Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

Arrêté du 11 juin 2021 portant adoption de la charte d'audit applicable aux audits relatifs au système national des données de santé

NOR : *SSAE2114736A*

Par arrêté du ministre des solidarités et de la santé en date du 11 juin 2021, la charte d'audit mentionnée à l'article 102 du décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés figure en annexe du présent arrêté.

ANNEXES

ANNEXE I

CHARTE D'AUDIT DU SYSTÈME NATIONAL DES DONNÉES DE SANTÉ

Présentation de la charte d'audit

La présente charte définit et précise les missions, les domaines d'intervention, les pouvoirs, les responsabilités ainsi que les règles de conduite à suivre dans le cadre des audits lancés par le comité d'audit concernant le système national des données de santé.

Elle est réalisée conformément à la norme ISO 19011 qui présente des lignes directrices et des conseils dans la réalisation des audits des systèmes de management. La charte est complétée d'une annexe relative à la déontologie qui définit les principes fondamentaux et les règles qui s'appliquent aux membres du comité d'audit et aux auditeurs réalisant les audits décidés par le comité d'audit.

Elle s'articule avec les dispositions prévues par les statuts particuliers qui s'imposent aux auditeurs qui en relèvent.

Les droits et devoirs des membres du comité d'audit, des auditeurs et des entités auditées y sont définis ainsi que l'organisation de la fonction d'audit dans le cadre de la gouvernance du système national des données de santé. La présente charte vise à garantir le respect des règles déontologiques, de permettre un bon fonctionnement de cette activité dans le cadre d'une démarche d'assurance et d'amélioration de la qualité, et de clarifier les principes régissant les relations entre le comité d'audit, les auditeurs et les entités contrôlées lors de la réalisation des missions d'audit.

La charte a notamment vocation à faciliter le déroulement des missions d'audit en informant les entités auditées des objectifs de l'audit et des méthodes développées qui reposent sur la conformité à la norme ISO 19011.

1. **Les principaux textes de référence**

– le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;
– le code de la santé publique, notamment ses articles L. 1461-1 et suivants et R. 1461-1 et suivants ;
– la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
– le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
– l'arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales ;
– l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au système national des données de santé ;
– l'arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études.

2. **Définition et objectifs de l'audit**

L'audit est une activité objective qui permet un examen du mode de fonctionnement et d'organisation d'une entité par un tiers indépendant et impartial dont la mission principale consiste à déceler puis localiser les éventuelles défaillances qu'il serait possible de rectifier afin de rendre l'entité auditée plus efficiente. Dans ce contexte, l'audit est un moyen d'apporter une amélioration continue au sein des services audités.

3. **Champ d'application et méthodologie des audits**

La Commission nationale de l'informatique et des libertés est l'autorité compétente pour contrôler tous les traitements à caractère personnel. Elle peut donc, dans le cadre de ses missions, évaluer la conformité des traitements entrant dans le périmètre du système national des données de santé ainsi que toutes les bases comportant des données du système national des données de santé.

Chaque organisme, responsable d'un traitement de données à caractère personnel, doit mettre en place les mesures garantissant le respect des dispositions du code de la santé publique relatives au système national des données de santé, de la loi du 6 janvier 1978 et du règlement général sur la protection des données. L'article 3 de l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au système national des données de santé indique notamment que « *tous les systèmes du SNDS élargi doivent être périodiquement contrôlés (fonctionnellement et techniquement) dans le cadre d'audits internes (éventuellement délégués à des prestataires PASSI) et d'audits externes* ».

Par ailleurs, la convention passée entre la Caisse nationale de l'assurance maladie ou la Plateforme des données de santé, responsables du traitement du système national des données de santé, et l'organisme qui a obtenu l'autorisation d'accéder aux données du système national des données de santé comporte des engagements relatifs aux contrôles et audits.

Enfin le comité d'audit du système national des données de santé, mis en place par l'article 77 de la loi du 6 janvier 1978, fixe la stratégie et la programmation d'audits en complément de ceux initiés par le responsable de traitement.

