Commission nationale de l'informatique et des libertés, décision n° 2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo (Programme de médicalisation des systèmes d'information (PMSI) – Traitement – Externalisation – Sécurité et confidentialité des données – Respect de la vie privée et des libertés individuelles – Manquements – Mise en demeure)

25/09/2013

L'attention de la Commission nationale de l'informatique et des libertés (CNIL) « *a été appelée, notamment par voie de presse, surles conditions dans lesquelles des établissements hospitaliers recourent à un traitement externalisé du programme de médicalisation des systèmes d'information (PMSI)* ». Sur ce fondement, elle a procédé à une mission de contrôle sur place auprès du centre hospitalier de Saint-Malo, concernant « *la conformité des traitements de données à caractère personnel mis en œuvre* [...] *aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée. En particulier, il s'est agi de contrôler la conformité des traitements mis en œuvre relatifs au codage des actes médicaux réalisés* ».
La CNIL constate en premier lieu un « *manquement à l'obligation de veiller à la sécurité et à la confidentialité des données* ». En effet, « *s'agissant des dossiers informatisés, un compte applicatif spécifique a été créé pour le prestataire avec des habilitations identiques à celles d'un profil DIM, comportant des droits notamment en écriture auxdits dossiers médicaux* ». De surcroît, *« une procédure a été mise en place entre l'établissement et le prestataire afin de permettre à ce dernier d'accéder aux dossiers en versions papier et numérique. Cet accès consiste notamment à mettre à la disposition du personnel non médecin du prestataire des dossiers, dans un bureau des archives de l'établissement, de surcroît hors la présence constante et continue du médecin du DIM ou d'un membre de son équipe* ». C'est pourquoi la CNIL affirme que « *ces pratiques conduisent à permettre un accès à des données couvertes par le secret médical par des tiers non autorisés, ce qui constitue un manquement à l'obligation deconfidentialité des données* ».
En second lieu, la CNIL souligne un «manquement à l'obligation de respecter la vie privée et les libertés individuelles», l'établissement ayant *«donné accès au prestataire chargé de l'analyse de l'activité de l'établissement à des données individuelles de santé, notamment par des moyens informatiques, sans que celui-ci participe à la prise en charge du patient, ni puisse être regardé comme faisant partie de l'équipe de soins ou ayant la qualité de médecin».*
L'établissement est donc mis en demeure, sous un délai de dix jours, de « m*ettre en œuvre les mesures de sécurité physiques et logiques pour garantir la sécurité et la confidentialité des dossiers médicaux des patients pris en charge dans l'établissement* », et en particulier, de « *veiller à ce que les dossiers des patients ne puissent pas être accessibles par des tiers, notamment par les prestataires choisis pour l'optimisation du codage, en supprimant le compte créé pour le prestataire et en établissant de nouvelles procédures en lien avec le service des archives afin que les dossiers sous format papier ne soient plus accessibles* ». Au terme de ce délai, si l'établissement s'est conformé à cette mise en demeure, la procédure sera considérée comme close ; dans le cas contraire, la présidente de la CNIL « *désignera un rapporteur qui pourra demander à la formation restreinte de prononcer une sanction dans les conditions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée* ».

Commission nationale de l'informatique et des libertés

Décision n° 2013-037 du 25 septembre 2013 mettant en demeure le centre hospitalier de Saint-Malo

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/461CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu le code pénal, notamment ses articles 121-2, 137-37, 131-38 et 226-17 ;

Vu le code de la santé publique, notamment ses articles L.1110-4, L.6111-1, L.6113-7, L.6113-8 et R.6113-1 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 45 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'arrêté du 22 février 2008 relatif au recueil et au traitement des données d'activité médicale et des données de facturation correspondantes, produites par les établissements de santé publics ou privés ayant une activité en médecine, chirurgie, obstétrique et odontologie, et à la transmission d'informations issues de ce traitement dans les conditions définies à l'article L. 6113-8 du code de la santé publique ;

Vu la délibération n° 2013-175 du 4 juillet 2013 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2013-164C du mardi 21 mai 2013 de la Présidente de la Commission nationale de l'informatique et des libertés de procéder à une mission de contrôle auprès du Centre hospitalier de Saint-Malo ;

Vu les procès-verbaux de contrôle n°2013-16411 et 2013-164/2 respectivement des 5 et6juin 2013;

Vu le rapport du médecin inspecteur de l'Agence régionale de santé établi dans le cadre de la mission de contrôle auprès du centre hospitalier de Saint-Malo ;

Constate les faits suivants

Le centre hospitalier de Saint-Malo (ci-après « l'établissement ») est un établissement public de santé régi par les dispositions du code de la santé publique, notamment les articles L.6111-1 et suivants. Il compte un peu plus d'un millier de lits et emploie environ 2000 agents. Ses dépenses de fonctionnement globales étaient de 140 millions d'euros en 2008.

L'attention de la Commission nationale de l'informatique et des libertés (ci-après «la CNIL » ou « la Commission ») a été appelée, notamment par voie de presse, sur les conditions dans lesquelles des établissements hospitaliers recourent à un traitement externalisé du programme de médicalisation des systèmes d'information (PMSI).

