires d'urgence, prise de constantes, alertes, traitement des alertes et historique. Compte tenu de toutes ces informations, il peut être conclu que le type d'application de santé crée, reçoit, maintient et transmet des informations de santé identifiables. L'HIPAA réglemente trois catégories : les entités couvertes, les associés et les sous-traitants. En ce qui concerne l'éditeur de logiciel, il ne peut s'agir d'une entité couverte. En effet, l'éditeur d'une l'application de suivi médical ne peut pas être considéré comme un plan de santé, un centre d'échange de soins de santé ou un fournisseur de soins de santé mais comme le commerçant en charge de la gestion du développement l'application santé au nom d'une entité couverte par l'HIPAA, précisément un fournisseur de soins de santé. Il s'agit alors d'un sous-traitant et, dans ce cas, il doit se conformer à certaines dispositions des règles de l'HIPAA. Ainsi, la plupart des entrepreneurs et sous-traitants qui fournissent des services ou exercent des fonctions pour les *covered entity* qui impliquent l'accès aux PHI sont considérés comme des *business associate*. Par exemple, une entreprise à laquelle une entité couverte donne accès aux PHI pour fournir et administrer un dossier médical personnel par l'entité couverte à ses patients.

Cependant, un accord d'interopérabilité seul ne crée pas de relations d'affaires[85] car cet accord existe seulement pour faciliter l'accès initié par le consommateur. L'éditeur du logiciel fournit un service au consommateur, à la demande de ce dernier et en son nom. L'éditeur de l'application transmet des données au nom du consommateur au fournisseur. C'est précisément le cas lorsqu'un consommateur télécharge sur son smartphone une application de santé conçue pour l'aider à gérer une maladie chronique. Le prestataire de soins de santé et l'éditeur de l'application ont conclu un accord d'interopérabilité à la demande du consommateur qui facilite l'échange sécurisé d'informations sur le consommateur entre le dossier de santé électronique (Electronic Health Record) du prestataire et l'application. Le consommateur remplit les informations sur l'application et demande à l'application de transmettre les informations du DSE (Dossier de santé électronique) du prestataire. Le consommateur peut accéder aux résultats des tests effectués par le fournisseur par l'intermédiaire de l'application[86].

À l'inverse, l'éditeur est considéré comme un business associate du fournisseur lorsque le patient télécharge une application de santé sur son smartphone, sur instruction de son fournisseur, le prestataire de soins de santé, en raison d'un partenariat entre le fournisseur et l'éditeur de l'application pour les services de gestion des patients, y compris les conseils de santé à distance, la surveillance de l'alimentation et de l'exercice des patients, la messagerie des patients, l'intégration des DSE et les interfaces des applications. En outre, les informations saisies par le patient sont automatiquement intégrées dans le DSE du prestataire de soins. Enfin, pour être considérée comme un partenaire commercial HIPAA, l'application pour les patients ne doit pas nécessiter de prescription pour y accéder.

---

[85] « Instructions for Completing AHC11236 Business Arrangement and Relationships Application », sur Alberta [en ligne], [consulté le 26 mars 2020].

[86] STEINFELD Lauren, « Privacy law and data protection », sur *Coursera*, 2020 [consulté le 10 mai 2020]

B) Les applications de suivi médical en vertu de la loi sur les aliments, les médicaments et les cosmétiques

La loi sur les aliments, les médicaments et les cosmétiques devrait maintenant être étudiée de plus près. En effet, en ce qui concerne l'outil d'orientation, l'application spécifique à la santé de notre étude pourrait être considérée comme un dispositif médical. En effet, l'outil de guidance indique que les applications « destinées à être utilisées dans le diagnostic de maladies ou d'autres conditions, ou dans la guérison, l'atténuation, le traitement ou la prévention de maladies » sont des dispositifs médicaux soumis à la loi FD&C. La FDA considère qu'un produit est un dispositif, et est soumis à sa réglementation, s'il répond à la définition d'un dispositif médical selon la section 201(h) de la loi sur les aliments, les médicaments et les cosmétiques : «Un instrument, un appareil, une machine, un dispositif, un implant, un réactif in vitro ou tout autre article similaire ou apparenté, y compris un composant ou un accessoire destiné à être utilisé dans le diagnostic d'une maladie ou d'autres conditions, ou dans la guérison, l'atténuation, le traitement ou la prévention d'une maladie[87] ». Toutefois, le terme « dispositif » ne comprend pas les fonctions logicielles exclues en vertu de l'article 520, point o). L'article 3060(a) de la loi sur les remèdes a modifié la loi FD&C pour ajouter l'article 520(o) de la loi FD&C 57, qui exclut certaines fonctions logicielles de la définition du dispositif à l'article 201(h) de la loi FD&C 58. Ensuite, l'article 520(o) exclut de la définition de « dispositif » les fonctions logicielles qui répondent aux critères suivants :

> « (1) n'est pas destiné à acquérir, traiter ou analyser une image médicale ou un signal provenant d'un dispositif de diagnostic in vitro ou un modèle ou un signal provenant d'un système d'acquisition de signaux (article 520(o)(1)(E) de la loi FD&C) ;
> (2) destinés à afficher, analyser ou imprimer des informations médicales sur un patient ou d'autres informations médicales (telles que des études cliniques évaluées par des pairs et des directives de pratique clinique) (article 520(o)(1)(E)(i) de la loi FD&C) ;
> (3) destiné à soutenir ou à fournir des recommandations à un professionnel de la santé sur la prévention, le diagnostic ou le traitement d'une maladie ou d'une affection (article 520(o)(1)(E)(ii) de la loi FD&C) ;
> et (4) destiné à permettre à ce professionnel de la santé d'examiner de manière indépendante les bases des recommandations que ce logiciel présente, de sorte que l'intention n'est pas que ce professionnel de la santé se fonde principalement sur l'une de ces recommandations pour poser un diagnostic clinique ou prendre une décision de traitement concernant un patient individuel (article 520(o)(1)(E)(iii) de la loi FD&C). »

[87] qui est « ... destiné à être utilisé pour le diagnostic de maladies ou d'autres affections, ou pour le traitement, l'atténuation, la guérison ou la prévention de maladies, chez l'homme ... » ou « ... destiné à affecter la structure ou toute fonction du corps de l'homme ou d'autres animaux ... » et "ne comprend pas les fonctions logicielles exclues en vertu de l'article 520(o) de la loi FD&C. Ainsi, les applications logicielles qui s'exécutent sur un ordinateur de bureau, un ordinateur portable, à distance sur un site web ou un « nuage », ou sur un ordinateur de poche peuvent être soumises à la réglementation des dispositifs si elles sont destinées à être utilisées pour le diagnostic ou la guérison, l'atténuation, le traitement ou la prévention d'une maladie, ou pour affecter la structure ou toute fonction du corps humain. Le niveau de contrôle réglementaire nécessaire pour assurer la sécurité et l'efficacité varie en fonction du risque que le dispositif présente pour la santé publique

En effet, comme l'expliquent de nombreuses directives officielles de la FDA, certains critères spécifiques doivent être remplis pour qu'une demande soit considérée comme un dispositif médical. Ensuite, de nombreuses fonctions logicielles sont considérées comme des dispositifs médicaux parce qu'elles ne répondent pas à la définition d'un dispositif au titre de la section 201(h) de la loi fédérale FD&C et que la FDA ne les réglemente pas. Dans notre cas, la demande de santé ne peut pas répondre aux critères et donc, ne peut pas être soumise à la loi FD&C.

C) Les applications de suivi médical en vertu de la loi FTC

Le titulaire de la demande étant une organisation à but lucratif, la **loi FTC s'**applique. La loi FTC interdit les actes déloyaux ou pratiques anti-concurrentielles. Cela signifie que le titulaire ne peut pas faire de déclarations trompeuses ou mensongères aux consommateurs sur les éléments essentiels du produit et, ne peut pas se livrer à des actes ou des pratiques qui causent ou sont susceptibles de causer aux consommateurs un préjudice important qu'ils ne peuvent éviter.

D) Le cas de violation de la loi FTC

Enfin, l'application de suivi médical étant mise à disposition pour traiter de données pour le compte d'une *covered entity*, **la règle de notification des atteintes à la santé de la loi FTC** ne s'applique pas.

II- Les extensions de conformité aux regards des relations établies entre les différents acteurs

En droit américain comme en droit européen, la conclusion d'un contrat doit constituer le préalable du partenariat commercial entre un établissement de santé et un éditeur de solutions digitales. En effet, les exigences imposées par la loi HIPAA doivent se traduire aussi par un accord entre les parties. Cet accord permettra ainsi de formaliser la relation et d'inscrire de façon claire les devoirs et obligations de chacun au regard de la réglementation en vigueur. En outre, cette obligation de contractualisation se traduit aussi par la mise en place de conditions générales, mentions légales et politique de confidentialité.

Bien que le droit américain en matière de données de santé ne prévoie aucunes obligations spécifiques en matière d'hébergement, la nécessité de respecter les règles énoncées par la loi HIPAA oblige les fournisseurs de ses services mais aussi les prestataires de ceux-ci à veiller avec précautions aux maintiens des diligences leur incombant. Cela passent avant tout par la souscription d'un hébergement privé.

A) L'obligation de contractualisation en matière de partenariat entre hôpitaux et service de solution digitale de suivi médical

Il a été affirmé précédemment, il est essentiel de mettre en place des garanties administratives, physiques et techniques. Certains points doivent être examinés plus en détail.

Premièrement, outre les garanties susmentionnées, des exigences organisationnelles telles que la rédaction d'un contrat doivent être respectées. En effet, l'article 164.308(b)(3) Security Rule exigeait des exigences organisationnelles la souscription de contrats d'association d'entreprises ou d'autres arrangements de l'article 164.314(a). Selon les paragraphes (a)(2)(i), (a)(2)(ii) et (a)(2)(iii) du § 164.314(a), il existe spécifiquement trois spécifications de mise en œuvre de cette exigence : les accords d'association d'entreprise (*business associate contracts*), autres arrangements et les accords d'association d'entreprise avec des sous-traitants. Pour les *Business associate contracts* et les accords avec des sous-traitants, le contrat doit prévoir que l'associé mettra en œuvre les mesures de protection administratives, physiques et techniques qui ont déjà fait l'objet de développements, afin de protéger la confidentialité[88], l'intégrité et la disponibilité des informations de santé électroniques protégées qu'il crée, reçoit, maintien ou transmet au nom de l'entité couverte et que ces éléments soient intégrés dans le contrat afin d'être formalisés.[89] Ensuite, concernant le contrat avec un sous-traitant, il permet de mettre en œuvre toutes les garanties raisonnables et appropriées nécessaires à la protection des informations de santé pour le compte du *business associate*. De plus, le contrat d'entreprise doit garantir l'obligation de signaler à l'entité couverte tout incident de sécurité dont elle a connaissance par le §164.410 sur la notification par les associés commerciaux inséré par la règle de notification des violations. En ce qui concerne les autres dispositions, le §164.314 prévoit certaines exigences lorsqu'une entité couverte et son associé sont tous deux des entités gouvernementales. Ce point n'étant pas directement lié au sujet traité, il ne sera pas examiné plus avant.

Un point essentiel reste à exprimer. Il convient d'indiquer que la politique de confidentialité est devenue primordiale, notamment depuis le scandale Cambridge Analytica. En effet, il s'agit d'une obligation légale. Cette politique devra notamment contenir un article concernant le recueil de données de personnes mineurs, la collecte des informations personnelles et la finalité de ces collectes, la présence ou non de cookies et leur finalité, la responsabilité de l'éditeur de l'application[90], de l'hébergeur, *business associate* et *covered entity* ainsi que des limites à ces responsabilités, les changements de politique et les exigences posées par la loi californienne en matière de données personnelles (California Online Privacy Protection Act et California Business and Professions Code).

Enfin, il convient de ne pas oublier que bien qu'il s'agisse d'une application d'une entreprise américaine, l'utilisation de celles-ci entraîne une collecte de données stockées sur des serveurs pouvant être aux États-Unis. Ainsi l'ensemble des droits des personnes concernées en vertu du RGPD doivent être énoncés.

Comme en droit européen, il n'existe pas d'obligation en matière de Conditions générales d'utilisation. Toutefois, cette étape est fortement recommandée et permettra notamment de démontrer

---

[88] CHAPITRE 1, I, B. Les exigences de conformité principales : sécurité et confidentialité
[89] Security Rule 45 CFR §164.314(a)(2)(i)(B)
[90] Il s'agit des concepteurs et des développeurs de l'application ou de l'entité ayant commandité l'application.

le recueil du consentement. Le droit européen nécessitant des étapes supplémentaires au regard du RGPD non prévue par la loi HIPAA, ce point sera détaillé au sein du chapitre II.

B) L'obligation de souscrire à un contrat d'hébergement de type cloud computing privé

En matière d'hébergement cloud de données de santé, la réglementation américaine n'octroie pas plus d'exigences aux parties comme cela a été mis en lumière précédemment. Cependant, la mise en place d'un cloud conforme HIPAA demandera face à un environnement d'hébergement standard plus de vigilance mais aussi bien plus de moyens lors du choix de la solution Cloud afin d'être conforme. Une entreprise souhaitant héberger dans le Cloud les données de santé qu'il traite au vu de son activité aura l'obligation de maintenir un niveau de sécurité et de confidentialité élevé, ce qui crée in fine des répercussions sur le choix du fournisseur d'hébergement en raison du besoin de mise à disposition de fonctionnalités supplémentaires. Avant de décrire les caractéristiques clés dont le type de solution choisi doit revêtir, il convient d'énoncer trois principes sans quoi une conformité suffisante ne peut aboutir au regard de la loi HIPAA. Comme cela a déjà été affirmé précédemment, au sein des articles de la loi HIPAA, la formation du personnelle de l'entreprise consiste en un point essentiel sans quoi le maintien de la confidentialité suffisante ne peut aboutir. En effet, le choix d'une technologie appropriée et d'une étude poussée de la réglementation ne sont pas suffisants. Il peut par exemple d'estimer que les communications avec les patients par le biais d'une boîte e-mail constitue un accès simple pour tout cyber hacker. L'ensemble des communications permettront de récolter des données sensibles qu'il conviendra de collecter, supprimer les messages ou les archiver. Afin de maintenir une conformité, les exigences techniques doivent être prise en considération. En outre, une recherche approfondie quant au niveau de mise en conformité du fournisseur est indispensable avant de choisir ou non de rentrer en relation. Il est notamment possible de vérifier cela par le biais des pratiques du fournisseur : la mise en œuvre d'audits support et interne documenté[91], la preuve documentée de mise en œuvre opérante des politiques et procédures prévues par la société, la sensibilisation aux données de santé au sein de l'entreprise, un programme de gestion des risques conforme mais aussi suffisamment vaste et complet, la mise en œuvre d'une Security by design ainsi que d'évaluation périodiques et annuelles.

Un des points essentiels est de démontrer la mise en œuvre d'une coordination de la *covered entity* ou du *business associate* avec le prestataire de solutions cloud. En effet, la loi HIPAA[92], ne rend pas seulement responsable la *covered entity* ou le *business associate*. Ainsi, la prise en charge de l'hébergement des données par un hébergeur conforme à la loi HIPAA va permettre de renforcer la confidentialité et sécurité des données, celui-ci étant dans l'obligation de protéger lesdites données de santé conformément au contrat d'association d'entreprise. Dans ce sens, le contrat d'association devra être constitué de plusieurs clauses relatives. L'ensemble des points devant impérativement faire partie de l'accord est, pour des raisons pédagogiques, listé dans le tableau suivant :

---

[91] Une vérification peut être faite par le biais des déclarations d'audites produite par l'American Institute of Certified Public Accountants Auditing Standards Board. Aujourd'hui, il s'agit de la Statement on Standards for Attestation Engagements No. 18 (SSAE 18)

[92] CHAPITRE I, II- L'application de la loi HIPAA en matière d'hébergement de données de santé

Les points clé devant figurer au sein d'un accord d'association d'entreprise avec un fournisseur de solutions d'hébergement conforme à la loi HIPAA :

- L'énonciation et la documentation du rôle et l'étendue de la responsabilité de chaque partie au contrat ;
- La description du maintien d'une sécurité physique optimale à niveaux minimaux, de la présence physique d'un personnel 24/7/365 gérant l'ensemble des problèmes techniques, violations et failles de sécurités ainsi que la mise en place de caméras au sein de l'établissement à des endroits stratégiques ;
- La mise en œuvre d'un audit d'accès documenté pour le site et les zones critiques
- Le chiffrement des données en transit mais aussi au repos
- La mise en œuvre de procédures des transferts d'équipement
- La formation du personnel et la mise en place d'habilitation
- Une évaluation de l'ensemble des risques et la mise en œuvre de procédures en cas de risques avérés
- La mise en œuvre d'une politique de notification des violations et la description des responsabilités en découlant

Enfin, il convient de faire remarquer que le ministère de la santé et des services sociaux ne reconnaît aucun programme ou certification. Ainsi, toute « certification HIPAA » constitue une « accréditation » mise en place entre les paires du secteur. Il convient ainsi de ne pas fonder son choix de prestataire sur une telle certification. Cependant, il existe des moyens pour s'assurer qu'un prestataire respecte les standards de la loi HIPAA notamment par le biais du protocole d'audit de l'OCR, de l'Auditing Standards Board ou de l'American Institute of Certified Public Accountants.