Le périmètre couvert par les opérations d'audit programmées par le comité d'audit concerne le système national des données de santé élargi. Il comprend l'ensemble des systèmes réunissant, organisant et mettant à disposition tout ou partie des données du système national des données de santé c'est-à-dire :

- le système national des données de santé tel qu'il est défini par les dispositions du I de l'article L. 1461-1 du code de la santé publique ;
- les systèmes sources qui alimentent en amont le système national des données de santé central en données ;
- les systèmes fils qui, sur la base d'autorisations de la Commission nationale de l'informatique et des libertés ou créés par les services de l'Etat, les établissements publics ou les organismes chargés d'une mission de service public autorisés à traiter des données à caractère personnel du système national des données de santé en application du III de l'article L. 1461-3 du code de la santé publique, hébergent ou mettent à disposition des données issues du système national des données de santé.

Les audits peuvent être réalisés auprès :

- des responsables de traitement du système national des données de santé ;
- des responsables de traitement des bases sources ;
- des responsables de traitement des systèmes fils ;
- des responsables d'un traitement de données issues du système national des données de santé, autorisé par la Commission nationale de l'informatique et des libertés ;
- et de leurs sous-traitants.

Les audits du comité d'audit sont menés sous la forme de missions ponctuelles et ciblées. Ils sont menés pour vérifier le respect des dispositions applicables. Les audits peuvent, par exemple, porter sur :

- la conformité des traitements aux dispositions applicables au système national des données de santé, et, plus particulièrement, au V de l'article L. 1461-1 du code de la santé publique ainsi que les modalités de recours aux laboratoires de recherche et bureaux d'études par les acteurs privés concernés ;
- le respect par l'organisme audité de l'autorisation de traiter des données du système national des données de santé dont il bénéficie, que cette autorisation ait été prévue par des dispositions législatives ou réglementaires ou délivrée par la Commission nationale de l'informatique et des libertés ;
- le respect des formalités relatives aux opérations liées aux habilitations et au recensement des traitements qui mobilisent des données du système national des données de santé pour les organismes disposant d'accès permanents ;
- l'architecture, la configuration, les codes sources, la possibilité d'intrusion ;
- les processus organisationnels et physiques.

4. **Organisation de la fonction audit du comité d'audit**

4.1. *Le comité d'audit*

Le comité d'audit est présidé par le Fonctionnaire de sécurité des systèmes d'information, par délégation du Haut fonctionnaire de défense et de sécurité assistant le ministre chargé de la santé. Il comprend des représentants des services du ministère en charge de la santé, de la Plateforme des données de santé, de la Caisse nationale de l'assurance maladie, des autres producteurs de données ainsi qu'une personne représentant les acteurs privés du domaine de la santé. Une personnalité qualifiée est également désignée. Le président de la Commission nationale de l'informatique et des libertés ou son représentant y assiste en tant qu'observateur.

Dans l'exercice de leur fonction, les membres du comité d'audit sont indépendants. Afin de préserver cette indépendance, ils sont protégés par les dispositions de la présente charte et s'abstiennent de s'engager dans des fonctions opérationnelles ou dans toute activité susceptible de compromettre leur indépendance et leur objectivité.

Chaque membre du comité d'audit informe le président, par déclaration écrite, des intérêts directs ou indirects, mandats et fonctions au sein d'un organisme public ou privé qu'il détient ou a détenus au cours des trois dernières années précédant sa déclaration. Il signale immédiatement par écrit tout changement affectant des aspects de sa situation personnelle et professionnelle qui surviendrait durant l'exercice de ses fonctions. Ces informations sont conservées par le président du comité d'audit dans des conditions garantissant leur confidentialité.

4.1.1. Indépendance du pilotage du comité d'audit

Les membres du comité d'audit disposent d'une vision stratégique adéquate pour décider de la stratégie d'audit à suivre en toute indépendance.

Le comité d'audit ne subit aucune ingérence dans ses prises de décision.

Les membres du comité d'audit doivent respecter l'annexe relative à la déontologie, l'ensemble des règles et obligations liées à leur fonction que celles relevant de l'article 40 du code de procédure pénale lorsque ses dispositions s'appliquent. Ils doivent signaler immédiatement tout soupçon d'irrégularité grave au comité d'audit.