En application de la décision n° 2013-164C du mardi 21 mai 2013 de la Présidente de la CNIL, une délégation de la CNIL a procédé à une mission de contrôle sur place le mercredi 5 juin et le jeudi 6 juin 2013 auprès du centre hospitalier de Saint-Malo. A cette occasion, elle a été assistée d'un médecin inspecteur de santé publique à l'Agence régionale de santé (ci-après ARS) Bretagne.

Dans le cadre de cette mission de contrôle, la délégation s'est attachée à examiner la conformité des traitements de données à caractère personnel mis en oeuvre au sein du centre hospitalier de Saint-Malo aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée. En particulier, il s'est agi de contrôler la conformité des traitements mis en oeuvre relatifs au codage des actes médicaux réalisés au sein de l'établissement en application des articles L6113-7 et suivants du code de la santé publique.

En vertu de ces dispositions, il appartient aux établissements de santé publics et privés de procéder à l'analyse de leur activité médicale et de transmettre aux services de l'État et à l'assurance maladie « les informations relatives à leurs moyens de fonctionnement et à leur activité ». A cette fin, ils doivent « mettre en oeuvre des systèmes d'information qui tiennent compte notamment des pathologies et des modes de prise en charge ». Ces systèmes d'information constituent le programme de médicalisation des systèmes d'information (ci-après désigné PMSI).
La délégation a ainsi été informée que le financement des établissements de santé repose sur l'activité réalisée par

chaque établissement telle qu'elle est décrite dans les dossiers des patients pris en charge, et codée dans le cadre du PMSI.

Il a été précisé à la délégation qu'afin de répondre à ses obligations de valorisation du PMSI, le centre hospitalier de Saint-Malo est doté d'un département d'information médicale (ci-après désigné DIM) composé de douze (12) personnes placées sous la responsabilité du médecin du département. Il a été indiqué que le codage des activités de soin est effectué par le DIM par extraction des informations issues des dossiers médicaux des patients pris en charge dans l'établissement.

La délégation a également été informée que la précision du codage des actes médicaux constitue un enjeu stratégique pour l'établissement dans la mesure où elle influe sur son financement. A cette fin, l'établissement de santé a recours, depuis l'année 2007, à l'expertise de sociétés extérieures (ci-après le prestataire) en charge d'affiner le codage et la description des actes médicaux et paramédicaux réalisés au sein de l'établissement. Cette procédure a révélé des marges d'amélioration significatives dans la description de l'activité, de sorte que l'établissement a pu obtenir de l'Agence régionale de santé Bretagne, le 11 décembre 2012, l'autorisation de procéder à la modification des informations de codage concernant une partie de l'activité de 2010 et 2011. Il a été précisé à la délégation que ces démarches permettent au centre hospitalier de Saint-Malo d'obtenir une augmentation de l'enveloppe budgétaire qui lui est allouée.

S'agissant de la gestion des dossiers médicaux des patients pris en charge par le centre hospitalier de Saint-Malo, la délégation a été informée que l'application métier de l'établissement contenant des données à caractère personnel relatives à la santé des patients, intitulée « SILLAGE », nécessite une authentification individuelle et a fait l'objet de formalités auprès de la Commission. Il a également été indiqué que l'établissement dispose d'un service des archives conservant les dossiers sous format papier.

Le médecin inspecteur de santé publique assistant la délégation pendant sa mission de contrôle a constaté que les dossiers sous format papier comportent le dossier médical (notamment les comptes-rendus de consultation, d'hospitalisation, d'imagerie, les observations médicales et les traitements prescrits) ainsi que le dossier infirmier.

La délégation a été informée que pour proposer un recodage plus fin, le médecin du DIM de l'établissement a déterminé avec le prestataire les modalités d'intervention de ce dernier sur le site du centre hospitalier. L'accès du prestataire aux dossiers des patients est notamment prévu. La délégation a été informée que cet accès s'opère soit par le biais d'une connexion à l'application métier SILLAGE avec un profil DIM comportant des droits en lecture et en écriture, soit par le biais de la consultation de dossiers médicaux sous format papier, ces derniers étant mis à la disposition du prestataire dans le bureau du service des archives.

La délégation a été informée de ce que, pour procéder au recodage des années 2010 et 2011, 950 dossiers ont été audités par un consultant non médecin employé par le prestataire, hors la présence constante et continue du médecin du DIM ou d'un membre de son service.

Sur la qualification de ces faits au regard de la loi du 6 janvier 1978

Un manquement à l'obligation de veiller à la sécurité et à la confidentialité des données

En premier lieu, s'agissant des dossiers informatisés, un compte applicatif spécifique a été créé pour le prestataire avec des habilitations identiques à celles d'un profil DIM, comportant des droits notamment en écriture auxdits dossiers médicaux.