Comme susmentionné, la souscription à une solution d'hébergement cloud conforme à la loi HIPAA nécessite un budget plus conséquent qu'un hébergement classique. Cependant, il ne s'agit pas d'un surcoût, mais d'un réel investissement primordial à ne pas négliger. S'entourer d'une personne qualifiée en la matière permettra de « désigner » la solution la plus adaptée aux activités de traitement. Dans le cas étudié les éléments suivants sont à privilégier afin de garantir au mieux la confidentialité et sécurité des données[93] [94]:

1) Le choix d'un hébergement privé

L'hébergement de données de santé provenant du suivi des dossiers médicaux de patients étant une donnée sensible, l'accès à celle-ci doit être le plus restreint possible. Ainsi, uniquement l'organisation doit pouvoir y avoir accès.

2) La mise en place d'un pare-feu entièrement géré.

[93] L'ensemble de ces règles sont à respecter aussi bien en vertu du droit fédéral américain que du droit français
[94] Enumération résultant de discussions avec des professionnels notamment un responsable sécurité des systèmes d'information et un ingénieur préparant une thèse dans le domaine des télécommunications.

Par la mise en place d'un pare-feu entièrement géré, la *covered entity* ou le *business associate* (non le fournisseur) est détenteur des choix quant à l'administration, la configuration, la surveillance et l'assistance du pare-feu. Ceci permettra de garantir un hébergement entièrement géré et donc privé.

3) Le choix d'un VPN crypté et d'une sauvegarde chiffrée

VPN est l'abréviation de « réseau privé virtuel ». La mise en place de ce type de VPN est nécessaire au cryptage des données.
Allant de pair avec le VPN le cas présent, la sauvegarde chiffrée est primordiale en matière de données sensibles afin que les données soient cryptées.

4) La mise en place d'un logiciel de journalisation

La mise en place d'un système de gestion des journaux est primordiale afin de pouvoir détecter d'éventuelles intrusions.

5) L'installation d'un anti-malware.

L'installation d'un anti-malware puissant et adapté aux traitements est nécessaire contre toute agression.

CHAPITRE II - L'UNION EUROPÉENNE ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Le RGPD a conduit à l'abandon du rôle prédominant des formalités pour en consacrer un nouveau à l'autorégulation. C'est alors qu'est né le principe de « responsabilité ». Au regard du RGPD, le responsable du traitement se définit comme la personne, l'autorité ou l'organisme qui seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. [95] Le sous-traitant peut lui se définir comme la personne agissant pour le compte du responsable de traitement.

Au-delà du rôle proactif du responsable du traitement et du sous-traitant, il existe de nombreuses obligations auxquelles ces acteurs doivent se conformer. Ainsi, il semble intéressant compte tenu du nombre conséquent d'obligations supportées par ces deux acteurs, de se recentrer sur celles qui paraissent les plus essentielles.

Les données de santé étant l'un des domaines où les États peuvent compléter le texte – ce qui est particulièrement le cas en France – les partenariats entre les établissements de santé et les solutions de suivi médical numérique nécessitent la mise en place d'une conformité spécifique afin de répondre aux différentes exigences fixées par le RGPD et le droit français. Exempli gratia, dans le cadre d'un partenariat ou d'une location d'un service de solutions digitales, les rôles de chaque acteur doivent

[95] Article 4§7 du Règlement (UE) 2016/679

être déterminés avec précision. En effet, une requalification en responsabilité conjointe du sous-traitant étant possible en raison de la complexité toujours croissante des traitements, il est ainsi nécessaire de formaliser scrupuleusement leur relation.

En outre, au regard des guides mis en place par de nombreuses autorités de contrôle, l'ensemble des traitements doivent être cartographiés et le statut de sous-traitant scrupuleusement examiné dans le cadre d'une solution digitale.

Section 1- Les principales obligations du responsable du traitement et du sous-traitant dans le secteur de la santé

Comme l'indique M. Didier Ambroise[96], la première difficulté que peut rencontrer un établissement de santé concerne la diversité des logiciels, des outils et des solutions mis en œuvre, ce qui conduit à une multitude d'acteurs et d'applications rendant délicat le travail de supervision et de mise en conformité.

Ainsi, il est plus qu'essentiel de définir précisément les responsabilités en matière de conformité qui incombent à chaque acteur, notamment celle du responsable du traitement et du sous-traitant directement lié au partenariat entre l'établissement de santé (le responsable du traitement) et le fournisseur de services de solutions digitales (le sous-traitant) au regard du droit européen mais aussi du droit français.

Enfin, la prise en compte de la responsabilité de l'ensemble des acteurs nécessite, lors du choix de l'hébergement des données, de connaître les règles applicables en matière d'hébergement de données de santé.

I- Un principe de garanties suffisantes, prise en compte des principes de protection des données by design et de protection des données par défaut

En vertu du nouveau règlement sur la protection des données, certains traitements en raison de leur caractère « risqué » font l'objet d'une interdiction au regard de l'article 9 du RGPD. En effet, le §1 indique qu'en matière de données concernant la santé, le traitement est interdit. Cependant, son paragraphe 2 prévoit des exceptions dans des cas précis, méritant ainsi en cas de traitement autorisé de ces données sensibles une protection plus élevée.

Les obligations revenant à la charge du responsable du traitement et du sous-traitant doivent être appréhendées et mis en pratique de façon stricte et précise aussi bien au regard du RGPD que de la loi n°78-17 du 6 janvier 1978 introduisant des conditions supplémentaires en matière de données de santé. Au regard de ces deux législations, tout projet e-santé devra respecter un principe de protection des droits des personnes ainsi que de confidentialité des données.

A- Les règles propres au RGPD

La connaissance de l'ensemble des obligations pesant sur le responsable du traitement et le sous-traitant dans le secteur de la santé constitue un point fondamental préalable en matière de conformité.

[96] Didier Ambroise est le fondateur de Doshas Consulting, un cabinet de conseil spécialisé dans la santé, l'assurance et la protection sociale. Ce cabinet a accompagné une majorité d'acteurs de la santé en matière de respect du RGPD.

En effet, en vertu du droit communautaire, toutes « les données relatives à la santé physique ou mentale passée, présente ou future d'une personne physique (y compris la prestation de services de santé) qui révèlent des informations sur l'état de santé de cette personne »[97] relèvent du champ d'application du règlement général sur la protection des données (RGPD). On peut alors diviser en trois sortes de catégories ce que peut représenter une donnée de santé. Bien que la définition donnée par le RGPD traduit un concept très large de ce que ces données sensibles représentent, est pris en compte pour les définir la prise en charge sanitaire d'une personne dans son ensemble. Il peut alors s'agir d'information permettant l'identification d'un patient au cours de la prise en charge par un acteur du secteur médico-social, d'informations collectées au cours d'un examen médical ou contrôle, ou d'informations sur l'état de santé d'un patient (maladies, risques, données cliniques ou thérapeutiques, handicapes diverses). Le type de données récoltées lors parcours de soins doit permettre de qualifier plus précisément le projet e-santé afin de respecter les exigences posées par la règlementation (définition des finalités du projet et des traitements, description de la nature et catalogue des données concernées, recensement des dispositifs techniques utilisés et recensement des acteurs ayant contribué et contribuant au projet e-santé).

Les responsables de traitements et les sous-traitants sont tenus de respecter certaines formalités établies par le RGPD et contrôlées par les autorités de contrôle de chaque pays membre. Toutefois, le réglement a envisagé une réduction de leurs obligations pour faire place à une responsabilité accrue et proactive. En effet, en contrepartie de l'abandon de certaines des formalités préalables requises jusqu'à présent, le contrôleur doit être en mesure de démontrer, à tout moment, sa conformité aux exigences du RGPD en retraçant toutes les démarches effectuées. C'est le principe de responsabilité qui garantit une conformité dynamique.

Ainsi, les formalités à accomplir auprès de l'autorité de contrôle, en France la CNIL, disparaissent pour les traitements portant sur les données de santé suivantes[98] : pour lesquels la personne concernée a donné son consentement explicite ; nécessaires à la protection de la vie humaine ; concernant des données à caractère personnel rendues publiques par la personne concernée ; nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé et effectués par un membre d'une profession de santé ou par une autre personne tenue au secret professionnel en raison de ses fonctions ; les recherches à effectuer sur la base de données effectuées par le personnel chargé de cette surveillance et destinées à son usage exclusif ; mises en œuvre à des fins de prestation de services ou de surveillance par les organismes chargés de la gestion d'un régime d'assurance maladie de base ainsi que du paiement des prestations par les organismes d'assurance maladie complémentaire ; effectuée au sein des établissements de santé par les médecins responsables de l'information médicale, dans le cadre du Programme de médicalisation des systèmes d'information locaux ; effectuée par les agences régionales de santé, par l'État et par la personne publique désignée par lui ; des données dans le domaine de la santé mises en œuvre par des organismes ou services chargés d'une mission de service public figurant sur une liste fixée par arrêté des ministres chargés de la santé et de la sécurité sociale, pris après avis de la CNIL, dont l'unique finalité est de répondre, en cas d'urgence, à une alerte sanitaire et d'en gérer les

[97] Article 4 du Règlement (UE) 2016/679 : « données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne »

[98] Article 9 §2 du Règlement (UE) 2016/679

conséquences. Dans notre cas, le traitement s'inscrivant dans le cadre d'un partenariat entre un établissement de santé et l'éditeur d'une solution digitale de suivi médical, ledit traitement est réalisé avec le consentement de la personne concernée, c'est-à-dire le patient. En effet, l'utilisation de l'application étant proposée aux patients, ceux-ci sont informés lorsque l'établissement de santé fournit un code d'accès et donnent leur consentement expresse lors du démarrage de l'application, lors de l'installation. Enfin, le partenariat conduisant à la collecte des données est, dans tous les cas, mis en place dans le seul but d'opérer un suivi du patient. Par conséquent, la collecte de données de santé et le traitement ne posent pas de problèmes tant que les obligations de conformité sont respectées.

Depuis l'entrée en vigueur du RGPD, chaque responsable du traitement doit choisir, en vertu de l'article 28, paragraphe 1, un sous-traitant offrant "des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées pour que le traitement réponde aux exigences (de la nouvelle réglementation) et garantisse la protection des droits de la personne concernée". En effet, comme l'indiquent Jean HERVEG et Jean-Marc VAN GYSEGHEM dans Le règlement général sur la protection des données (RGPD / GDPR) : analyse approfondie / sous la direction de Cécile de Terwangne et Karen Rosier ; avant-propos d'Yves Poullet : il s'agit de « garantir l'étanchéité du circuit de traitement des données », c'est-à-dire de garantir la confidentialité et la « protection de la personne concernée » et de ses données[99]. Ainsi, le sous-traitant doit être en mesure d'exécuter la tâche que le responsable du traitement entend lui confier afin de se conformer au RGPD. Une question fondamentale doit alors être posée : quels moyens un responsable du traitement doit-il mettre en œuvre pour vérifier l'existence ou non de capacités adéquates du sous-traitant ? Au regard du de l'article 28.1(1) et du considérant 81, on peut voir que l'existence de « garanties suffisantes » doit être appréciée à la lumière des connaissances, de la fiabilité et des ressources du sous-traitant afin de « mettre en œuvre des mesures techniques et organisationnelles qui satisfont aux exigences du présent règlement, y compris pour la sécurité des traitements ». On peut également considérer que la preuve du respect de l'article 28 peut être trouvée, entre autres, par l'application d'un code de conduite approuvé, comme prévu à l'article 40, ou de systèmes de certification approuvés, comme prévu à l'article 42.[100]

Avant tout traitement il conviendra toutefois de déterminer si ce traitement constitue un risque élevé par le biais d'une analyse d'impact. En matière de données de santé, les traitements concernés par une analyse d'impact sont: les traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médicosociaux pour la prise en charge des personnes, traitements portant sur des données génétiques de personnes dites « vulnérables », traitements des données de santé nécessaires à la constitution d'un entrepôt de données ou d'un registre ou traitements pour finalités de l'accompagnement médico-social des personnes[101] . Le traitement dans le cadre du

[99] DE TERWANGNE Cécile, ROSIER Karen, « Le règlement général sur la protection des données (RGPD / GDPR) : analyse approfondie », Edition Larcier, 2018, p746, §46

[100] Considérant 81 du Règlement (UE) 2016/679 : "L'adhésion du sous-traitant à un code de conduite approuvé ou à un mécanisme de certification approuvé peut être utilisée comme élément pour démontrer le respect des obligations du responsable du traitement".

[101] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », sur cnil.fr [en ligne], [consulté le 20 juin 2020].

partenariat faisant l'objet d'une collecte de données sensibles mis en œuvre par un établissement de santé concernant la constitution d'un dossier patient, une analyse d'impact doit être impérativement menée dans un premier temps. L'analyse d'impact devra comprendre la description des opérations de traitements envisagées, l'évaluation de la proportionnalité et nécessité du traitement, des mesures de conformité envisagées, l'évaluation des risques potentiels et avérés pour les droits et libertés des personnes concernées, les mesures pour y faire face, ainsi que la documentation afférente comme le rappel la CNIL mettant à disposition sur son site un logiciel à télécharger.[102]

Toutefois, il conviendra de distinguer le traitement de données de santé des salariés du responsable de traitement dans le cadre de l'exercice de l'activité de l'établissement de ceux des professionnels de santé exerçant à titre individuel. En effet, un professionnel de santé peut, pour une partie de son activité, exercée à titre individuel. Sa propre activité devra alors impérativement être distinguée de celle, en tant que salarié, pour le compte de l'établissement de santé.

Cependant, si le RGPD pose un principe d'interdiction en vertu de l'article 9 du RGPD des traitements de données sensibles telles que les données de santé, il existe des exceptions comme énoncé, mais aussi des possibilités pour les États membres d'introduire des conditions supplémentaires et des limitations aux traitements des données de santé.

B- les règles d'extension de garanties mise en place en droit français en matière de données de santé

En Europe, il existe un cadre règlementaire européen en matière de protection des données. Toutefois, ce cadre réglementaire unique autorise les États membres à bénéficier d'une marge de manœuvre afin d'introduire « des conditions supplémentaires y compris des limitations en ce qui concerne le traitement […] des données concernant la santé »[103]. Ainsi, en France, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi informatique et libertés) modifiées en 2018 permet de compléter le texte européen. La loi informatique et libertés doit toujours s'articuler en matière de données de santé avec le Code de la santé publique. Une résonnance doit notamment s'opérer avec l'article L. 1110-4 du C. santé publique énonçant un droit au respect de la vie privée et du secret des informations concernant la personne prise en charge par un professionnel de santé, un établissement ou un service, un professionnel ou organisme concourant à la prévention ou aux soins dont les conditions d'exercice ou activités sont régies par le Code de la santé publique. La protection des droits des personnes et la confidentialité des données de santé sont réitérées par ce texte.

Reprenant le principe d'interdiction énoncé au sein du RGPD, l'article 44 de la loi informatique et libertés énonce les cas où le traitement de données ne serait pas illégal. Il existe précisément 6 catégories d'exceptions. Dans le cas de cette étude, il s'agirait de tout traitement nécessaire aux fins de l'administration de soins ou de traitements mis en œuvre par un membre d'une profession de santé

[102] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, « Outil PIA : téléchargez et installez le logiciel de la CNIL », sur cnil.fr [en ligne], publié le 24 juin 2020, [consulté le 20 juin 2020].
[103] Article 9§4 du Règlement (UE) 2016/679

soumise au secret professionnel. Couvrant l'ensemble des traitements relatifs aux données de santé, la loi informatique et libertés permet aux responsables du traitement et au sous-traitant de n'être soumis à aucune formalité, seulement au respect des dispositions du RGPD en vertu de l'article 65. En effet, les autres traitements devront faire l'objet de formalités comprenant la démonstration dans un premier temps de l'existence d'un intérêt public et, dans un second temps, de garantie de normes suffisantes et élevées par le biais d'une conformité à des référentiels et règlements types établis par la CNIL ou d'une autorisation expresse de celle-ci. Dans le cadre du partenariat, les principes suivants doivent alors seulement être respectées : des données adéquates, pertinentes, non excessives et mises à jour ; une finalité devant être déterminée ainsi que légitime ; une durée de conservation limitée ; le maintien d'une sécurité élevée ; et le respect de l'ensemble des droits de la personne concernée par le traitement.