4.1.2. Objectivité individuelle

Les membres du comité d'audit ont une attitude impartiale, dépourvue de préjugés et évitent les conflits d'intérêts. Ils doivent se déporter en tant que de besoin en cas de liens personnels ou professionnels avec les entités auditées.

4.1.3. Atteinte à l'indépendance ou à l'objectivité

Si l'objectivité ou l'indépendance des membres du comité d'audit est compromise dans les faits, ou si les circonstances laissent penser qu'elle peut l'être, le comité d'audit en est informé dans les plus brefs délais par le membre du comité d'audit concerné. Le président du comité d'audit peut décider de son exclusion au regard de la gravité des faits.

Si le président du comité d'audit a connaissance d'une atteinte à l'indépendance ou à l'objectivité de l'un de ses membres alors que ce membre ne l'a pas tenu informé de sa situation, il décide de son exclusion au regard de la gravité des faits.

4.1.5. Protection des informations et confidentialité

Les membres du comité d'audit sont tenus à un strict devoir de réserve et de discrétion à l'égard des informations obtenues dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.

Ils respectent le contenu et la propriété des informations qu'ils reçoivent. Ils ne divulguent ces informations qu'avec les autorisations requises à moins qu'une obligation légale ou professionnelle ne les oblige à le faire.

Des mesures de sécurité destinées à protéger la confidentialité des échanges nécessaires au bon déroulement de la mission d'audit aussi bien entre le président du comité d'audit et les auditeurs qu'entre ces derniers et les entités auditées sont mises en place.

4.2. *Le président du comité d'audit*

Le président du comité d'audit est garant de l'indépendance des auditeurs dans la conduite des travaux qui leur sont confiés.

Le président du comité d'audit suit le déroulement des audits. Il est tenu informé par les auditeurs d'une éventuelle opposition aux audits, des situations d'urgence ou des constats susceptibles de révéler des manquements et des dysfonctionnements graves. Il les signale sans délai au président de la Commission nationale de l'informatique et des libertés afin que, le cas échéant, celui-ci adopte les mesures correctrices relevant de sa compétence ou saisisse la formation restreinte de la Commission en vue du prononcé d'une sanction.

Le président du comité d'audit présente les principales conclusions et recommandations au comité d'audit dont les membres ne sont pas destinataires des rapports d'audit par souci de confidentialité. La communication de ces informations ne donne lieu à la divulgation d'aucune donnée à caractère personnel à l'exception du nom du responsable de traitement et du sous-traitant, le cas échéant, et d'aucun élément portant sur les mesures de sécurité mis en œuvre par les entités auditées.

4.3. *Les auditeurs*

La réalisation des audits est confiée à des cabinets d'audit indépendants sélectionnés dans le cadre de marchés publics respectant les dispositions du code de la commande publique. Les audits sont réalisés par des auditeurs choisis selon des critères et modalités permettant de disposer de garanties attestant de leur compétence en matière d'audit de systèmes d'information et de leur indépendance à l'égard des entités auditées.

Chaque auditeur informe le président, par déclaration écrite, des intérêts directs ou indirects, mandats et fonctions au sein d'un organisme public ou privé qu'il détient ou a détenus au cours des trois dernières années précédant sa déclaration. Il signale immédiatement par écrit tout changement affectant des aspects de sa situation personnelle et professionnelle qui surviendrait durant l'exercice de ses fonctions. Ces informations sont conservées par le président du comité d'audit dans des conditions garantissant leur confidentialité.

Aucun auditeur ne peut être désigné pour effectuer un audit dans une entité au sein de laquelle :

– il détient un intérêt direct ou indirect, exerce des fonctions ou une activité professionnelle ou détient un mandat ;
– il a, dans un délai de trois ans, détenu un intérêt direct ou indirect, exercé des fonctions ou une activité professionnelle ou détenu un mandat.

Les auditeurs ne sont pas autorisés à :

– accomplir des tâches opérationnelles pour l'organisation auditée ;
– initier ou approuver des transactions financières ;
– diriger les activités de tout salarié ou agent de l'entité auditée, sauf dans le cas où cette personne a été appelée à l'assister.