En outre, une procédure a été mise en place entre l'établissement et le prestataire afin de permettre à ce dernier d'accéder aux dossiers en versions papier et numérique. Cet accès consiste notamment à mettre à la disposition du personnel non médecin du prestataire des dossiers, dans un bureau des archives de l'établissement, de surcroît hors la présence constante et continue du médecin du DIM ou d'un membre de son équipe.

En deuxième lieu, l'article L.6113-7 du code de la santé publique prévoit que: « Les établissements de santé, publics ou privés procèdent â l'analyse de leur activité. Dans le respect du secret médical et des droits des malades, ils mettent en oeuvre des systèmes d'information qui tiennent notamment compte des pathologies et des modes de prise en charge en vue d'améliorer la connaissance et l'évaluation de l'activité et des coûts et de favoriser l'optimisation de l'offre de soins».

En l'espèce, bien que le prestataire et le personnel qu'il emploie soient soumis à une clause de confidentialité (seul le directeur de la société ayant cependant la qualité de médecin), ils ne sont pas placés sous l'autorité du médecin DIM de l'établissement. Or, l'article R.6113-5 du code de la santé publique dispose que : « Les médecins chargés de la collecte des données médicales nominatives ou du traitement des fichiers comportant de telles données sont soumis à l'obligation de secret dont la méconnaissance est punie conformément aux articles 226-13 et 226-14 du code pénal. Il en est de même des personnels placés ou détachés auprès de ces médecins et qui travaillent à l'exploitation des données nominatives sous leur autorité, ainsi que des personnels intervenant sur le matériel et les logiciels utilisés pour le recueil des traitements de données ».

Il en résulte que les dispositions précitées ne sont pas respectées. En effet, ces pratiques conduisent à permettre un accès à des données couvertes par le secret médical par des tiers non autorisés, ce qui constitue un manquement à l'obligation de confidentialité des données.

En troisième lieu, bien que le dernier prestataire sélectionné dispose d'une autorisation de la CNIL de procéder à des analyses de l'activité des établissements de santé, il convient de relever que les termes de cette autorisation ne lui permettent pas d'accéder à des données nominatives de patients.

Au vu des pratiques consistant à permettre à des prestataires externes à l'établissement, qui ne sont pas placés sous l'autorité du médecin DIM de l'établissement et qui ne participent pas à la prise en charge des malades, d'accéder à des données individuelles de santé de patients, le centre hospitalier de Saint-Malo a commis un manquement à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée disposant que : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Il est rappelé qu'en application des articles 121-2, 137-37, 131-38 et 226-17 du code pénal combinés, le fait de procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n°78-17 du 6 janvier 1978 précitée est puni de 1.500.000€ d'amende.

Un manquement à l'obligation de respecter la vie privée et les libertés individuelles

Il ressort du contrôle effectué par la Commission que le centre hospitalier de Saint-Malo a donné accès au prestataire chargé de l'analyse de l'activité de l'établissement à des données individuelles de santé, notamment par des moyens informatiques, sans que celui-ci participe à la prise en charge du patient, ni puisse être regardé comme faisant partie de l'équipe de soins ou ayant la qualité de médecin.

Or, l'article L.1110-4 du code de la santé publique prévoit que : « Toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et au secret des informations la concernant. Excepté dans les cas de dérogation, expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé, ainsi qu'à tous les professionnels intervenant dans le système de santé f...].

Il apparaît dès lors qu'en organisant l'accès aux dossiers médicaux des patients dans les conditions précitées, le centre hospitalier de Saint-Malo a porté atteinte à la vie privée des personnes ce qui constitue un manquement tant au code de la santé publique qu'à l'article 1 er de la loi du 6 janvier 1978 modifiée qui dispose que « l'informatique doit être au service de chaque citoyen. (...). Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

En conséquence, la Présidente de la CNIL met en demeure le centre hospitalier de Saint-Malo, sis 1 rue de la Marne à SAINT-MALO (35400), sous un délai de dix (10) jours à compter de la notification de la présente décision, de :

• mettre en oeuvre les mesures de sécurité physiques et logiques pour garantir la sécurité et la confidentialité des dossiers médicaux des patients pris en charge dans l'établissement ;
• en particulier, veiller à ce que les dossiers des patients ne puissent pas être accessibles par des tiers, notamment par les

prestataires choisis pour l'optimisation du codage, en supprimant le compte créé pour le prestataire et en établissant de nouvelles procédures en lien avec le service des archives afin que les dossiers sous format papier ne soient plus accessibles ;

• justifier auprès de la CNIL que l'ensemble des demandes précitées a bien été respecté, et ce dans le délai imparti.

À l'issue de ce délai, si le centre hospitalier de Saint-Malo s'est conformé à la présente mise en demeure, la Présidente de la CNIL considérera que la procédure est close et lui adressera un courrier en ce sens.

À l'inverse, si, au vu de l'ensemble des éléments qui auront été portés à sa connaissance, la Présidente constate que le centre hospitalier de Saint-Malo ne s'est pas conformé à la présente mise en demeure, elle désignera un rapporteur qui pourra demander à la formation restreinte de prononcer une sanction dans les conditions prévues par l'article 45 de la loi du 6 janvier 1978 modifiée.

La Présidente