Au regard de la législation française, le rôle du tiers de confiance ainsi que du tiers technique doivent être envisagé, nécessitant le respect des obligations formulées par le RGPD. Le tiers de confiance peut être définit comme une personne, une entité extérieure au responsable du traitement assurant des missions relatives à la mise en conformité, notamment la sécurité, des traitements de données. Le tiers technique constitue l'intervenant technique impliqué au sein de la mise en œuvre des systèmes d'information et de communications par exemple d'une application. Ces deux types d'intervenant peuvent se retrouver au sein d'un même organisme, exerçant ces deux rôles, tels qu'un hébergeur de données ou un éditeur de logiciels. En cas de non-respect de leurs obligations, de failles de sécurité ou de divulgation des données à des tiers, leur responsabilité peut être engagée au regard de l'article 9 et 1240 du Code civil et de l'article 226-22 du Code pénal français.

En outre, le droit français exige de la part des acteurs du secteur de la santé d'établir leur conformité, au regard notamment de diverses certifications. Deux mises en conformité doivent retenir l'attention du lecteur.

Au regard de l'article L 5211-3 du Code de la santé publique, les dispositifs médicaux « ne peuvent être importés, mis sur le marché, mis en service ou utilisés, s'ils n'ont reçu, au préalable, un certificat attestant leurs performances ainsi que leur conformité à des exigences essentielles concernant la sécurité et la santé des patients, des utilisateurs et des tiers. ». On entend par dispositif médical tout instrument, appareil, équipement, matière, produit, […] y compris les accessoires et logiciels nécessaires au bon fonctionnement de celui-ci, destinés par le fabricant à être utilisés chez l'homme à des fins médicales et dont l'action principale voulue n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens[104]. Constitue également un dispositif médical le logiciel destiné par le fabricant à être utilisé spécifiquement à des fins diagnostiques ou thérapeutiques[105]. La procédure à mettre en œuvre en matière de certification dépendra du type de classe auquel se rattache le dispositif médical en fonction du degré de risques que celui peut engendrer pour le patient, nécessitant des procédures proportionnelles au risque. N'ayant pas un impact prédominant pour notre étude, il convient de se

[104] Afin d'identifier en cas de doute s'il s'agit d'un dispositif médical, la lecture des lignes directrices du MEDDEV 2.1/6 de juillet 2016 peut être opportun.
[105] Article L. 5211-1 du Code de la santé publique

concentrer prioritairement sur l'examen de l'article L. 1110-4-1 du Code de la santé publique imposant la conformité des systèmes d'information ainsi que des outils numériques est primordiale. En effet, cet article énonce une obligation de conformité aux référentiels d'interopérabilité et de sécurité élaboré par l'Agence du numérique en santé (ANS)[106] ayant pour finalité de garantir l'échange, le partage, la sécurité et la confidentialité des données de santé au regard de la loi informatique et libertés et du RGPD.

Enfin, l'article L. 1111-8 du Code de la santé publique exige l'entrée en conformité des hébergeurs de données de santé par la détention d'un certificat de conformité. Ce certificat découle d'une procédure de certification modifiée en avril 2019, nécessitant une évaluation des hébergeurs au regard d'un référentiel de certification. En effet, le décret n°2018-137 du 26 février 2018 relatif à l'hébergement des données de santé à caractère personnel énonce l'ensemble des conditions. La procédure de certification est constituée d'un audit en deux étapes : documentaire et sur site. Cette procédure se fonde sur les exigences spécifiques à l'hébergement de données de santé notamment au regard de l'article R.1111-11 du Code de la santé publique et de la norme ISO 17021 elle-même issue de l'assemblage de plusieurs normes internationales[107] qui, en cas de conformité de l'hébergeur, entraînera la délivrance du certificat par l'organisme certificateur choisi par l'hébergeur. Cet organisme doit être un organisme accrédité par le Comité français d'accréditation (COFRAC)[108].

Les partenariats entre les établissements de santé et les solutions digitales de suivi médical nécessitent la mise en place d'une conformité spécifique afin de répondre aux différentes exigences posées en droit européen et en droit français. Il est donc nécessaire d'examiner plus en détail certaines des obligations incombant au responsable du traitement et aux sous-traitants.

II- Les principales obligations du responsable du traitement et du sous-traitant

Dans ce paragraphe, sera abordé les principales obligations du responsable du traitement et du sous-traitant. En effet, notre objectif est d'identifier les politiques et procédures générales à mettre en place en termes de conformité dans le secteur de la santé concernant les partenariats entre hôpitaux et le service de solution de suivi médical numérique.

A) Transparence et traçabilité

Il est avant tout nécessaire de formaliser la relation entre le responsable du traitement et le sous-traitant. Ainsi, la première obligation qui se présente est celle d'être régi par un contrat. L'article 28.3 du RGPD dispose que « le traitement effectué par un sous-traitant est régi par un contrat ou tout autre

[106] L'ANS est l'agence française régulant la e-santé en posant des cadres et bonnes pratiques. Elle conduit les projets d'intérêt national ainsi que le déploiement national et territorial des projets e-santé.
[107] La norme ISA 17021 prend en compte l'ensemble des normes internationales reconnus tel que la norme ISO 27001 relative au système de gestion de la sécurité des systèmes d'information, la norme ISO 20000-1 relative au système de gestion de la qualité des services, la norme ISO 27018 relative à la protection des données à caractère personnel et de la norme ISO 27017 portant sur les aspects de la sécurité de l'information du cloud computing.
[108] Une liste des hébergeurs certifiés et des organismes accrédités est disponible sur le site de l'ANS.

acte juridique relevant du droit de l'Union ou du droit des États membres, qui lie le sous-traitant au responsable du traitement et qui détermine l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement ». Le considérant 79 du RGPD permet de comprendre l'importance de cette obligation. Afin d'identifier la responsabilité de chaque partie, une répartition claire des responsabilités permet d'assurer une protection suffisante des droits et libertés des personnes concernées ainsi que la responsabilité des responsables du traitement et des sous-traitants par la détermination des finalités et des moyens du traitement, notamment dans le cas d'un traitement effectué avec d'autres responsables du traitement ou lorsqu'un traitement est effectué pour le compte d'un responsable du traitement. En outre, le considérant 81 du RGPD permet, toujours dans le but de garantir une mise en œuvre effective du réglement, de déterminer ce qu'il adviendra des données relatives à la santé collectées après le traitement. En droit français, à l'issue d'une période de 20 ans à compter de la date du dernier séjour ou de la dernière consultation du patient dans l'établissement, les données doivent être détruites, sauf exceptions.[109] Enfin, « après la fin du traitement pour le compte du responsable du traitement, le sous-traitant doit, au choix du responsable du traitement, restituer ou supprimer les données à caractère personnel, sauf si le droit de l'Union ou de l'État membre auquel le sous-traitant est soumis, prévoit l'obligation de conserver les données à caractère personnel ».

B) L'obligation de garantir la sécurité des données traitées

En outre, le RGPD a renforcé les dispositions relatives à la sécurité du traitement en imposant au responsable du traitement et au sous-traitant l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées. L'article 32 du RGPD, qui traite de la sécurité des traitements, nous permet de constater la volonté du législateur européen d'accorder un rôle proactif au responsable du traitement et au sous-traitant dans la mise en œuvre des mesures nécessaires pour assurer la confidentialité des données. Le premier paragraphe indique que des mesures techniques et organisationnelles appropriées doivent être mises en œuvre pour assurer un niveau de sécurité approprié au risque, notamment en ce qui concerne l'identification du risque lié au traitement, leur évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques pour atténuer le risque.[110] L'établissement de codes de conduite approuvés, de certifications approuvées et de lignes directrices données par le Comité ou les conseils donnés par un délégué à la protection des données sont des mesures appropriées pour démontrer le respect de ces règles par l'entité par l'intermédiaire du responsable du traitement ou du sous-traitant. Néanmoins, l'article 32 du RGPD rappelle que ces mesures doivent être mises en œuvre afin de garantir « les droits et libertés des personnes physiques ». Mais quels sont précisément ces droits ? Toutes les personnes concernées par le traitement de leurs données de santé bénéficient de certains droits[111] : le droit à la transparence et à l'information, le droit d'accès aux données de santé, le droit à la portabilité appliquée aux données

[109] Article R. 1112-7 du Code de la santé publique
[110] Considérant 77 du Règlement (UE) 2016/679
[111] Art 12 du Règlement (UE) 2016/679

de santé, le droit de ne pas faire l'objet de décisions automatisées, le droit de rectification, le droit d'effacement, le droit de limitation du traitement et le droit d'opposition au traitement des données.

Une liste non exhaustive de mesures a été établie afin de guider les praticiens dans la mise en conformité concernant la sécurité du traitement. Ces mesures sont les suivantes : la pseudonymisation et le cryptage des données à caractère personnel ; la capacité à assurer en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ; la capacité à rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique ; un processus permettant de tester, d'évaluer et de juger régulièrement l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité du traitement. En ce qui concerne les partenariats entre les hôpitaux et le service de solution de suivi médical numérique, une pseudonymisation stricte et simple n'est pas possible, ce qui rendrait impossible la réalisation des objectifs souhaités, c'est-à-dire le suivi dit personnalisé.

Selon l'article 32, paragraphe 4 du RGPD, « le responsable du traitement et le sous-traitant prennent des mesures pour que toute personne physique agissant sous l'autorité du responsable du traitement ou du sous-traitant qui a accès à des données à caractère personnel ne les traite que sur instruction du responsable du traitement ». À la lumière de cet article, les responsables du traitement et les sous-traitants doivent donc contrôler l'accès aux données à caractère personnel et, par conséquent, garantir que toute personne physique placée sous leur autorité ne peut avoir accès aux données que sur instruction de ces derniers, sauf si elle y est légalement tenue.

En ce qui concerne l'article 32 du RGPD, nous pouvons apprécier l'obligation de mettre en place des mesures à la fois techniques et organisationnelles.[112] Si nous prenons la pseudonymisation par exemple, le traitement des données personnelles ne peut plus être attribué à une personne spécifique sans l'utilisation d'informations supplémentaires. Ensuite, les informations complémentaires doivent être conservées séparément et faire l'objet de mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne soient pas attribuées à une personne physique identifiée ou identifiable.

En général, la mise en œuvre de mesures organisationnelles implique la formation du personnel ayant accès aux données relatives à la santé, l'établissement de règles internes strictes et la mise en place de structures efficaces pour prévenir les failles de sécurité qui entraîneraient la perte de données, leur destruction ou leur modification non autorisée ou un accès non autorisé : un ensemble de mesures visant à assurer une organisation adéquate et efficace. En ce qui concerne les mesures techniques, cela se traduit, comme dans la loi américaine HIPPA concernant les obligations techniques et physiques, par des mesures adéquates de protection des traitements telles que la mise en place de règles d'accès strictes par des mots de passe composés de lettres, de majuscules, de signes de ponctuation, de chiffres et de phonétique ou un blocage du compte en cas de non-renouvellement du mot de passe à une date déterminée.

[112] Voir annexe 4 à propos des mesures à mettre en place.

Au total, on peut constater que nombre de ces mesures sont à la fois à la charge du responsable du traitement et, partiellement ou non, à la charge du sous-traitant. Ce constat résulte de l'intervention du sous-traitant dans le traitement et de ses connaissances spécifiques. A cet égard, on peut apprécier la réelle coordination devant exister entre le sous-traitant et le responsable du traitement, premier contact du patient. Le fait que le sous-traitant a acquéri aient un rôle proactif dans la mise en œuvre du respect de la RGPD pour tenir compte des risques liés aux données en cas l'accès illégitime aux données (profilage, revente, distribution, vol, etc...), de modification ou de la disparition non souhaitée des données suite à un dysfonctionnement ou un blocage.

C) L'obligation de signaler les infractions à la sécurité

Malgré les garanties techniques et les mesures organisationnelles mises en place, en cas de violation de la sécurité, le responsable du traitement reste tenu d'informer l'autorité nationale de contrôle au moyen d'une notification. En effet, l'article 4 stipule que les données font l'objet d'une violation si celle-ci entraîne une perte de disponibilité, d'intégrité, de confidentialité des données à caractère personnel, qu'elle soit accidentelle ou illicite. Si l'incident constitue un risque pour la vie privée des personnes concernées, le responsable du traitement doit notifier l'incident à l'autorité nationale. Selon le considérant 85 du RGPD, il s'agit d'une violation susceptible, en cas d'intervention tardive et inappropriée, de « causer un préjudice physique, matériel ou moral aux personnes physiques concernées ».[113] Ainsi, la notification n'est requise que si la violation est d'une certaine gravité. En tout état de cause, le responsable du traitement doit documenter l'incident en interne en déterminant : la nature de la violation si possible, les catégories et le nombre approximatif de personnes concernées par la violation ; les catégories et le nombre approximatif de dossiers de données à caractère personnel concernés ; décrire les conséquences probables de la violation ; décrire les mesures prises ou envisagées pour empêcher que l'incident ne se reproduise ou pour en atténuer les conséquences négatives.[114] La documentation ainsi compilée permet à l'autorité de contrôle de vérifier le respect du RGPD.

Conformément à l'article 33.2 du RGPD, le sous-traitant, après avoir pris connaissance d'une violation de données à caractère personnel, en informe le responsable du traitement sans délai excessif. En effet, sans la documentation mise en place par le sous-traitant, le responsable du traitement ne serait pas en mesure de remplir son obligation de notification, le cas échéant, à l'autorité nationale de contrôle.

---

[113] Considérant 85 du Règlement (UE) 2016/679 : "comme la perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, la discrimination, l'usurpation ou la fraude d'identité, la perte financière, l'annulation non autorisée de la pseudonymisation, l'atteinte à la réputation, la perte de confidentialité des données à caractère personnel protégées par le secret professionnel ou tout autre désavantage économique ou social important pour la personne physique concernée".

[114] Article 33.3 du Règlement (UE) 2016/679 : "Notification d'une violation de données à caractère personnel à l'autorité de contrôle".

D) L'obligation de tenir un registre

Il existe une masse considérable de traitements dans les organisations sans qu'il y ait de véritables classifications de ces traitements. Dans cette optique, le RGPD exige que les salaires soient enregistrés dans un registre. Cela permettra de savoir quels sont les traitements et donc de vérifier leur conformité. Cela facilitera également un principe essentiel du nouveau règlement, à savoir documenter la conformité. En outre, la pratique a montré que l'établissement de registres facilite les demandes des personnes inscrites au dossier. En vertu de l'article 30 du RGPD, le règlement exige l'établissement d'un registre sous forme écrite ou électronique. Ce registre fonctionnera comme un index afin de pouvoir organiser les différents traitements sous forme de listes dans des termes pertinents et appropriés. En cas de lacunes ou de contrôles, ce registre est très important et doit donc être établi avec soin. Il s'agit d'un outil de responsabilisation.

Outre le responsable du traitement, les sous-traitants sont tenus de tenir ce registre pour leur activité en tant que responsable du traitement mais aussi en tant que sous-traitant. Ce registre peut être établi par le délégué à la protection des données mais n'est pas lié à lui. En outre, le registre des traitements n'est obligatoire que dans deux cas : lorsqu'une entreprise ou une organisation compte plus de 250 employés ou lorsque le traitement effectué est susceptible, en vertu de l'article 30.5, de présenter un risque « d'entraîner un risque pour les droits et libertés des personnes concernées, que le traitement ne soit pas occasionnel ou qu'il porte sur des catégories particulières de données visées à l'article 9.1, ou sur des données à caractère personnel relatives aux condamnations pénales et aux infractions visées à l'article 10 ». L'article 9 concerne les données dites sensibles et les infractions/condamnations visées à l'article 10. Cependant, dans la pratique, le registre est indispensable, comme nous l'avons vu. Il est donc plus que nécessaire d'en établir un afin de disposer d'un programme de protection des données qui fonctionne (tableau 1).