Lorsque les critères relatifs aux condamnations à une peine correctionnelle ou criminelle ou à l'indépendance et l'objectivité de l'auditeur ne sont plus respectés, sa mission prend fin.

Le président du comité d'audit peut refuser la candidature d'un auditeur lorsqu'il estime que les critères formulés par la présente charte ne sont pas remplis. Le cabinet d'audit s'engage à présenter un nouvel auditeur dont la compétence et l'indépendance correspondent aux critères définis par la présente charte.

Les auditeurs conduisent les missions sans préjugé, avec objectivité, impartialité et honnêteté. Ils se conforment à l'annexe relative à la déontologie, à l'ensemble des règles et obligations liées à leur mission.

Les auditeurs doivent respecter la programmation établie par le président du comité d'audit. Ils communiquent régulièrement au président du comité d'audit des informations sur le degré d'avancement des travaux, et les difficultés rencontrées dans la mise en œuvre du plan d'audit et des audits. Ils informent sans délai le président du comité d'audit en cas d'opposition à l'audit, ou de constats susceptibles de révéler des manquements ou dysfonctionnements graves.

Les auditeurs respectent le droit de réserve à l'égard des informations obtenues dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.

4.4. *Le médecin, lorsque sa présence est requise*

Le médecin informe le président, par déclaration écrite, des intérêts directs ou indirects, mandats et fonctions au sein d'un organisme public ou privé qu'il détient ou a détenus au cours des trois dernières années précédant sa déclaration. Il signale immédiatement par écrit tout changement affectant des aspects de sa situation personnelle et professionnelle qui surviendrait durant l'exercice de ses fonctions. Ces informations sont conservées par le président du comité d'audit dans des conditions garantissant leur confidentialité.

Aucun médecin ne peut être désigné pour participer à l'audit d'une entité au sein de laquelle :

– il détient un intérêt direct ou indirect, exerce des fonctions ou une activité professionnelle ou détient un mandat ;
– il a, dans un délai de trois ans, détenu un intérêt direct ou indirect, exercé des fonctions ou une activité professionnelle ou détenu un mandat.

Le médecin désigné n'est pas autorisé à :

– accomplir des tâches opérationnelles pour l'organisation auditée ;
– initier ou approuver des transactions financières ;
– diriger les activités de tout salarié ou agent de l'entité auditée, sauf dans le cas où cette personne a été appelée à l'assister.

Lorsque ces critères relatifs aux condamnations à une peine correctionnelle ou à l'indépendance et l'objectivité du médecin ne sont plus respectés, sa mission prend fin.

Le médecin conduit ses missions sans préjugé, avec objectivité, impartialité et honnêteté. Il se conforme à l'annexe relative à la déontologie, à l'ensemble des règles et obligations liées à sa profession.

Le médecin respecte le droit de réserve à l'égard des informations obtenues dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.

5. **Déroulement des missions d'audit**

5.1. *Le lancement de la mission*

Une notification adressée aux responsables des entités auditées informe ces dernières du lancement de la mission par lettre recommandée avec accusé de réception. Conformément aux dispositions de l'article 103 du décret du 29 mai 2019 précité, la notification prévoit les informations relatives au déroulement de la mission. Elle doit également mentionner les délais et voies de recours dont dispose l'entité auditée. Cette notification est signée par le président du comité d'audit et les auditeurs individuellement désignés.

Le démarrage de la mission donne lieu à une réunion d'ouverture entre l'entité auditée et les auditeurs. La présence du délégué à la protection des données, désigné par l'entité auditée, est obligatoire à la réunion d'ouverture. Le président du comité d'audit ou son représentant peut y participer. Cette réunion permet notamment de présenter la mission, ses objectifs, le périmètre de l'audit, d'identifier les contacts nécessaires pour la mener à bien et de présenter les principaux documents attendus. L'entité auditée doit au minimum fournir, à cette occasion, les documents prévus par le règlement général sur la protection des données, par l'arrêté du 22 mars 2017 précité et, le cas échéant, les documents prévus par les dispositions relatives au système national des données de santé.

5.2. *La réalisation de la mission*

Les audits obéissent aux règles du débat oral et contradictoire.

Les audits sont réalisés sur place et sur pièces.

Tout au long de leur mission, les auditeurs demeurent soucieux du dialogue avec l'entité auditée.

Les auditeurs réalisent leur mission en appliquant respectivement les procédures qualité de leur cabinet et une méthodologie garantissant la conformité avec les normes du cadre de référence de l'audit interne de l'Etat.

Les auditeurs rendent régulièrement compte de l'avancée de leurs missions au président du comité d'audit. Il rend lui-même compte au président de la Commission nationale de l'informatique et des libertés ou à son représentant notamment des faits susceptibles de révéler des manquements et des dysfonctionnements graves de manière à ce que la Commission se prononce sur la démarche à adopter et sur la qualification des faits. Dans le respect de ces dispositions, les auditeurs restent maîtres et responsables de leurs méthodes de travail et du champ de leurs investigations en fonction du périmètre défini pour chaque audit.

Les auditeurs mettent en œuvre des outils et appliquent des méthodes d'audit qui leur permettent de détecter et d'évaluer les risques, de corroborer et de justifier leurs observations.

Les auditeurs peuvent demander communication de tous documents, quel qu'en soit le support, et en prendre copie ce qui suppose :

- la communication spontanée des éléments utiles à l'appréhension de l'objet de la mission ;
- la mise à disposition des moyens nécessaires à la mission ;
- des réponses apportées par écrit, de manière circonstanciée et dans le respect des délais aux interrogations des auditeurs ;
- la communication des pièces demandées dans le respect des délais impartis ;
- des réponses apportées par écrit et de manière circonstanciée au rapport d'audit dans les délais impartis explicitant les modalités de mise en œuvre des recommandations ;
- la fourniture des informations actualisées sur l'état d'avancement du plan d'action.

Les auditeurs peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins de l'audit. Leurs échanges avec les entités auditées, les réponses et documents apportés sont des éléments concourant à la validation de leurs travaux sans attendre la phase contradictoire. Ils sont également susceptibles de corriger leurs appréciations et de réorienter leurs travaux.

Si le périmètre de l'audit implique des données médicales individuelles, le président du comité d'audit doit prévoir la présence d'un médecin auprès des auditeurs pour tous les aspects de l'audit concernant ces données.

Tout membre du personnel du service audité doit collaborer avec les auditeurs pendant la conduite de la mission et en faciliter le déroulement. Les auditeurs peuvent s'entretenir avec tout membre du personnel, quels que soient son statut, son grade, sa fonction, et assister à des réunions qui présentent un lien avec l'objectif de la mission.

Pour chaque mission, les auditeurs doivent être en mesure de détailler leurs méthodes de travail. Chaque mission donne lieu à la tenue par les auditeurs d'un dossier d'audit de nature à assurer la traçabilité des preuves. Toute réunion organisée entre les auditeurs et l'entité audité, y compris la réunion d'ouverture et la réunion de fin d'audit, donne lieu à un procès-verbal. Celui-ci rend compte de l'état d'avancement des travaux, fait état des discussions, des réponses données et des engagements pris par l'entité auditée ainsi que des éventuelles difficultés soulevées et des décisions prises.

5.3. *La restitution des résultats*

Les observations, conclusions et recommandations sont portées régulièrement à la connaissance des entités auditées, du président du comité d'audit, et, le cas échant, du président de la Commission nationale de l'informatique et des libertés.

Chaque mission donne lieu à une réunion de fin d'audit qui a pour objectif d'informer des observations, conclusions et recommandations les entités auditées. Elle vise également à rappeler l'importance de la mise en œuvre des recommandations par les entités auditées et à les inciter à prendre des mesures correctives dans le cadre d'un plan d'action. Elle peut avoir lieu en présence du président du comité d'audit ou de son représentant si sa présence s'avère nécessaire.

La mission se conclut par un rapport d'audit. Un projet de rapport est soumis à l'entité auditée et énonce la nature des vérifications effectuées. Il indique également l'objet de la mission, les membres présents, les personnes rencontrées, le cas échéant, leurs déclarations, les demandes formulées par les auditeurs ainsi que les éventuelles difficultés rencontrées. Pour étayer leurs constats, les auditeurs doivent mentionner dans le rapport d'audit les pièces justificatives auxquelles ils se réfèrent. Les observations, conclusions et les recommandations y sont consignées. L'inventaire des pièces et documents dont les auditeurs ont pris copie y est annexé.