Contenu du registre du responsable du traitement	**Contenu du registre du sous-traitant**
Le registre doit contenir au moins les informations suivantes : - les objectifs du traitement, - les catégories de personnes concernées et les catégories de données, - catégories de bénéficiaires, - les transferts de données à l'extérieur de l'Union, - « dans la mesure du possible » le délai d'effacement des données et la description des mesures de sécurité	Le registre doit contenir au moins les informations suivantes : - les catégories de traitements effectués pour le compte de chaque traitement, - le cas échéant, les transferts de données à caractère personnel, - dans la mesure du possible, une description générale de la sécurité technique et organisationnelle.

Tableau 1 : Le contenu des registres des traitements

E) L'obligation de recourir aux services d'un délégué à la protection des données

L'article 37 du RGPD définit les conditions dans lesquelles la désignation d'un délégué à la protection des données (DPD) est obligatoire. En effet, chaque responsable de traitement et sous-traitant n'est tenu de désigner un DPD que dans des cas spécifiques. Toutefois, dans un premier temps, il convient d'identifier clairement ce qu'est un DPD : il s'agit de toute personne physique exerçant une fonction d'assistance et de conseil à l'égard du responsable du traitement et du sous-traitant afin de

s'assurer que le traitement des dossiers effectué est conforme au règlement applicable. Le délégué à la protection des données est une nouvelle profession à laquelle plusieurs types de professions ont droit. En effet, il n'existe pas de compétences spécifiques pour exercer cette profession. Comme nous avons pu le dire, sa désignation est obligatoire dans certains cas. Elle est obligatoire pour les structures du secteur public, dans le secteur privé pour les entreprises mettant en œuvre des traitements dont le suivi est « régulier et systématique sur une grande échelle d'individus » (profilage, segmentation comportementale, analyse fine de la navigation d'un internaute comme pour la lutte contre la fraude, traitement marketing ciblé) ou consiste en un traitement à grande échelle de données sensibles ou de données relatives à des infractions (ce qui est le cas pour les données relatives à la santé).

Toutefois, le DPD doit avoir les qualités nécessaires pour exercer ses fonctions, telles qu'une expertise en matière de lois et de pratiques relatives à la protection des données. Dans le domaine des données de santé au sein des hôpitaux, il est plus que nécessaire que le DPD ait une bonne connaissance du droit de la santé et plus particulièrement des droits du patient, de l'organisation des établissements hospitaliers et de toute règle relative aux dossiers des patients. Le rôle du DPD est de conseiller et d'accompagner les organes qui le désignent en matière d'évaluation de l'impact du traitement et de la protection des données, de coopérer avec l'autorité de contrôle et d'agir en tant que personne de contact avec l'autorité de contrôle. À cette fin, l'article 38 stipule que le DPD doit être associé à toutes les questions qui le concernent, qu'il doit disposer des ressources nécessaires à l'exécution de ses tâches, qu'il doit avoir accès aux données concernées et qu'il doit être libre d'exercer ses fonctions, c'est-à-dire totalement indépendant. En outre, il ne sera pas responsable en cas de non-respect du règlement.

En Europe, il n’existe pas de seuil précisant qu’il s’agit d’un traitement à grande échelle entraînant l’obligation de désigner un DPD. Cependant, des lignes directrices[115] permettent d’identifier ce que pourrait constituer un traitement à grande échelle. En matière de projet e-santé, on pourrait estimer le nombre de patients dont le traitement des données de santé en suivi post-opératoires se servant de l’application doit être conséquent par rapport à celui ne s’en servant pas au sein d’un même établissement de santé dans le cadre du déroulement régulier de ses activités de suivi de patients.

Au-delà des règles générales en matière de protection des données de santé, une application spécifique aux partenariats entre les établissements de santé et les éditeurs de solutions digitales ainsi que les hébergeurs doit être faites.

Section 2- L'application de la réglementation en matière de partenariats entre hôpitaux et service de solution digitale de suivi médical

L’éditeur de l'application de suivi médical effectuant le traitement des données est considéré par la législation européenne comme un sous-traitant. En effet, il agit pour le compte du responsable du

[115] FALQUE-PIERROTIN Isabelle, GROUPE DE TRAVAIL «ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01 [en ligne], 2017, p. 8-11, [consulté le 1er juillet 2020].

traitement, c'est-à-dire les établissements de santé avec lesquels il a conclu un partenariat. Certaines obligations propres lui incombent, ne pouvant être assimilé à un subordonné.

Ainsi, en cas de partenariat entre un responsable de traitement et un sous-traitant, les rôles de chaque partie doivent être déterminés avec précision, au vu de la possibilité de requalification en tant que co-responsables de traitement en raison de la complexité toujours croissante des traitements. Outre la rédaction minutieuse du contrat de sous-traitance classique afin d'éviter toutes requalifications postérieures, il convient de la distinguer de celle du contrat de Cloud computing nécessitant l'inclusion d'articles/clauses spécifiques, en tenant notamment compte qu'il s'agisse d'une relation de sous-traitance ou de co-traitance.

I- Les principales diligences dans le cadre du RGPD en matière d'applications de données de santé

Le développement d'une application de e-santé exige que la protection des données personnelles collectées soit garantie. Il est donc essentiel de mettre l'accent sur certains types de diligences raisonnables devant être mises en œuvre en amont du déploiement de l'application.

A) L'application des obligations en matière de protection des données aux applications mobiles et sites web

Contrairement aux conditions générales de vente, la constitution des conditions générales d'utilisation ne constitue pas une obligation légale. Toutefois, comme indiqué dans le Chapitre I, celle-ci est essentielle. En droit européen, les mentions devant y figurer sont différentes des conditions générales d'utilisation mise à la disposition des résidents américain en raison notamment des droits accordés aux personnes concernées par des traitements de leurs données à caractère personnel au regard du RGPD.

La nouvelle règlementation a accordé une plus grande importance au consentement de l'utilisateur. Ainsi, doit être ajouté au sein des formulaires une case obligatoire à cocher, proposant à vos utilisateurs de consulter et accepter vos conditions et politiques de confidentialité des données personnelles. Le consentement constituera alors un acte positif clair au regard du considérant 32 du RGPD dès qu'il s'agira de la base légale : ce qui est le cas en l'espèce. La mise en place de la politique de confidentialité est primordiale et permettra en outre de démontrer, au-delà de la conformité de l'entreprise la volonté d'accorder un niveau de sécurité suffisant aux utilisateurs. La question qu'il convient de se poser en matière de politique de confidentialité est la suivante : que doit contenir une page de politique de confidentialité ? Celle-ci doit réunir les éléments principaux nécessaires pour les utilisateurs et consommateurs de façon clair, transparente et précise. En effet, il convient toujours de se référer à l'article 12 du RGPD lors de la rédaction des différentes informations à l'attention des personnes concernées. Toute communication à l'attention de ceux-ci, y compris dans le cadre de l'énonciation de ces droits et de leur exercice, doit être réalisée en des termes « clairs et simples » et « d'une façon concise, transparente, compréhensible et aisément accessible ». Ainsi, au regard d'une ligne directrice du G29 du 28 novembre 2017, il convient a minima d'indiquer à la personne concernée : l'identité du responsable du traitement, la finalité de

chaque traitement de données pour lequel le consentement est recueilli, les catégories de données collectées et utilisées, l'existence du droit de retirer son consentement, l'existence d'une prise de décision automatisée incluant une mesure de profilage et, si le consentement concerne des transferts de données, les risques potentiels inhérents à un transfert vers un pays tiers en l'absence d'une décision d'adéquation ou d'une garantie appropriée. [116] En outre, au regard de l'article 7 2° du RGPD, le consentement au traitement des données doit être distinct de l'acceptation d'un contrat et l'acceptation ainsi de conditions générales ne saurait être considérée comme un acte positif clair exprimant un consentement à un traitement de données à caractère personnel. Le responsable du traitement doit donc s'assurer que les exigences en la matière sont strictement respectées par l'éditeur de l'application, la charge de la preuve lui incombant. Un enregistrement du consentement au regard de l'article 7 1° et du considérant 42 afin de prouver que ladite personne a consenti à l'opération de traitement est nécessaire.

Au-delà de la modélisation de l'interface de l'application devant permettre aux utilisateurs d'être informés de leurs droits ainsi que des obligations du sous-traitant et du responsable du traitement, la mise en œuvre d'une conformité by design est nécessaire avant la mise sur le marché et le déploiement de l'application de suivi médical. Cette mise en conformité by design nécessite notamment de qualifier précisément chaque partie.

B) Les obligations spécifiques en matière de partenariat et le statut du sous-traitant en matière d'application du suivi médical

L'autorité de contrôle française, la CNIL, a publié un guide pratique concernant les applications mobiles de santé en matière de protection des données personnelles.[117] Selon ce guide, certaines questions principales doivent être posées. Il convient ensuite de structurer notre réflexion à la lumière de ce guide.

En corrélation avec le principe du Privacy by design, toute application avant son développement et sa commercialisation doit établir si elle est soumise au RGPD. Si l'application a pour objet d'offrir des fonctionnalités permettant de fournir un service à distance lors de son utilisation ou si elle comporte une connexion externe, elle entre dans le champ d'application de la réglementation. L'application visée dans notre dossier de stratégie dont l'objectif est d'assurer un suivi médical à distance entre le patient et le professionnel hospitalier est donc soumise au RGPD.

En outre, ce type de demande devra respecter le principe de « minimisation » : les données à caractère personnel traitées doivent être - au regard des finalités poursuivies, devant être déterminées, explicites et légitimes - pertinentes, adéquates et limitées. En effet, seules les données nécessaires au traitement doivent être collectées.

En ce qui concerne la durée de conservation des données collectées, il est nécessaire de revenir sur la finalité de la collecte des données. Les données à caractère personnel ne peuvent être conservées

[116] L'absence d'une information obligatoire est punie d'une amende de 1 500 €. Tout traitement informatique non consenti des données recueillies est puni de 5 ans d'emprisonnement et de 300 000 € d'amende.
[117] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, « Applications mobiles en santé et protection des données personnelles : Les questions à se poser », sur cnil.fr [en ligne], publié le 17 août 2018, [consulté le 1er juillet 2020].

que pour la finalité du traitement. Dans notre cas, cela signifie la durée d'utilisation de l'application. Par exemple, le moment du suivi postopératoire. En outre, compte tenu des informations données par la CNIL, la question doit être posée en cas de suppression ou d'inactivité du compte. En effet, « concernant les applications relatives au « bien-être » n'étant pas des outils de gestion de santé, les données collectées ne peuvent être conservées au-delà de la suppression du compte ou de l'inactivité du compte ». Il est alors possible d'envisager que la suppression d'un compte patient suivi puisse éventuellement entraîner une obligation de suppression des données au sein de l'application, ces données étant déjà enregistrées dans les serveurs du responsable du traitement par le biais notamment du dossier patient (l'établissement de santé).

Enfin, si « l'application mobile est utilisée comme un outil de gestion de la santé (par exemple une application utilisée dans le cadre d'un dispositif de surveillance médicale à distance), le consentement exprès de la personne n'est pas nécessaire ».

Acteur omniprésent dans la gestion des données des patients, le sous-traitant, fournisseur de solutions cloud, est l'un des nouveaux métiers de la santé. Le sous-traitant est devenu un acteur incontournable grâce à son expertise, ses équipements et ses moyens matériels, principalement pour le traitement des données personnelles, qu'il peut mettre à la disposition des établissements de santé, responsables du traitement. En raison d'un coût supplémentaire qui serait exorbitant, le responsable du traitement ne peut ou ne veut pas prendre en charge la gestion des données des patients.

Comme énoncé précédemment, le sous-traitant doit se conformer, en de nombreuses occasions, à la même procédure que le responsable du traitement. Ainsi, son statut entraîne des obligations de conformité au regard du RGPD. Il doit donc être distingué du subordonné car il invoque sa responsabilité. En outre, il convient de traiter le sous-traitant classique de type « Cloud computing ». En effet, le type de service n'est pas nécessairement le même, il est donc impératif d'approfondir ce point. Enfin, la responsabilité de chaque acteur au sein du partenariat sera différente en fonction de son statut.

Le sous-traitant peut être considéré comme un partenaire commercial, similaire à celui envisagé dans l'HIPAA. Ainsi, le sous-traitant ne peut pas être considéré comme un subordonné. En effet, en vertu de l'article 4.8 du RGPD, le sous-traitant traite les données uniquement pour le compte du responsable du traitement. Il s'agit d'un organe externe au responsable du traitement, et possède donc une personnalité juridique distincte. Enfin, il n'y a pas de relation hiérarchique entre eux. Même si le sous-traitant ne peut pas exécuter ses tâches sans instructions du responsable du traitement, il n'agira jamais sous l'autorité de ce dernier. Cette absence de lien hiérarchique se traduira à la fois par l'inexistence d'un lien de subordination et par l'absence de gestion du traitement des données à caractère personnel au sens organisationnel et opérationnel du terme.

Dans la pratique, cependant, la différence entre le sous-traitant et le subordonné en termes de tâches est ténue. En effet, qu'est-ce qui distingue réellement l'instruction donnée par le responsable du traitement au sous-traitant des ordres donnés au subordonné ? Si l'on reprend la différence entre le travail subordonné et le travail indépendant, un premier indice peut permettre d'exprimer cette différence. Le sous-traitant agit, à la différence du subordonné, dans le cadre d'un contrat de prestation de services, en étant propriétaire de ses instruments de travail, en supportant les risques de son activité

et en pouvant refuser la mission proposée par le responsable du traitement.[118] Ainsi, outre le fait qu'il n'est pas tenu d'exécuter des tâches, le sous-traitant a certaines responsabilités distinctes de celles du responsable du traitement (respect des règles, désignation d'un délégué à la protection des données). Le sous-traitant met en œuvre des mesures techniques et organisationnelles distinctes de celles qui doivent être mises en place par le responsable du traitement. Ce point précis est essentiel. Lors de la rédaction future des mentions légales, politique de confidentialité et CGU/CGV (Conditions générales d'utilisation/Conditions générales de vente) devant être à disposition des utilisateurs, la relation entre les parties doit être clairement définie afin de permettre aux dits utilisateurs d'exercer leurs droits.

Comme nous l'avons vu précédemment, le sous-traitant n'est pas un subordonné. Mais qu'en est-il d'un statut de co-entrepreneur ? En outre, quels seront les obligations en matière contractuelle à considérer lors de la rédaction du contrat Cloud computing ?

II- - Les extensions de conformité aux regards des relations établies entre les différents acteurs

Dans la pratique, de nombreuses questions peuvent se poser quant au rôle réel du prestataire de services considéré comme un sous-traitant. Si les tâches ne sont pas suffisamment définies et que certaines exigences ne sont pas satisfaites, le prestataire de services ne peut plus être considéré comme un sous-traitant. En effet, dans la pratique, la frontière est pour le moins ténue, il est donc important d'être prudent.

Les contrats Cloud, c'est-à-dire de contrats relatifs aux services de types « cloud » qu'il s'agisse du IaaS, SaaS ou Paas, pouvant revêtirent de nombreuses situations, leur rédaction requiert une attention particulière afin d'adapter le contrat au type de relation précise souhaitée entre les parties. En effet, au-delà de la prise en considération dans ce type de contrat de l'enjeu des négociations, de – phase précontractuelle – une vigilance doit être accordé à la qualification des parties mais aussi à la règlementation particulière en matière d'hébergement de données de santé.

A) Une requalification éventuelle en tant que co-responsable du traitement du sous-traitant

Au regard de la pratique, les éditeurs de logiciels de suivi médical sont classiquement sous-traitant. Toutefois, par sa participation quant aux choix des finalités et moyens de traitements des données, l'éditeur de logiciel pourra être considéré comme responsable conjoint dès lors qu'un certain seuil d'implication sera franchi au regard de l'article 26 du RGPD et du guide[119] fournit par la CNIL. Une connaissance accrue du fonctionnement des divers type de solution Cloud mis à la disposition des utilisateurs est alors nécessaire. Enfin, afin d'éviter toute requalification possible en cas de conflit,

[118] Selon la loi et les juridictions françaises, "le rapport de subordination est caractérisé par l'exécution du travail sous l'autorité de l'employeur, qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné. Le travail dans un service organisé peut être une indication du lien de subordination lorsque l'employeur détermine unilatéralement les conditions d'exécution du travail". (Cass. soc., 13 novembre 1996).

[119] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS, "GUIDE DU SOUS-TRAITANT", édition septembre 2017 [en ligne], [consulté le 2 mars 2020].

il convient de respecter scrupuleusement les règles énoncées par le RGPD en matière de contrat de sous-traitance.