Le rapport définitif comporte, outre les observations, les conclusions et les recommandations définitives, les observations éventuelles de l'entité auditée et son plan d'action. Il inclut également les actions de mise en conformité qui sont attendues. Il est transmis au président de la Commission nationale de l'informatique et des libertés.

La communication des résultats de la mission d'audit au personnel de l'entité auditée relève de la décision de cette entité.

Dans une démarche de qualité, il est recommandé que le cabinet d'audit propose à l'entité auditée un questionnaire permettant d'apprécier sa perception du déroulement de la mission d'audit. Les réponses à ce questionnaire sont portées à la connaissance du président du comité d'audit et du comité d'audit.

5.4. *Le suivi des recommandations découlant de la mission d'audit*

Le plan d'action doit prévoir un calendrier de mise en œuvre, les actions envisagées et préciser les responsables associés à chacune de ces actions. Il intègre, dans la mesure du possible, des indicateurs de mesure de réalisation de ces actions et tout document permettant de justifier cette réalisation.

L'entité audité adresse régulièrement un rapport de suivi des recommandations au président du comité d'audit.

5.5. *Les traitements mis en œuvre dans le cadre de la mission d'audit*

Lorsque, dans le cadre des audits, des traitements de données à caractère personnel sont mis en œuvre, les mesures techniques et organisationnelles appropriées sont mises en place pour assurer la sécurité de ces traitements.

Le président du comité d'audit est responsable des traitements nécessaires à l'exercice de ses missions qui incluent le traitement de données relatives aux membres du comité d'audit, aux auditeurs et aux personnels des entités auditées.

Les prestataires auxquels il fait appel pour la réalisation des audits sont des sous-traitants au sens de l'article 28 du règlement général relatif à la protection des données.

Ces audits sont soumis aux règles applicables aux prestataires d'audit de la sécurité des systèmes d'information.

6. **La Commission nationale de l'informatique et des libertés**

Conformément à l'article 101 de la loi du 6 janvier 1978, la stratégie d'audit ainsi que la programmation des audits sont transmises par le président du comité d'audit au président de la Commission nationale de l'informatique et des libertés. Cette transmission se fait postérieurement à chaque réunion du comité d'audit et pour toute modification de la stratégie ou de la programmation des audits décidée par le président du comité d'audit, dans un délai de 15 jours, par voie électronique.

Le président de la Commission nationale de l'informatique et des libertés ou son représentant peut être présent lors des différentes réunions de travail organisées par les auditeurs et le président du comité d'audit lorsque les auditeurs rendent compte de l'avancement de leurs travaux et des faits constatés.

Aux termes du *g* du 2° du I de l'article 8 de la loi du 6 janvier 1978, la Commission nationale de l'informatique et des libertés « *peut, par décision particulière, charger un ou plusieurs de ses membres ou le secrétariat général, dans les conditions prévues à l'article 19, de procéder ou de faire procéder par les agents de ses services à des vérifications portant sur tous traitements et, le cas échéant, d'obtenir des copies de tous documents ou supports d'information utiles à ses missions* ». La Commission nationale de l'informatique et des libertés peut, indépendamment du comité d'audit, décider de contrôler les entités concernées par le système national des données de santé élargi.

Seule la Commission nationale de l'informatique et des libertés prononce les mesures correctrices prévues à l'article 20 de la loi du 6 janvier 1978 précitée vis-à-vis des entités concernées, en cas de violation.

7. **Relations avec les autres services d'audit ou corps d'inspection et avec les auditeurs externes**

Les auditeurs doivent articuler leurs travaux d'audit avec les services d'audit des établissements et organismes audités lorsqu'ils existent, ainsi qu'avec les auditeurs externes.

Les auditeurs tiennent compte dans leurs travaux de ceux qui ont été préalablement menés par d'autres auditeurs internes ou externes et qui, de manière directe ou indirecte, participent à l'évaluation du dispositif de maîtrise des risques des entités contrôlées.