1) La notion de responsable commun du traitement des données relatives à la santé

Un grand nombre de services peuvent être considérés comme de la sous-traitance aux fins du règlement. Mais à la lumière des déclarations ci-dessus, le risque d'un responsable conjoint peut être évalué. Comme nous l'avons vu, la conformité d'un responsable du traitement ne s'arrête pas à la conformité des données à caractère personnel mais s'étend aux traitements en cours. Il doit ensuite identifier clairement les sous-traitants de données à caractère personnel, ce qui est une condition préalable nécessaire à la conformité de l'organisme avec le RGPD (garanties suffisantes pour les sous-traitants, protection des droits de la personne concernée). La frontière entre la sous-traitance et la responsabilité conjointe étant ténue, il est alors nécessaire de s'assurer exactement du pourquoi, c'est-à-dire des finalités, et du comment, c'est-à-dire des moyens essentiels. En raison de sa participation au choix des finalités et des moyens de traitement des données à mettre en œuvre, le sous-traitant peut, dès qu'un certain seuil est franchi, voir sa responsabilité accrue. Selon l'article 26 du RGPD, le sous-traitant ne sera alors plus considéré comme un sous-traitant mais comme un co-responsable du traitement. Ce co-responsable se retrouve souvent dans les services Cloud. Par exemple, un éditeur qui propose un « clé en main » dans le cadre du Cloud Computing de type SaaS, pourrait désormais être considéré comme co-responsable du traitement mis en œuvre pour en avoir déterminé les moyens. En effet, dans ce cas précis, le responsable du traitement n'aurait fait que déterminer les finalités.

La détermination de la finalité du traitement entraînera systématiquement la qualification du responsable du traitement. En revanche, en ce qui concerne les moyens, la détermination doit porter sur les aspects essentiels du traitement pour être qualifiée comme telle. Ceux-ci comprennent notamment la détermination des données à caractère personnel à traiter, la détermination de la durée de conservation et/ou les mesures concernant l'accès telles que les autorisations.

En outre, plusieurs règles énoncées dans le RGPD et appliquées dans notre analyse peuvent, selon nous, permettre de déterminer si le sous-traitant est effectivement un co-responsable du traitement : transparence (le prestataire se présente-t-il sous son propre nom ?), niveau d'éducation, niveau de contrôle des services et des données, expertise-lui permettant d'imposer les moyens à mettre en place, etc.

Comme indiqué dans l'introduction de ce chapitre, l'article 4.2 qui définit le traitement comprend un large éventail de mesures. Toutefois, dans le cas d'un service de cloud computing, qui peut constituer un service d'externalisation, cela n'est pas automatique. En effet, il est possible de distinguer trois sous-catégories de services de cloud computing : le logiciel en tant que service (Saas), l'infrastructure en tant que service (Iaas) et la plate-forme en tant que service (Paas). Le cloud computing de type « Software as a service », comme son nom l'indique, est la fourniture d'un service d'hébergement sur les serveurs de l'organisation externe pouvant déterminer les conditions d'utilisation de leurs services tel que le droit d'accès aux données ou le droit d'effectuer leur propre

traitement. En effet, le responsable du traitement demande d'héberger des données à caractère personnel mais ceux-ci sous conditions variables en fonction de contrat. Ainsi, en tant que sous-traitant ou co-responsable, il a des obligations qui lui incombent. A l'inverse, dans le cas d'un service dit « infrastructure en tant que service », seule la fourniture de matériel est mise à la disposition du responsable du traitement ; il s'agit de la fourniture d'une infrastructure externe c'est-à-dire d'un hébergement managé (prise en charge de l'installation des serveurs de fichiers, des réseaux et du stockage des données). On ne peut donc pas considérer que ce type de service relève de la définition de « sous-traitant » donnée par le RGPD. Enfin, dans le cas du service « Platform as a service », le client loue l'exploitation des serveurs et des outils intégrés (serveurs, stockage et réseaux, le prestataire de services fournit également toutes les applications middleware : système d'exploitation, base de données, serveur web). Ces différents éléments doivent donc être pris en considération. En effet, le service fourni par l'application mobile peut être composé de services d'externalisation classiques mais aussi de cloud-computing de type PaaS ou SaaS. Dans notre cas, compte tenu des services offerts par ce type d'application de suivi médical, il peut s'agir d'un sous-traitant ou d'un co-responsable de traitement suivant le fait notamment qu'il s'agisse ou non d'une solution dite « clé en main ».

Étant donné que le type d'application visé dans le présent document stratégique peut offrir certains de ces services de cloud computing, il convient donc d'aborder cette question avant la conclusion de tout partenariat afin de garantir la conformité opérationnelle et d'éviter toute sanction. La règle du respect de la vie privée by design est alors la règle d'or.

Enfin, il convient de rappeler que la responsabilité conjointe ne signifie pas une responsabilité égale.[120]

Afin d'assurer le rôle de chaque acteur. L'objectif étant de respecter la conformité requise par le RGPD ainsi que d'éviter autant que possible toute requalification ultérieure, la relation entre le responsable du traitement, le coresponsable ou le sous-traitant doit être formalisée.

2) L'obligation de formaliser la relation entre le responsable du traitement et le sous-traitant

Classiquement, au regard de la pratique, la majorité des éditeurs de logiciels de suivi médical sont considérés au terme du contrat conclu avec les établissements de santé comme des sous-traitants. En effet, malgré la mise à disposition d'une solution « clé en main » de Cloud computing, seul l'établissement de santé est responsable du traitement, notamment pour des raisons pratiques. On peut estimer que l'établissement de santé souhaitant avoir la main sur l'ensemble des traitement – notamment au regard du caractère sensible de ces données – ayant pour finalité de préparer l'hospitalisation du patient et/ou d'assurer le suivi médical. L'établissement de santé pourra généralement, aux termes du contrat, déterminer selon son protocole interne les données pouvant faire l'objet d'une collecte et d'un traitement à des fins administratives et médicales.

En ce qui concerne la sous-traitance, un contrat de sous-traitance devrait être conclu afin de s'assurer, en particulier, que le sous-traitant fournit des garanties suffisantes quant à la mise en œuvre

[120] CJUE, 5 juin 2018, affaire C-210/16.

de mesures techniques et organisationnelles appropriées, qu'il agit en tant que sous-traitant et qu'il n'est ni un responsable subordonné ni un responsable commun du traitement. En effet, à la lumière de l'article 28, paragraphe 3, du RGPD, le traitement effectué par un sous-traitant est régi par un contrat ou un autre acte juridique relevant du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant au responsable du traitement, qui définit la finalité et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement.

Les garanties prévues aux articles 28 et 32 du RGPD sont constituées par des clauses contractuelles. En effet, le règlement prévoit que le responsable du traitement doit fixer les conditions de la communication des données à caractère personnel. Un travail de rédaction important est donc indispensable.

Plusieurs points à traiter dans le cadre du contrat de sous-traitance peuvent être soulevés.
Le contrat doit en effet contenir des clauses afin de :
- indiquer clairement la politique du sous-traitant en matière de protection des données à caractère personnel,
- décrire le traitement externalisé,
- documenter les moyens utilisés et les fins (qui a déterminé quoi) et la nature des opérations,
- documenter les instructions données au sous-traitant en matière de sécurité et de confidentialité des données,
- définir les règles de gestion et de notification des incidents,
- indiquer la possibilité pour le sous-traitant de faire appel ou non à un autre sous-traitant,
- les garanties des droits des personnes concernées,
- la vérification des contrats existants pour les mettre en conformité avec le RGPD, notamment par le biais d'avenants.

Pour plus d'informations sur les clauses types, le site de la CNIL consacre une page à ce sujet : https ://www.cnil.fr/fr/sous-traitance-exemple-de-clauses.

Enfin, le service de sous-traitance ne doit pas être lancé sans avoir signé un contrat avec le prestataire de services énonçant les exigences prévues à l'article 28 du règlement général sur la protection des données. Dans le cas contraire, le responsable du traitement sera tenu responsable du non-respect de ces exigences. Enfin, en cas de traitement total ou, dans le cas des applications de suivi médical, pour une partie de l'utilisation des services de cloud computing, une obligation de veiller à ce qu'une garantie soit mise en place quant à la localisation géographique réelle des données et de vérifier les conditions juridiques et les éventuelles formalités auprès de l'autorité nationale de contrôle pour les transferts de données en dehors de l'Union européenne.

En cas de conclusion d'un contrat de prestation avec un tiers concernant la fourniture d'une solution Cloud computing, la rédaction du contrat est-elle similaire à celle du contrat type de sous-traitance ou demande-t-elle un aménagement ?

B) La distinction de rédaction du contrat Cloud computing du contrat de sous-traitance classique

Au regard de la variété des prestations pouvant être proposées par un fournisseur de service Cloud computing, la première étape afin de déterminer la nature du contrat est de déterminer précisément quelles prestations en font l'objet. En effet, l'identification des règles applicables en matière de contrats spéciaux dépendra du type de prestations nécessaire. Bien qu'une partie de la doctrine, au regard du caractère immatériel des données, n'envisage pas la possibilité d'appliquer le régime du contrat de dépôt en matière d'hébergement de données, le mouvement de dématérialisation des biens et les conditions rends l'application de ce type de contrat possible. Dans le cas d'hébergement de données, le responsable de traitement confierait celles-ci à un prestataire afin d'en assurer la garde pour une période déterminée. Le dépôt au regard de l'article 1915 du Code civil revêt cette définition. Dans tout type de contrat de Cloud computing, la question de l'hébergement et des droits et obligations afférentes constituent une partie essentielle des négociations (confidentialité, disponibilité et intégrité des données). Au regard des règles imposés en matière de protection des données à caractère personnel, l'utilisation du régime du contrat de dépôt peut être avantageux afin de compléter la règlementation et ne contreviendrait au regard des articles 1927 à 1946 du Code civil pas au RGPD. [121] Par exemple, la confidentialité des données au regard du RGPD mais aussi le secret du dépôt au regard du régime du contrat de dépôt seraient garantis.

Ainsi, l'application cumulative du régime du contrat de dépôt et d'entreprise lors de la rédaction d'un contrat Cloud computing pourrait être opportun.

En pratique, est retenue seulement l'utilisation du contrat d'entreprise, en matière de Cloud computing afin de permettre contre rémunération l'exécution d'un travail déterminé[122]. Ce type de contrat va alors permettre d'englober une variété de prestations. Bien que constitué de dispositions encadrant ce type de contrat, il englobe les obligations relevant du droit commun[123] et nécessite une rédaction précise, rigoureuse et faisant suite à des négociations précontractuelles suffisantes. C'est pourquoi la quantité et qualité des services, la qualité des parties et les conditions de conservations, réversibilité et portabilité des données au regard de l'amplitude de possibilités de rédactions doit être envisagé en toute connaissance du droit et des évolutions futures.

En plus de la rédaction d'un contrat qui soit complet et conforme, il conviendra toujours de veiller au sein d'un contrat cloud computing à la confidentialité et sécurité des données mais aussi de spécifier le cas des transferts vers un pays tiers. L'ensemble de ses obligations devront notamment faire l'objet d'articles au sein des conditions générales d'utilisation et de vente.

En fonction de s'il s'agit d'un contrat cloud de sous-traitance ou de co-traitance, la rédaction des articles ne sera pas la même. En effet, en cas de services notamment de type SaaS contenant des

---

[121] L'article 1937 du Code civil permet par exemple à l'éditeur de l'application d'être le destinataire des données et l'article 1342-1 d'empêcher celui-ci de faire appel à un sous-traitant sans l'accord préalable de l'établissement de santé.

[122] Article 1710 du Code civil

[123] Notamment l'obligation de bonne foi et le devoir d'information.

fonctionnalités métiers[124], une partie de la finalité des traitements est souvent partagée. Même si le contrat SaaS et d'hébergement de cette étude permet d'estimer que sera conclu vraisemblablement des contrats cloud de sous-traitance, l'énonciation des deux types de rédaction des articles du contrat paraît opportun (tableau 2) :

Spécificités : articles comparés en matière de contrat Cloud computing	
Responsabilité conjointe	**Sous-traitance**
Description du traitement : - « Finalité(s) » : un article concernant le partage des missions quant à la ou les finalités du traitement - « Moyens » : énonciation de l'ensemble des mesures techniques et organisationnelles	Description du traitement : - « Finalités » : rappel des finalités - « Moyens » : rappel des moyens fournit par le prestataire du service Cloud
Formalisme de la relation : établissement des obligations respectives	Obligations du sous-traitant : les obligations générales du sous-traitants (les traitements sur la base d'instructions du responsable de traitement) ainsi que l'énonciation des interdictions à son encontre (interdiction de copies, stockages, divulgations, etc…)
Obligation de transparence à l'égard des tiers : mise à disposition des tiers de la répartition de leur rôle	×
×	Obligations substantielles propres au sous-traitant (obligation de vigilance et d'alerte, de conseil et d'assistance, d'information, sort des données, etc …)
×	Obligations du responsable de traitement vis-à-vis du sous-traitant
×	Les obligations communes aux parties au regard de l'article 28 du RGPD

Tableau 2 : Articles comparés en matière de contrat Cloud computing

En matière d'hébergement de données de santé, il convient de se référer au Code de la santé publique. En effet, comme il a pu être mentionné au sein de cette étude, le droit français a complété le texte en matière de protection des données à caractère personnel. Ainsi, l'article R 1111-11 du CSP permet d'envisager la façon dont ce type de contrat entre l'hébergeur et le client doit être conclu. En vertu de cet article, le prestataire de solutions cloud et l'éditeur de l'application devra conclure un contrat comprenant au minimum 14 clauses obligatoires[125]. Enfin, comme l'énonce le §2 de l'article R.1111-11 du CSP, dès lors que « le responsable de traitement de données de santé […] fait appel à un prestataire qui recourt lui-même pour l'hébergement des données à un hébergeur certifié, le contrat qui lie le responsable de traitement […] avec son prestataire reprend les clauses mentionnées au I telles qu'elles figurent dans le contrat liant le prestataire et l'hébergeur certifié ».

[124] Lorsque l'on parle de fonctionnalité métiers, il convient de se référer à la notion de fonction logiciel métiers spécifique qui est une fonction développée pour répondre à des besoins spécifiques, réalisée sur mesure selon un cahier des charges précis.
[125] Se référer à l'annexe 5 énonçant ces clauses

Ainsi, le contrat de sous-traitance entre l'établissement de santé et l'éditeur de l'application devra prendre en considération ce texte en amont de la rédaction du contrat de sous-traitance.

Conclusion

Au vu des observations faites, les législations américaine et européenne s'accordent pour mettre en place une législation contraignante forte en matière de protection et de confidentialité des données de santé. En effet, ces deux législations comportent des garanties administratives, organisationnelles, techniques et physiques.

Cependant, sur le plan pratique, il semble plus compliqué pour un justiciable de connaître les lois fédérales américaines applicables. En effet, contrairement au droit européen, le droit fédéral américain en matière de protection des données est sectoriel.

Contrairement au droit fédéral américain, le droit européen peut manquer d'outils d'orientation qui permettrait au justiciable d'avoir une première indication avancée du type de conformité à mettre en œuvre. Cependant, les autorités de contrôles comme la CNIL rédige de plus en plus de référentiels et d'avis afin de les aider.

D'un point de vue juridique, le droit américain s'appliquant au prestataire d'un service de type Saas, par exemple, celui-ci peut se voir dans l'obligation de garantir une certaine conformité, bien que souvent similaires, imposées par des textes différents, entraînant ainsi un fort manque de clarté. En outre, comme l'a déclaré Lauren Steinfeld : « les prestataires de soins de santé qui continuent à facturer en utilisant des dossiers papier, des fax et des courriers […] ne sont pas couverts par l'HIPAA […]. Comment cela est-il possible ? Pourquoi les patients de ces organisations mériteraient-ils moins de respect à de leur vie privée que ceux des cabinets et des hôpitaux qui facturent par voie électronique ? Eh bien, ce n'est pas qu'il y ait une raison politique de traiter ces deux populations différemment. Cependant, l'autorité statutaire que le Congrès a accordée, a été construite sur les prémisses qu'un partage électronique accru des données facilité par les nouvelles dispositions de simplification administrative de l'HIPAA devrait s'accompagner de protections supplémentaires aux fins de protection de la vie privée. En d'autres termes, les particularités et les aspects techniques d'une loi peuvent parfois avoir une incidence considérable sur le fait qu'une organisation soit soumise ou non à un régime de conformité ». La pratique américaine sur ce point est donc regrettable.

En ce qui concerne le droit européen, la question du reclassement du sous-traitant en tant que responsable conjoint, bien qu'elle ait une corrélation directe avec le droit du travail, reste à résoudre. En effet, qu'est-ce qui distingue réellement la sous-traitance de la co-direction ? La différence est, à notre avis, beaucoup trop ténue et mérite d'être précisée. Cependant, contrairement au droit américain, il est opportun de faire remarquer la volonté du droit français, en accordance avec le RGPD, de légiférer en matière d'hébergement de données de santé. Cette légifération en la matière permet de garantir un niveau de confidentialité et de sécurité adéquat par le biais de certificats mais aussi par le biais d'exigences contractuelles. Bien que la création d'un régime spécial en matière de contrat Cloud computing, pouvant évoluer avec le temps, serait plus que bienvenu afin de « lisser » la pratique

actuelle, les efforts du droit français – face au manque de législations du droit américain – est prometteur.

Enfin, ces deux régimes, bien qu'ils présentent certains inconvénients, sont suffisamment bien construits et équilibrés pour offrir de solides garanties aux personnes concernées. Quant aux entreprises, leur implantation sur ces deux territoires peut être avantageuse dans un sens. En effet, le respect de ces règles peut être apprécié comme une garantie de la qualité de protection des données personnelles mise en œuvre et, plus encore, comme une volonté de l'entreprise d'apporter des garanties aux patients et aux établissements de santé.

Toutefois, au regard notamment du Cloud act, un avertissement doit être formulé. Tout entreprise souhaitant contracter avec une entreprise américaine doit prendre en compte les risques pouvant résulter de cette loi. En effet, en cas d'enquêtes des forces de l'ordre américaines, un contentieux pourrait naître afin de défendre le non-transfert des données des personnes concernées. Plus de vigilance devra être accordée lors des négociations contractuelles sur ce point. Cependant, bien qu'un risque réel existe – ce qu'à démontrer la CJUE en invalidant le Privacy Shield – il existe toutefois aujourd'hui des moyens juridiques mais aussi techniques afin d'empêcher toute captation de données par les autorités américaines tant qu'un accord ne sera pas conclu.

Notes de bas de page

[1] MALAFOSSE Jeanne Bossi, BANDON-TOURRET Diane, *Lancer un projet e-santé*, Editions Legislatives, 2020, p.14.

[2] Société nouveal e-santé, « Les parcours de soins connectés avec e-fitback » [en ligne], [consulté le 25 juillet 2020]

[3] Cabinet Alain Bensoussan Avocats Lexing, « Cloud computing et droit, retour sur une année de grands changements », *Revue Lamy Droit de l'Immatériel, Nº 138.*, [en ligne] 1er juin 2017, p. 2 [consulté le 25 juillet 2020].

[4] La Commission Nationale de l'Informatique et des Libertés (CNIL) est l'autorité de contrôle française en matière de données, il s'agit du régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

[5] Bien avant qu'apparaisse l'expression " Cloud Computing ", les architectes réseau schématisaient Internet par un nuage. En anglais, le terme « the Cloud », était couramment utilisé pour désigner Internet.

[6] COMMISSION NATIONALE INFORMATIQUE ET LIBERTES, "Cloud computing : les conseils de la CNIL pour les entreprises qui utilisent ces nouveaux services", publié le 25 juin 2012 [en ligne], [consulté le 12 juin 2020], sur https://www.cnil.fr/

[7] MELL Peter, GRANCE Tomothy, « Recommendations of the National Institute of Standards and Technology : The NIST Definition of Cloud Computing », *NIST Special Publication 800-14* [en ligne], septembre 2011, p. 2 [consulté le 25 juillet 2020]

[8] Ibid.

[9] Art. 4, 15 du règlement (UE) 2016/679

[10] Le Congressional Research Service, une composante de la Bibliothèque du Congrès, effectue des recherches et des analyses pour le Congrès sur un large éventail de questions de politique nationale.

[11] F. FEFER Rachel, « Data Flows, Online Privacy, and Trade Policy », *Congressional Research Service Report* [en ligne], mars 2019, sommaire, [consulté le 25 juillet 2020]

[12] Accord général sur le commerce des services de l'OMC, Effort plurilatéral de l'OMC, Lignes directrices de l'OCDE sur la protection de la vie privée, Déclaration ministérielle sur l'économie numérique du G-20 de 2018, Cadre de protection de la vie privée de l'APEC de 2005 ou Règles transfrontalières de l'APEC sur la protection de la vie privée.

[13] Commission européenne, Recommandation de décision du Conseil autorisant l'ouverture de négociations en vue de la conclusion d'un accord entre l'Union européenne et les États-Unis d'Amérique sur l'accès transfrontalier aux preuves électroniques aux fins de la coopération judiciaire en matière pénale, COM, 70 final, 2019, p. 1.

[14] Il s'agit d'un ancien texte adopté en 1986 permettant les communications de données électroniques sur le sol américain. Ce texte n'envisageait pas à l'époque la situation où les données électroniques sont accessibles depuis les États-Unis mais stockées sur des serveurs à l'étranger.

[15] Treaties and Agreements, sur U.S Departement of State Archive, [en ligne] publié le 7 mars 2012, [consulté le 25 juillet 2020]

[16] CONGRES AMERICAIN, Public Law 114-26, titre I, Sect. 102 (b)(6)(C), 9 juin 2015, 129 STAT. 319

[17] L'administration Trump a retiré les États-Unis de l'accord en janvier 2017. Toutefois, l'accord reflète la politique américaine en matière de données personnelles, qui était encore similaire sous l'administration Trump.

[18] Cette exigence s'inscrit à la suite de l'arrêt de la CJUE dit « Schrems I », du 6 octobre 2015 dans l'affaire C-362/14 Maximillian Schrems / Data Protection Commissioner antérieur à l'arrêt du 16 juillet 2020 dit « Schrems II » invalidant le Privacy Shield.

[19] INTERNATIONAL TRADE ADMINISTRATION, European Businesses, sur *Privacy Shield Framework* [en ligne], [consulté le 10 février 2020 et 20 aout 2020]

[20] INTERNATIONAL TRADE ADMINISTRATION, « Obligatory Contracts for Onward Transfers », sur *Privacy Shield Framework* [en ligne], [consulté le 10 février 2020 et 20 aout 2020]

[21] JELINEK Andrea, « Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems », sur le site du Comité européen de la protection des données [en ligne], adopté le 23 juillet 2020 [consulté le 25 juillet 2020]

[22] Il sera détaillé l'importance du choix d'un service d'hébergement et les règles afférentes au sein des chapitres suivants.

[23] KADZIK Peter, Lettre de l'assistant du général de division au vice-président Joseph R. Biden, président du Sénat des États-Unis [courriel], 15 juillet 2016.

[24] Ibid.

[25] CALLAWAY David et DETERMANN, « The New US Cloud Act – History, Rules, and Effects », The Computer & Internet Lawyer, Vol. 35, n°8, 2018, §III.

[26] Titre 18 du Code des États-Unis, Chap. 119 - Interception des communications filaires et électroniques et interception des communications orales, §2510(15) [en ligne] : « tout service qui fournit [...] aux utilisateurs [...] la possibilité d'envoyer ou de recevoir des communications par fil ou par voie électronique »).

[27] Titre 18 du Code des États-Unis, Chap. 121 – Accès aux communications électroniques et aux documents transactionnels stockés, § 2711(2) [en ligne] : l 'expression "service informatique à distance" désigne la fourniture au public de services de stockage ou de traitement informatique au moyen d'un système de communications électroniques.

[28] Titre 18 du Code des États-Unis, Chap. 121, § 2711 [en ligne]

[29] Le fournisseur, « y compris un service de communication électronique étranger ou tout service information à distance.

[30] Il convient de noter qu'une requête en annulation nécessite qu'un tribunal américain procède à une analyse de courtoisie. Nous étudierons dans notre seconde partie les conséquences de cette analyse en matière de choix d'hébergeur pour une entreprise ou un hôpital français.

[31] La courtoisie internationale est à distinguer notamment du droit international public. Il s'agit d'un ensemble d'usage suivis à titre de simples convenances et pour des raisons de commodité pratique. Dans le contexte de l'internationalisation, la courtoisie constitue une coopération fortement utilisée supposant qu'un pays examine la demande que lui adresse un autre pays en vue d'engager ou d'élargir une procédure d'application de ses réglementations afin de mettre un terme à une pratique gravement préjudiciable aux intérêts du pays requérant.

[32] Titre 18 du Code des États-Unis, Chap. 121 §2523(b)(1) [en ligne]

[33] Annexe 1.

[34] Considérant 101 du Règlement(UE) 2016/679

[35] CNIL, « La protection des données dans le monde, sur le site de la CNIL » [en ligne], publié le19 novembre 2019, [consulté le 20 mars et 25 août 2020].

[36] La compatibilité avec le RGPD a été exigée en ce qui concerne ses règles d'accès aux données à des fins de procédures pénales et de sécurité nationale et ses conditions juridiques spécifiques permettant aux européens de porter plainte contre des entreprises japonaises.

[37] BOURGEOIS Mattier, « CLOUD COMPUTING - Notions et enjeux», JurisClasseur Communication [en ligne], mai 2020, [consulté le 27 juillet 2020]

[38] Titre 18 du Code des États-Unis, Chap. 121, §2703(h)(1)(A)(i)

[39] Titre 18 du Code des États-Unis, Chap. 121, § 2703(h)(2)(B)

[40] JACOB Patrick, « Quand les nuages ne s'arrêtent pas aux frontières, Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », *Cahier de droit de l'entreprise*, n° 4, dossier 28, Juillet 2018 -Lexis 360® [consulté le 14 juillet 2020].

[41] BISMUTH Regis, « Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ? », *Revue critique de droit international privé*, [en ligne] 2019, p.681, [consulté le 12 août 2020].

[42] Cloud Act, H.R. 4943 § 103(c)

[43] AUGAGNEUR Luc-Marie, Héberger ses données chez les GAFAM : quel discours croire sur le Cloud Act ?, Revue Lamy Droit de l'Immatériel, Nº 162, [en ligne] 1er août 2019, [consulté le 12 août 2020].

[44] CHRISTAKIS Théodore, « a communication aux autorités américaines de données sur la base du Cloud Act est-elle en conflit avec le règlement général sur la protection des données ? », *Revue critique de droit international privé* 2019/3 (N° 3), pages 695 à 707, [en ligne], [consulté le 11 août 2020].

[45] Comme l'énonce le professeur Regis Bismuth : « Le RGPD peut avoir une portée extraterritoriale car il a ainsi vocation à s'appliquer dans la situation où les données d'un américain vivant aux États-Unis et qui n'a jamais été en Europe sont stockées dans un serveur situé dans l'UE. Même dans ce cas, un prestataire tel que Facebook, Google ou Microsoft ne pourrait accéder à la demande des autorités américaines de transférer directement ces données sans contrevenir aux dispositions du RGPD. » Ainsi, un réel conflit de lois peut être envisageable dès lors que l'interprétation du RGPD fait l'objet de plus de clarté. En effet, même en cas d'un futur accord intergouvernemental avec les États-Unis, le manque de clarté notamment de l'article 49 du RGPD posera toujours problème.

[46] Article 45 du Règlement (UE) 2016/679

[47] Article 46 du Règlement (UE) 2016/679

[48] Article 47 du Règlement (UE) 2016/679

[49] Article 48 du Règlement (UE) 2016/679

[50] Cette décision a remis en cause la décision d'adéquation existant entre l'Union Européenne et les États-Unis.

[51] Lignes directrices 2/2018 sur les dérogations à l'article 49 du 2016/679, p. 5.

[52] Il s'agit d'un ancien groupe de travail.

[53] Il s'agit d'un service notamment d'hébergement des données de santé ayant obtenu en janvier 2019 en France la certification HDS.

[54] MERCIER Anne-Laure, « Stephan Hadinger (AWS France) : "Un client optant pour un stockage en France a l'assurance que ses données y restent bien" », sur mindhealth [en ligne], publié le 28 mai 2019, [consulté le 31 juillet 2020].

[55] CONGRES AMERICAIN, Loi sur la portabilité et la responsabilité de l'assurance maladie (Health Insurance Portability and Accountability Act), 1996.

[56] U.S. DEPARTEMENT OF HEALTH AND HUMAN SERVICES, « Règlement de simplification administrative » [en ligne], mars 2013, p. 11-12.

[57] U.S. DEPARTEMENT OF HEALTH AND HUMAN SERVICES, Texte du règlement de simplification administrative de l'HIPAA, mars 2013, p. 14.

[58] Un site web du gouvernement fédéral géré et payé par les centres américains pour les services Medicare et Medicaid.

[59] ADMINISTRATION DE LA SECURITE SOCIALE AMERICAINE, Titre 18 du Code des États-Unis, Sect. 1861, Part. E, Sec. 1861, Compilation des lois sur la sécurité sociale [en ligne].

[60] HigherEducation, « The Medical Billing Process », sur MB&CC [en ligne], [consulté le 20 juillet 2020].

[61] DEPARTEMENT DE LA SANTE ET DES SERVICES SOCIAUX, « Covered Entities and Business Associates », [en ligne], publié le 16 juin 2017, [consulté le 27 août 2020]

[62] Un expert-comptable (CPA) est un professionnel de la comptabilité qui a réussi l'examen uniforme de CPA. La désignation CPA est une certification d'expertise dans le domaine de la comptabilité.

[63] Il s'agit d'un résumé schématique des "Directives sur les entités couvertes" établi pour cette carte de visite.

[64] DEPARTEMENT DE LA SANTE ET DES SERVICES SOCIAUX, Guide de normes de simplification administrative adoptées par le HHS en vertu de la loi de 1996 sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA), [en ligne], [consulté le 20 février 2020].

[65] DEPARTEMENT DE LA SANTE ET DES SERVICES SOCIAUX AMERICAIN, « May a HIPAA covered entity or business associate use a cloud service to store or process ePHI? », [en ligne], publié le 6 octobre 2016 sur hhs.gov, [consulté le 25 juin 2020].

[66] Il s'agit de la norme d'évaluation du paragraphe §164.308(a)(8) de la règle de sécurité.

[67] DEPARTEMENT DE LA SANTE ET DES SERVICES SOCIAUX, « Security Standards: Administrative SafeguardsSecurity », *HIPAA Security SERIES* [en ligne], 2005, Vol. 2, [consulté le 20 février 2020].

[68] Security Rule, §164.308(b)(1)

[69] Nous apporterons plus de précisions à ce sujet.

[70] Security Rule, §164.308(a)(7)

[71] Security Rule, §164.308(a)(5)

[72] Security Rule, §164.308(a)(6)

[73] Security rule §164.312(a)(1)

[74] Security rule §164.312(a)(2)(i)

[75] Security rule §164.312(a)(2)(ii)

[76] Security rule §164.312(b)

[77] Security rule §164.312(c)(1)

[78] BUREAU DES DROITS CIVILS, U.S. DEPARTEMENT OF HEALTH AND HUMAN SERVICES « MODEL NOTICES OF PRIVACY PRACTICES QUESTIONS AND INSTRUCTIONS », [en ligne], 2014 , [consulté le 20 février 2020] et « MODEL : Your Information. Your Rights. Our Responsibilities », [en ligne], 2014, [consulté le 20 février 2020].

[79] BUREAU DES DROITS CIVILS, U.S. DEPARTEMENT OF HEALTH AND HUMAN SERVICES, « OCR PRIVACY BRIEF, SUMMARY OF THE HIPAA PRIVACY RULE », [en ligne], 2003, p. 11-13, [consulté le 20 février 2020].

[80] Il s'agit d'une infrastructure dans laquelle la puissance de calcul et le stockage sont gérés par des serveurs distants auxquels les usagers se connectent via une liaison Internet sécurisée.

[81] U.S. DEPARTEMENT OF HEALTH AND HUMAN SERVICES, « Guidance on HIPAA & Cloud Computing », sur HHS.gov [en ligne], publié le 16 juin 2017, [consulté le 7 mars 2020].

[82] 45 CFR § 164.504 (e) (2) (ii) (E) - (G)

[83] Se référer notamment à l'accord de résolution conclut avec le Département de santé et services sociaux des États-Unis ainsi qu'au communiqué de presse du gouvernement.

[84] SCARFORNE Karen, SOUPPAYA Murugiah, SEXTON Matthew, « Guide to Storage Encryption Technologies for End User Devices », sur CSRC [en ligne], publié en novembre 2007, [consulté le 25 mars 2020].