Dans le respect des règles de diffusion des rapports et des règles de confidentialité, notamment en matière de défense, et sauf disposition légale contraire, le président du comité d'audit tient à la disposition du Haut fonctionnaire de défense et de sécurité du ministre chargé de la santé, des responsables des entités auditées et de tout organe de contrôle susceptible d'intervenir dans son périmètre d'action (chefs des inspections générales, Autorité de contrôle prudentiel et de résolution, Cour des comptes…) les rapports produits.

ANNEXE II

RÈGLES RELATIVES À LA DÉONTOLOGIE

1. **Introduction**

La déontologie peut être définie comme l'ensemble des règles et devoirs que l'exercice de leur activité impose à des individus. Cet ensemble doit être mis en relation avec les droits reconnus et garanties données pour que cette activité soit convenablement exercée.

La présente annexe, en complément de la charte d'audit, a notamment pour but de promouvoir une culture de l'éthique au sein de la profession.

Elle s'articule avec les droits et obligations définis par le statut général de la fonction publique et par les statuts particuliers qui s'imposent aux auditeurs qui en relèvent.

Elle s'applique aux auditeurs en charge des audits programmés par le comité d'audit, ainsi qu'à toute personne qui serait associée à ces audits.

2. **Définition de l'audit**

L'audit est une activité exercée de manière indépendante et objective qui donne à chaque ministre ou à chaque entité qui le demande, une assurance sur le degré de maîtrise des opérations et lui apporte des conseils pour les améliorer. L'audit s'assure ainsi que les dispositifs de contrôle interne sont efficaces.

3. **Définition des auditeurs**

Les auditeurs concernés par la présente annexe sont ceux en charge des audits décidés par le président du comité d'audit.

4. **Principes fondamentaux**

Il est attendu des auditeurs qu'ils respectent et appliquent les principes fondamentaux suivants :

1. Intégrité : les auditeurs exercent leurs missions avec responsabilité, honnêteté et droiture. Ils s'abstiennent en toute circonstance de tout agissement contraire à l'honneur et à la probité. L'intégrité des auditeurs est à la base de la confiance et de la crédibilité accordées à leur jugement.

2. Objectivité : les auditeurs montrent le plus haut degré d'objectivité professionnelle en collectant, évaluant et communiquant les informations relatives à l'activité ou au processus examiné. Ils évaluent de façon équitable tous les éléments pertinents et ne se laissent pas influencer dans leur jugement par leurs propres intérêts ou par autrui.

3. Confidentialité : les auditeurs respectent le contenu et la propriété des informations qu'ils reçoivent. Ils ne divulguent ces informations qu'avec les autorisations requises, à moins qu'une obligation légale et professionnelle ne les oblige à le faire.

4. Compétence : les auditeurs utilisent et appliquent les connaissances, savoir-faire et expériences requis pour la réalisation de leurs travaux.

5. Indépendance : les auditeurs devant être indépendants personnellement, hiérarchiquement et fonctionnellement de l'entité auditée, tout lien d'intérêt direct ou par personne interposée avec l'entité auditée susceptible de créer une situation de conflit d'intérêts est proscrit.

6. Discernement : les auditeurs doivent, vis-à-vis des sujets audités comme des personnels rencontrés, apprécier avec justesse et clairvoyance les situations, les faits et adopter les comportements les plus adaptés au contexte de l'entité auditée.

5. **Règles de conduite**

5.1. *Intégrité*

1.1. Les auditeurs respectent les lois et règlements ainsi que les règles de la profession et font les révélations requises.

1.2. Ils ne doivent pas prendre part à des activités illégales ou s'engager dans des actes déshonorants pour l'activité d'audit ou leur organisation.

1.3. Ils respectent et contribuent aux objectifs du ministère des solidarités et de la santé.

1.4. Tout auditeur à qui est confié une mission d'audit est responsable de son exécution ainsi que de la rédaction du rapport d'audit. Il conserve cette responsabilité lors de la remise du rapport et au-delà.

5.2. *Objectivité*

2.1. Les auditeurs ne doivent pas prendre part à des activités ou établir des relations qui pourraient compromettre ou risquer de compromettre le caractère impartial de leur jugement. Ce principe vaut également pour les activités ou relations d'affaires qui pourraient entrer en conflit avec les intérêts de l'Etat.