[85] « Instructions for Completing AHC11236 Business Arrangement and Relationships Application », sur Alberta [en ligne], [consulté le 26 mars 2020].

[86] STEINFELD Lauren, « Privacy law and data protection », sur *Coursera*, 2020 [consulté le 10 mai 2020].

[87] qui est "... destiné à être utilisé pour le diagnostic de maladies ou d'autres affections, ou pour le traitement, l'atténuation, la guérison ou la prévention de maladies, chez l'homme ..." ou "... destiné à affecter la structure ou toute fonction du corps de l'homme ou d'autres animaux ..." et "ne comprend pas les fonctions logicielles exclues en vertu de l'article 520(o) de la loi FD&C.". Ainsi, les applications logicielles qui s'exécutent sur un ordinateur de bureau, un ordinateur portable, à distance sur un site web ou un "nuage", ou sur un ordinateur de poche peuvent être soumises à la réglementation des dispositifs si elles sont destinées à être utilisées pour le diagnostic ou la guérison, l'atténuation, le traitement ou la prévention d'une maladie, ou pour affecter la structure ou toute fonction du corps humain. Le niveau de contrôle réglementaire nécessaire pour assurer la sécurité et l'efficacité varie en fonction du risque que le dispositif présente pour la santé publique.

[88] CHAPITRE 1, I, B. Les exigences de conformité principales : sécurité et confidentialité.

[89] Security Rule 45 CFR §164.314(a)(2)(i)(B)

[90] Il s'agit des concepteurs et des développeurs de l'application ou de l'entité ayant commandité l'application.

[91] Une vérification peut être faite par le biais des déclarations d'audites produite par l'American Institute of Certified Public Accountants Auditing Standards Board. Aujourd'hui, il s'agit de la Statement on Standards for Attestation Engagements No. 18 (SSAE 18).

[92] CHAPITRE I, II- L'application de la loi HIPAA en matière d'hébergement de données de santé.

[93] L'ensemble de ces règles sont à respecter aussi bien en vertu du droit fédéral américain que du droit français.

[94] Enumération résultant de discutions avec des professionnels notamment un responsable sécurité des systèmes d'information et un ingénieur préparant une thèse dans le domaine des télécommunications.

[95] Article 4§7 du Règlement (UE) 2016/679

[96] Didier Ambroise est le fondateur de Doshas Consulting, un cabinet de conseil spécialisé dans la santé, l'assurance et la protection sociale. Ce cabinet a accompagné une majorité d'acteurs de la santé en matière de respect du RGPD.

[97] Article 4 du Règlement (UE) 2016/679 : « données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne ».

[98] Article 9 §2 du Règlement (UE) 2016/679

[99] DE TERWANGNE Cécile, ROSIER Karen, « Le règlement général sur la protection des données (RGPD / GDPR) : analyse approfondie », Edition Larcier, 2018, p746, §46.

[100] Considérant 81 du Règlement (UE) 2016/679 : "L'adhésion du sous-traitant à un code de conduite approuvé ou à un mécanisme de certification approuvé peut être utilisée comme élément pour démontrer le respect des obligations du responsable du traitement".

[101] COMMISSION NATIONALE INFORMATIQUE & LIBERTES, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », sur cnil.fr [en ligne], [consulté le 20 juin 2020].

[102] COMMISSION NATIONALE INFORMATIQUE & LIBERTES, « Outil PIA : téléchargez et installez le logiciel de la CNIL », sur cnil.fr [en ligne], publié le 24 juin 2020, [consulté le 20 juin 2020].

[103] Article 9§4 du Règlement (UE) 2016/679

[104] Afin d'identifier en cas de doute s'il s'agit d'un dispositif médical, la lecture des lignes directrices du MEDDEV 2.1/6 de juillet 2016 peut être opportun.

[105] Article L. 5211-1 du Code de la santé publique

[106] L'ANS est l'agence française régulant la e-santé en posant des cadres et bonnes pratiques. Elle conduit les projets d'intérêt national ainsi que le déploiement national et territorial des projets e-santé.

[107] La norme ISA 17021 prend en compte l'ensemble des normes internationales reconnus tel que la norme ISO 27001 relative au système de gestion des la sécurité des systèmes d'information, la norme ISO 20000-1

relative au système de gestion de la qualité des services, la norme ISO 27018 relative à la protection des données à caractère personnel et de la norme ISO 27017 portant sur les aspects de la sécurité de l'information du cloud computing.

[108] Une liste des hébergeurs certifiés et des organismes accrédités est disponible sur le site de l'ANS.

[109] Art R. 1112-7 du Code de la santé publique

[110] Considérant 77 du Règlement (UE) 2016/679

[111] Art 12 du Règlement (UE) 2016/679

[112] Voir annexe 4 à propos des mesures à mettre en place.

[113] Considérant 85 du Règlement (UE) 2016/679 : "comme la perte de contrôle sur leurs données à caractère personnel ou la limitation de leurs droits, la discrimination, l'usurpation ou la fraude d'identité, la perte financière, l'annulation non autorisée de la pseudonymisation, l'atteinte à la réputation, la perte de confidentialité des données à caractère personnel protégées par le secret professionnel ou tout autre désavantage économique ou social important pour la personne physique concernée".

[114] Article 33.3 du Règlement (UE) 2016/679 : "Notification d'une violation de données à caractère personnel à l'autorité de contrôle".

[115] FALQUE-PIERROTIN Isabelle, GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES, « Lignes directrices concernant les délégués à la protection des données (DPD) », WP 243 rev.01 [en ligne], 2017, p. 8-11, [consulté le 1er juillet 2020].

[116] L'absence d'une information obligatoire est punie d'une amende de 1 500 €. Tout traitement informatique non consenti des données recueillies est puni de 5 ans d'emprisonnement et de 300 000 € d'amende.

[117] COMMISSION NATIONALE INFORMATIQUE & LIBERTES, « Applications mobiles en santé et protection des données personnelles : Les questions à se poser », sur cnil.fr [en ligne], publié le 17 août 2018, [consulté le 1er juillet 2020].

[118] Selon la loi et les juridictions françaises, "le rapport de subordination est caractérisé par l'exécution du travail sous l'autorité de l'employeur, qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné. Le travail dans un service organisé peut être une indication du lien de subordination lorsque l'employeur détermine unilatéralement les conditions d'exécution du travail". (Cass. soc., 13 novembre 1996).

[119] COMMISSION NATIONALE INFORMATIQUE & LIBERTES, "GUIDE DU SOUS-TRAITANT", édition septembre 2017 [en ligne], [consulté le 2 mars 2020].

[120] CJUE, 5 juin 2018, affaire C-210/16.

[121] L'article 1937 du Code civil permet par exemple à l'éditeur de l'application d'être le destinataire des données et l'article 1342-1 d'empêcher celui-ci de faire appel à un sous-traitant sans l'accord préalable de l'établissement de santé.

[122] Article 1710 du Code civil

[123] Notamment l'obligation de bonne foi et le devoir d'information.

[124] Lorsque l'on parle de fonctionnalité métiers, il convient de se référer à la notion de fonction logiciel métiers spécifique qui est une fonction développée pour répondre à des besoins spécifiques, réalisée sur mesure selon un cahier des charges précis.

[125] Se référer à l’annexe 5 énonçant ces clauses.

Bibliographie

Ouvrages spéciaux

CAPEL Elodie, GRUSON David, JAAFAR Delphine, LOULERGUE Pierre, MEHL Judith, PARMENTIER Florent, PERSON Anaïs, *La révolution du pilotage des données de santé : enjeux juridiques, éthiques et managériaux, Enjeux juridiques, éthiques et managériaux,* préface de LUCAS Jacques, LEDH Edition, 2019, 146 p.

MALAFOSSE Jeanne Bossi, BANDON-TOURRET Diane, *Lancer un projet e-santé*, Editions Legislatives, 2020, 204 p.

POULLET Yves, *Law, norms and freedoms in cyberspace, Droit, normes et libertés dans le cybermonde*, sous la direction de DEGRAVE Elise, DE TERWANGNE Cécile, DUSOLLIER Séverine, QUECK Robert, Louvain la neuve, 2018, 799 p.

DE TERWANGNE Cécile, ROSIER Karen, *Le règlement général sur la protection des données (RGPD / GDPR) : analyse approfondie.* Avant-propos d'Yves Poullet, Edition Larcier, 2018, 928 p.

Actes de colloques – Travaux collectifs – Rapports officiels

ADMINISTRATION AMERICAINE DES DENREES ALIMENTAIRES ET DES MEDICAMENTS, « Device Software Functions Including Mobile Medical Applications », [en ligne], 2019, [consulté le 2 juillet 2020] sur https://www.fda.gov/

ADMINISTRATION AMERICAINE DES DENREES ALIMENTAIRES ET DES MEDICAMENTS, « Examples of Software Functions for Which the FDA Will Exercise Enforcement Discretion », [en ligne], 2019, [consulté le 2 juillet 2020] sur https://www.fda.gov/

AGENCE DU NUMERIQUE EN SANTE, « Règlement européen sur la protection des données personnelles: une révolution, une contrainte et une opportunité », *FEHAP 1ère journée régionale « Système d'information en santé »*, 2018.

AGENCE AMERICAINE POUR LA RECHERCHE ET LA QUALITE DES SOINS DE SANTE, « Privacy and Security Solutions for Interoperable Health Information Exchange », [en ligne], 20 décembre 2007, [consulté le 2 juillet 2020], sur https://digital.ahrq.gov/:

AGENCE AMERICAINE POUR LA RECHERCHE ET LA QUALITE DES SOINS DE SANTE, « Privacy and Security Solutions for Interoperable Health Information Exchange », [en ligne], 20 décembre 2007, [consulté le 2 juillet 2020] sur https://digital.ahrq.gov/:

BUREAU AMERICAIN POUR LES DROITS CIVILS, « *Guidance on HIPAA & Cloud Computing* », [en ligne], 16 juin 2017, [consulté le 2 juillet 2020] sur https://www.hhs.gov/

BUREAU DU COORDINATEUR NATIONAL DES TECHNOLOGIES DE L'INFORMATION SUR LA SANTE, « Permitted Uses and Disclosures: Exchange for Health Care Operations

45 Code of Federal Regulations (CFR) 164.506(c)(4) », [en ligne], janvier 2016, [consulté le 2 juillet 2020] sur https://www.healthit.gov/

BUREAU DU COORDINATEUR NATIONAL DES TECHNOLOGIES DE L'INFORMATION SUR LA SANTE, « Permitted Uses and Disclosures: Exchange for Treatment 45 Code of Federal Regulations (CFR) 164.506(c)(2) », [en ligne], janvier 2016, [consulté le 2 juillet 2020] sur https://www.hhs.gov/

COMMISSION NOTIONALE INFORMATIQUE & LIBERTES, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », [en ligne], [consulté le 17 juillet 2020] sur https://www.cnil.fr/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « Health App Use Scenarios & HIPAA », [en ligne], février 2016, [consulté le 2 juillet 2020] sur https://assets.hcca-info.org/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act, Guidance for Industry and Food and Drug Administration Staff», [en ligne], septembre 2019, [consulté le 27 juillet 2020] sur https://www.fda.gov/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX - Office des droits civils, « HIPAA Administrative Simplification », mars 2013.

F. FEFER Rachel, « Data Flows, Online Privacy, and Trade Policy », Congressional Research Service Report [en ligne], mars 2019, sommaire, [consulté le 25 juillet 2020] sur https://fas.org/sgp/crs/row/R45584.pdf

MELL Peter, GRANCE Timothy, « The NIST Definition of Cloud Computing . *Publication spéciale 800-145* », [en ligne], septembre 2011, [consulté le 15 août 2020] sur https://nvlpubs.nist.gov/

PARLEMENT EUROPEEN, « REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free », [en ligne], avril 2016, [consulté le 16 août 2020] sur https://eur-lex.europa.eu/

TRUMP Donald, Président des États-Unis, Washington D.C., La Maison Blanche, « National Security Strategy of the United States of America », [en ligne], décembre 2017, [consulté le 8 juillet 2020] sur https://www.whitehouse.gov/

Articles et chroniques

ANDRY François (2020), « Cloud et plateformes : pourquoi ces technologies ont-elles autant d'impact ? » *Dalloz IP/IT*, 344 [en ligne], 2020, [consulté le 26 juillet 2020] sur https://www.dalloz.fr

BAYLE Aurélie, « L'habeas date à l'ère de l'e-santé », *Dalloz IP/IT* , p. 285 [en ligne] , 2020, [consulté le 26 juillet 2020] sur https://www.dalloz.fr

BISMUTH Regis, « Le Cloud Act face au projet européen e-evidence : confrontation ou coopération ? », *Revue critique de droit international privé*, [en ligne] 2019, p.681, [consulté le 26 juillet 2020] sur https://www.dalloz.fr

BOURGEOIS Mattier, « CLOUD COMPUTING - Les défis contractuels du Cloud computing », *JurisClasseur Communication* [en ligne], mai 2020, [consulté le 27 juillet 2020] sur https://www.lexis-nexis.fr

BOURGEOIS Mattier, « CLOUD COMPUTING - Notions et enjeux», *JurisClasseur Communication* [en ligne], mai 2020, [consulté le 27 juillet 2020] sur https://www.lexis-nexis.fr

CALLAWAY David et DETERMANN, « The New US Cloud Act – History, Rules, and Effects », *The Computer & Internet Lawyer*, Vol. 35, n°8, 2018, §III.

CABINET ALAIN BENSOUSSAM AVOCATS LEXING, « Cloud computing et droit, retour sur une année de grands changements », *Revue Lamy Droit de l'Immatériel*, Nº 138., [en ligne] 1er juin 2017, p. 2 [consulté le 25 juillet 2020] sur https://www.lamyline.lamy.fr

AUGAGNEUR Luc-Marie, Héberger ses données chez les GAFAM : quel discours croire sur le Cloud Act ?, *Revue Lamy Droit de l'Immatériel*, Nº 162, [en ligne] 1er août 2019, [consulté le 1er août 2020]

JACOB, « Quand les nuages ne s'arrêtent pas aux frontières - Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act, » *CDE 2018 n°4*, 2018.

Documents officiels

California Business and Professions Code.

California Online Privacy Protection Act.

Clarifying Lawful Overseas Use of Data Act.

Code de santé publique.

Code des États-Unis (U.S.C).

Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE)2016/679.

Health Insurance Portability and Accountability Act.

Health Information Technologie for Economic and Clinical Health Act.

Genetic Information Non-discrimination Act.

Patient Protection and Affordable Care Act.

Federal Food, Drug and Cosmetics Act.

Federal Trade Commission Act.

Mutual Legal Assistance Treaty.. Récupéré sur https://2009-2017.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

Patriot Act.

Patriotic Act.

Réglement général sur la protection des données.

Stored Communications Act.