2.2. Les auditeurs ne doivent rien accepter qui pourrait compromettre ou risquer de compromettre leur jugement professionnel.

2.3. Les auditeurs sont tenus de révéler tous les faits matériels dont ils ont connaissance et qui, s'ils n'étaient pas révélés, auraient pour conséquence de fausser le rapport sur les activités examinées.

2.4. Les auditeurs s'efforcent dans leurs rapports à la rigueur et à la précision. La rédaction ne doit être ni vague ni ambiguë.

2.5. Les auditeurs s'attachent à respecter les principes du contradictoire.

5.3. *Confidentialité*

3.1. Les auditeurs utilisent avec prudence et protègent les informations recueillies dans le cadre de leurs activités, le cas échéant, les informations extraites des systèmes audités et le contenu des rapports d'audit sans préjudice des obligations qui s'imposent à tout fonctionnaire en cas de suspicion de fraude.

3.2. Les auditeurs ne doivent pas utiliser ces informations pour en retirer un bénéfice personnel ou d'une manière qui contreviendrait aux dispositions légales et réglementaires ou porterait préjudice aux objectifs de l'administration.

5.4. *Compétence*

4.1. Les auditeurs ne doivent s'engager que dans des travaux pour lesquels ils ont les connaissances, le savoir-faire et l'expérience nécessaires.

4.2. Les auditeurs réalisent leurs travaux d'audit dans le respect des normes ISO, du cadre de référence de l'audit dans l'administration de l'Etat et des procédures déterminées dans les guides relatifs à l'audit établis au sein du ministère des solidarités et de la santé.

4.3. Il revient aux auditeurs d'entretenir leurs connaissances, d'améliorer leur compétence, l'efficacité et la qualité de leurs travaux.

4.4. Les auditeurs participent à l'amélioration des méthodes appliquées par les équipes d'audit et font profiter de leur expérience les membres des équipes avec lesquelles ils sont amenés à travailler.

5.5. *Indépendance*

5.1. Les auditeurs se récusent lorsqu'il leur est proposé une mission qu'ils n'estiment pas pouvoir assurer avec l'indépendance nécessaire. En cas de doute, ils saisissent le chef du service d'audit dont ils dépendent qui consulte le président du comité d'audit qui prendra la décision de retirer ou maintenir l'auditeur sur la mission.

5.2. Les auditeurs ne peuvent participer à une mission s'ils sont liés par parenté, alliance, intérêt économique et financier, notamment, avec l'un des acteurs de l'entité auditée ou s'ils ont un intérêt moral ou affectif, économique ou financier, notamment, dans l'entité auditée.

5.3. Les auditeurs ne peuvent intervenir dans la réalisation d'une mission d'audit concernant une entité qu'ils ont quittée depuis moins de trois ans.

5.4. Aucun auditeur ne doit être affecté dans une entité qu'il a auditée au cours des douze derniers mois.

5.5. Les auditeurs refusent, dans le déroulement des missions, les situations qui pourraient porter atteinte à leur indépendance.

5.6. *Discernement*

6.1. Les auditeurs orientent leurs travaux pour répondre avec efficacité aux objectifs de l'audit tout en favorisant l'atteinte des objectifs généraux du comité d'audit.

6.2. Les auditeurs limitent leurs demandes à destination des services aux éléments utiles pour leurs missions et adaptent autant que possible les modalités de ces missions à la charge et au calendrier de travail des entités auditées pour éviter toute situation d'inutile tension.

6.3. Les auditeurs doivent faire preuve de courtoisie, s'abstenir de toute parole blessante, de toute attitude malveillante, de tout écrit public ou privé susceptibles de nuire à l'entité et à ses agents.

Les présentes règles doivent être connues de l'ensemble des acteurs qui participent aux missions programmées par le président du comité d'audit.

Tous les membres du comité d'audit signent un exemplaire du présent document détenu par le président du comité d'audit signifiant qu'ils ont pris de connaissance des obligations qui s'imposent à eux dans le cadre de l'exercice de leur participation au comité d'audit et qu'ils s'engagent à les respecter.