Correspondances

KADZIK P., (15 juillet 2016). *Lettre de l'assistant du général de division à l'attention du vice-président Hoseph R. Biden, président du Sénat américain.* Récupéré sur https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf

Sites internet – Documents sur site internet

COMMISSION NOTIONAL INFORMATIQUE & LIBERTES, « Applications mobiles en santé et protection des données personnelles : Les questions à se poser », [en ligne], 17 août 2018, [consulté le 2 juillet 2020], sur https://www.cnil.fr

COMMISSION NOTIONAL INFORMATIQUE & LIBERTES, « La protection des données dans le monde », [en ligne], 19 novembre 2019, [consulté le 2 juillet 2020] sur https://www.cnil.fr/

COMMISSION NOTIONAL INFORMATIQUE & LIBERTES, « La protection des données dans le monde », [en ligne], 4 octobre 2017, [consulté le 2 juillet 2020] sur https://www.cnil.fr/

COMMISSION FEDERALE DU COMMERCE, « 5 principles to help keep your health claims healthy », [en ligne], [consulté le 20 juillet 2020] sur https://www.ftc.gov/

COMMISSION FEDERAL DU COMMERCE, « Mobile Health Apps Interactive Tool », [en ligne], [consulté le 2 juillet 2020] sur https://www.ftc.gov/

COMMISSION NOTIONAL INFORMATIQUE & LIBERTES, « Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise », [en ligne], [consulté le 12 août 2020] sur https://www.cnil.fr/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « Marketing Your Mobile App: Get it Right from the Start », [en ligne], avril 2013, [consulté le 2 juillet 2020] sur https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « Notice of Privacy Practices », [en ligne], juin 2017, [consulté le 2 juillet 2020] sur https://www.hhs.gov/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « Policy for Device Software Functions and Mobile Medical Applications. *Guidance for Industry and Food and Drug Administration Staff* », [en ligne], septembre 2019, [consulté le 2 juillet 2020] sur https://www.fda.gov/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « *The HIPAA Privacy Rule* », [en ligne], avril 2015, [consulté le 2 juillet 2020] sur Récupéré sur https://www.hhs.gov/

DEPARTEMENT AMERICAIN DE LA SANTE ET DES SERVICES SOCIAUX, « The HIPAA Privacy Rule », [en ligne], décembre 2019, [consulté le 2 juillet 2020] sur Récupéré sur https://www.hhs.gov/

DEPARTEMENT DU COMMERCE AMERICAIN, « Privacy Shield Framework, Obligatory Contracts for Onward Transfers», [en ligne], [consulté le 6 juillet 2020] sur Récupéré sur https://www.privacyshield.gov

DEPARTEMENT DU COMMERCE AMERICAIN, « Privacy Shield Framework, Contract Requirements for Data Transfers to a Processor», [en ligne], [consulté le 6 juillet 2020] sur Récupéré sur https://www.privacyshield.gov

Table des matières

ANNEXE 1

Les dispositions devant être incluses ou exclues au sein des accords exécutifs dans le cadre du Cloud Act [1] [2]

La loi CLOUD précise les dispositions de fond suivantes qui doivent être incluses dans les accords exécutifs :

- Les termes de l'accord ne doivent pas créer d'obligation pour les fournisseurs d'être capables de décrypter les données ou de limitation qui empêche les fournisseurs de décrypter les données ;
- Le gouvernement étranger ne peut pas cibler intentionnellement une personne américaine ou une personne située aux États-Unis ;

L'accord doit en outre exiger, en ce qui concerne toute ordonnance qui fait l'objet de l'accord :

- Le gouvernement étranger ne peut pas cibler une personne non américaine si l'objectif est d'obtenir des informations concernant une personne américaine ;
- Le gouvernement étranger ne peut pas émettre un ordre à la demande du gouvernement américain ou pour obtenir des informations à fournir au gouvernement américain ;
- un ordre émis par le gouvernement étranger :

  (i) a pour but d'obtenir des informations relatives à la prévention, à la détection, aux enquêtes ou aux poursuites concernant des infractions graves, y compris le terrorisme ;

  (ii) doit identifier une personne, un compte, une adresse ou un dispositif personnel spécifique, ou tout autre identifiant spécifique comme étant l'objet de l'ordre ;

  (iii) doit être conforme à la législation nationale de ce pays, et toute obligation pour un fournisseur ... de produire des données découle uniquement de cette législation ;

  (iv) doit être fondée sur l'exigence d'une justification raisonnable basée sur des faits articulables et crédibles, sur la particularité, la légalité et la gravité du comportement faisant l'objet de l'enquête ;

  (v) doit faire l'objet d'un examen ou d'une surveillance par un tribunal, un juge, un magistrat ou une autre autorité indépendante avant ou pendant la procédure d'exécution de l'ordonnance ;

  (vi) Dans le cas d'une ordonnance d'interception de communications électroniques, et de toute prolongation de celle-ci, l'ordonnance d'interception doit exiger que :

    (I) être d'une durée fixe et limitée

    (II) ne peut pas durer plus longtemps qu'il n'est raisonnablement nécessaire pour atteindre les objectifs approuvés de l'ordonnance ; et

    (III) n'est délivrée que si la même information ne peut raisonnablement être obtenue par une autre méthode moins intrusive.

---

[1] Cet annexe reprend les dispositions énoncées au sein du Titre 18 du Code des Etats-Unis §2523(b)(3) et suivants

[2] Il s'agit d'une traduction de l'écrit de CALLAWAY David et DETERMANN, The New US Cloud Act – History, Rules, and Effects, The Computer & Internet Lawyer, Vol. 35, n°8, 2018, p. 6.

LES DROITS DES PATIENTS

1) Voir et recevoir des copies de leur dossier médical

Sauf dans certaines circonstances, les personnes ont le droit d'examiner et d'obtenir une copie de leurs informations de santé protégées dans l'ensemble de dossiers désigner d'une entité couverte (groupe de dossiers tenus par ou pour une entité couverte ou les dossiers médicaux et de facturation d'un prestataire).

2) Demander une modification de leur dossier

La loi donne aux personnes le droit de faire modifier par les entités couvertes leurs informations de santé protégées dans un dossier désigner lorsque ces informations sont inexactes ou incomplètes.
Si une entité couverte accepte, elle doit faire des efforts raisonnables pour fournir la modification aux personnes que l'individu a identifiées comme en ayant besoin. Si la demande est refusée, un refus écrit est demandé.

3) Contrôler qui est informé de ses informations de santé

Les individus ont le droit de contrôler qui est informé. En règle générale, les entités couvertes ne peuvent pas divulguer des informations sur les patients sans leur consentement.

4) Comptabilisation des divulgations non routinières

Les personnes ont droit à une communication des divulgations de leurs informations de santé protégées par une entité couverte ou par les associés de l'entité couverte. La période maximale de comptabilisation des divulgations est de six ans précédant immédiatement la demande de comptabilisation, sauf qu'une entité couverte n'est pas obligée de comptabiliser toute divulgation faite avant sa date de mise en conformité obligatoire.

5) Demande d'opposition

Les personnes ont le droit de demander à une entité couverte de restreindre l'utilisation ou la divulgation d'informations de santé protégées pour le traitement, le paiement ou les opérations de soins de santé, la divulgation aux personnes impliquées dans les soins de santé de la personne ou le paiement des soins de santé, ou la divulgation pour informer les membres de la famille ou d'autres personnes de l'état général de la personne, de sa localisation ou de son décès.

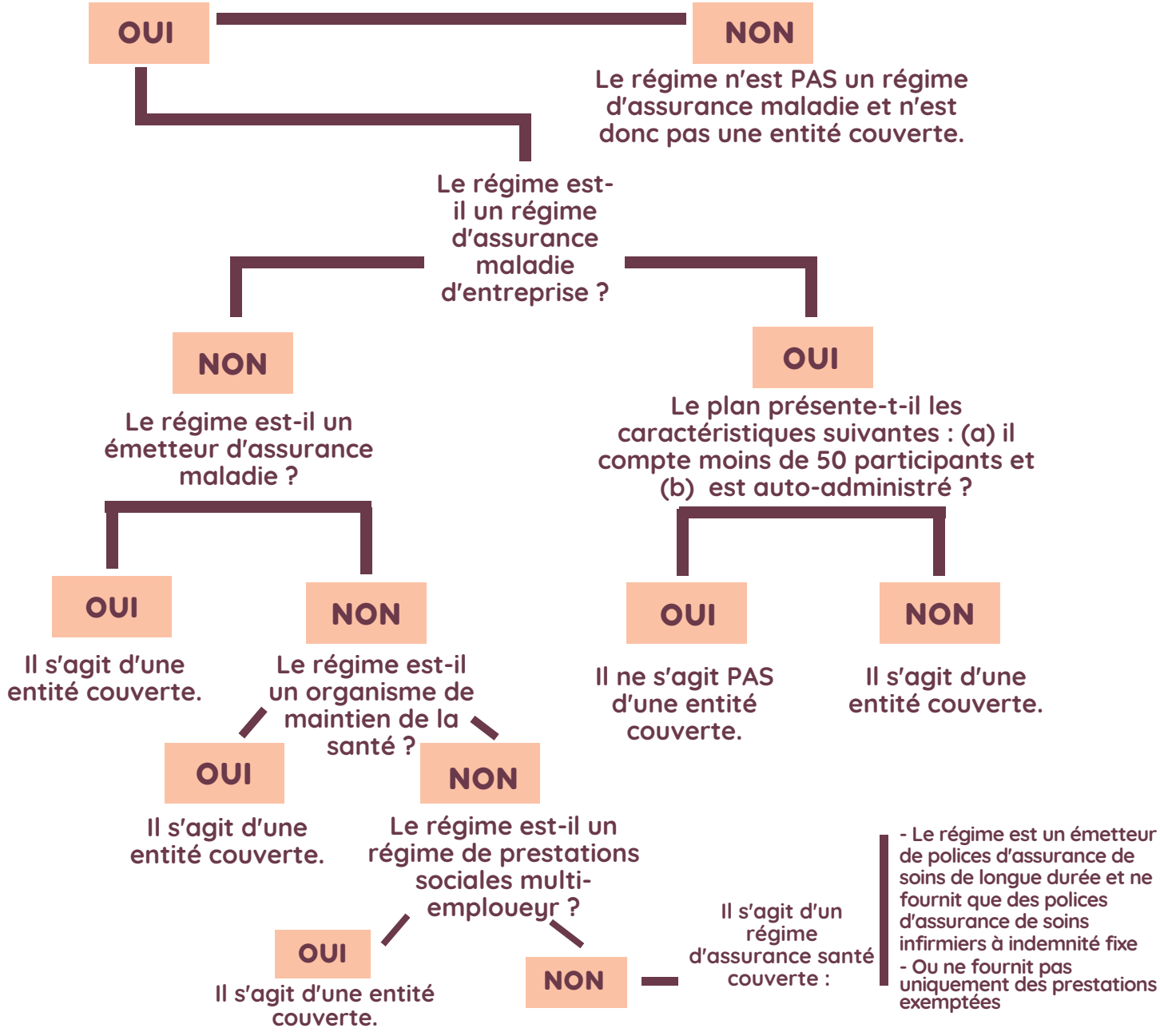
6) Droit à la portabilité

Les plans de santé et les prestataires de soins de santé couverts doivent permettre aux personnes de demander un autre moyen ou un autre lieu pour recevoir des communications d'informations de santé protégées par des moyens autres que ceux que l'entité couverte utilise habituellement.

LOI HIPAA

UN RÉGIME PRIVÉ DE PRESTATIONS EST-IL UN RÉGIME DE D'ASSURANCE MALADIE ?

S'agit-il d'un régime individuel ou collectif, ou d'une combinaison de régimes, qui fournit des soins médicaux ou en paie le coût ?



LOI HIPAA

UN PROGRAMME FINANCÉ PAR LE GOUVERNEMENT EST-IL UN RÉGIME D'ASSURANCE SANTÉ ?

Un programme financé par le gouvernement est-il un plan de santé ?

OUI

Le plan est un régime d'assurance de santé et donc une entité couverte.

NON

Le programme est-il un régime individuel ou collectif qui fournit des soins médicaux ou en paie le coût ?

OUI

Le programme est-il une réserve à haut risque ?

OUI

Il s'agit d'une entité couverte

NON

Le régime est-il un organisme de maintien de la santé ?

OUI

Il s'agit d'une entité couverte

NON

L'activité principale du programme consiste-t-elle à fournir directement des soins de santé ?

OUI

Il ne s'agit PAS d'une entité couverte

NON

Il s'agit d'une entité couverte si :

- L'activité principale du programme n'est PAS l'octroi de subventions pour financer la fourniture directe de soins de santé ;
- L'objectif principal du programme est de fournir ou de payer le coût des soins de santé ;
- Le programme n'offre PAS uniquement des avantages exclusifs.

NON

The plan is NOT a health plan and therefore not a covered entity.

Annexe 4

Recommandations en matière de mesures techniques et organisationnelles[1]

Recommandation	Exemples de mesures à mette en place
Sensibiliser les utilisateurs du responsable de traitement et du sous-traitant	Informer et sensibiliser les personnes manipulant les données et rédiger une charte informatique contraignante.
Authentifier les utilisateurs	Les utilisateurs doivent être authentifiés pour n'accéder qu'aux informations dont ils ont besoin
Gérer les habilitations	Seuls les personnels dont la mission nécessite d'avoir accès à l'information doivent être habilités à y accéder (principe du moindre privilège).
Tracer les accès et gérer les incidents	Les accès aux systèmes doivent être journalisés afin de savoir qui a accédé à quoi et, le cas échéant, de détecter les accès frauduleux ou illégitimes
Sécuriser les postes de travail et les supports mobiles	Les postes de travail doivent être protégés afin de prévenir les attaques ou de les identifier. Les équipements mobiles doivent être sécurisés afin de prévenir toute prise de connaissance des informations par un tiers. Des solutions d'effacement à distance peuvent également être utilisées
Protéger le réseau informatique interne et les serveurs	Il convient de séparer le réseau interne et le réseau externe, l'accès à distance doit être sécurisé via un VPN (etc.).
Sécuriser les sites internet	Les espaces personnels doivent être sécurisés à l'aide de certificat https (etc.
Sauvegarder et prévoir la continuité d'activité	Les données doivent être sauvegardées de manière régulière. Ces sauvegardes doivent être testées afin d'évaluer leur capacité à permettre une reprise d'activité.
Archiver de manière sécurisée	Les données qui ne sont plus utilisées au quotidien doivent être archivées, afin d'éviter toute perte d'information ou qu'un tiers non autorisé y ait accès.
Encadrer la maintenance et la destruction des données	Les opérations de maintenance comme les changements de serveur doivent être réalisés dans des environnements sûrs. Les matériels destinés à la destruction doivent faire l'objet d'un process permettant de supprimer toutes les données personnelles qu'ils comportent.
Sécuriser les échanges avec d'autres organismes	Les données doivent être échangées d'une manière permettant d'éviter qu'un tiers ne puisse en prendre connaissance (via serveur FTP ou email chiffré).
Protéger les locaux	Les locaux doivent être protégés via des dispositifs de contrôle d'accès
Encadrer les développements informatiques	Les développements informatiques doivent être réalisés à l'aide de bases de données de test, fictives.
Chiffrer, garantir l'intégrité ou signer	Les algorithmes de chiffrement doivent être robustes et à jour. Par ailleurs, il ne faut pas confondre chiffrement et anonymisation qui correspondent à deux opérations différentes, l'une visant à sécuriser des données (personnelles ou non), l'autre à rendre non personnelles des données qui initialement l'étaient
Cloud	Savoir où les services traitent et stockent les données, vérifier ce que stipulent les contrats en ce qui concerne le traitement, s'assurer que seule les données nécessaires sont collecté par le service et porter une attention particulière sur les données sensible, prendre les mesures nécessaire pour protéger les données de la perte de la détérioration ou usage non autorisé et s'assurer d'effacer les données lors de l'arrêt de l'usage du service
Gérer la sous-traitance	Les relations avec les prestataires qui traitent des données au nom et pour le compte du responsable de traitement (l'organisme employeur) doivent faire l'objet d'un accord écrit. Cet accord doit contenir une ou des clauses spécifiques relatives aux obligations respectives des parties résultant du traitement des données à caractère personnel. L'accord doit notamment prévoir les conditions de restitution et de destruction des données. Il incombe au responsable de traitement de s'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.).

[1] Référentiels de la CNIL

Annexe 5

Articles R-1111-11 du Code de la santé publique
Hébergement de données de santé

L'article R 1111-11 du CSP permet d'envisager la façon dont ce type de contrat entre l'hébergeur et le client doit être conclu. En vertu de cet article, le prestataire de solutions cloud et l'éditeur de l'application devra conclure un contrat comprenant au minimum les 14 clauses suivantes

1° L'indication du périmètre du certificat de conformité obtenu par l'hébergeur, ainsi que ses dates de délivrance et de renouvellement ;

2° La description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées ;

3° L'indication des lieux d'hébergement ;

4° Les mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé dont notamment :

-les modalités d'exercice des droits de portabilité des données ;

-les modalités de signalement au responsable de traitement de la violation des données à caractère personnel ;

-les modalités de conduite des audits par le délégué à la protection des données ;

5° La mention du référent contractuel du client de l'hébergeur à contacter pour le traitement des incidents ayant un impact sur les données de santé hébergées ;

6° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci ;

7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'hébergeur ;

8° Les modalités retenues pour encadrer les accès aux données de santé à caractère personnel hébergées ;

9° Les obligations de l'hébergeur à l'égard de la personne physique ou morale pour le compte de laquelle il héberge les données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par le cadre légal applicable ;

Annexe 5

10° Une information sur les garanties et les procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part ;

11° La mention de l'interdiction pour l'hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé ;

12° Une présentation des prestations à la fin de l'hébergement, notamment en cas de perte ou de retrait de certification et les modalités de mise en œuvre de la réversibilité de la prestation d'hébergement de données de santé ;

13° L'engagement de l'hébergeur de restituer, à la fin de la prestation, la totalité des données de santé au responsable de traitement ;

14° L'engagement de l'hébergeur de détruire, à la fin de la prestation, les données de santé après l'accord formel du responsable de traitement et sans en garder de copie.