NORME INTERNATIONALE

ISO 27789

Première édition
2013-03-01

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

Health informatics — Audit trails for electronic health records

Numéro de référence
ISO 27789:2013(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 27789 a été élaborée par le comité technique ISO/TC 215, *Informatique de santé*.

0 Introduction

0.1 Généralités

Parmi tous les types d'informations personnelles, les informations personnelles de santé sont considérées comme étant les plus confidentielles et la protection de leur confidentialité est essentielle au respect de la vie privée des sujets de soins. Afin de protéger la qualité des informations en matière de santé, il est également important que leur cycle de vie entier puisse être entièrement expertisé. Il convient de créer, de traiter et de gérer les dossiers de santé de façon à garantir l'intégrité et la confidentialité de leur contenu et à permettre aux sujets de soins de contrôler de manière tout à fait légitime la façon dont les dossiers sont créés, utilisés et conservés.

Se reposer sur des dossiers informatisés de santé nécessite des éléments de sécurité physiques et techniques ainsi que des éléments d'intégrité des données. Les exigences en matière d'expertise et de contrôle d'accès comptent parmi les plus importantes exigences de sécurité pour la protection des informations personnelles propres à la santé et l'intégrité des dossiers. Elles permettent de respecter les obligations envers les sujets de soins confiant leurs informations aux systèmes de dossiers informatisés de santé (DIS). Elles permettent également de protéger l'intégrité du dossier, car elles incitent fortement les utilisateurs à se conformer aux politiques organisationnelles appliquées à l'usage de ces systèmes.

Une expertise et un contrôle d'accès efficaces peuvent favoriser la découverte d'abus perpétrés sur des systèmes de DIS ou des données de DIS et peuvent aider les organisations et les sujets de soins à obtenir réparation des utilisateurs ayant abusé de leurs privilèges d'accès. Afin que l'expertise soit efficace, il est nécessaire que les historiques d'expertise contiennent suffisamment d'informations pour permettre le traitement de situations très diverses (voir Annexe A).

Les rapports d'expertise et les contrôles d'accès sont complémentaires. Les rapports d'expertise fournissent un moyen d'évaluer la conformité avec les politiques organisationnelles en matière d'accès et peuvent contribuer à l'amélioration et à l'épuration de la politique en elle-même. Mais étant donné que ces politiques doivent anticiper les cas imprévus et les cas d'urgence, l'analyse de ces rapports d'expertise devient dans ces cas-là le meilleur moyen d'assurer le contrôle des accès.

La présente Norme internationale est strictement limitée au contrôle de l'accès aux événements. Les modifications de valeurs effectuées sur les champs d'un DIS sont supposées être enregistrées dans la base de données de DIS et non dans le rapport d'expertise. Le système de DIS est supposé contenir les valeurs de chaque champ, avant et après leur mise à jour. Cela est conforme aux architectures de base de données actuelles. Le rapport d'expertise en soi n'est supposé contenir aucune information personnelle autre que les identifiants et les liens visant les dossiers.

Le dossier informatisé de santé propre à un certain individu peut appartenir à plusieurs systèmes d'informations situés à l'intérieur ou au-delà des frontières organisationnelles voire même juridictionnelles. Afin de garder la trace de toutes les actions impliquant les dossiers relatifs à un sujet de soins en particulier, l'existence d'une structure commune est nécessaire. La présente Norme internationale fournit cette structure. Afin de permettre l'obtention d'historiques d'expertise à travers divers domaines distincts, il est essentiel d'inclure des références au sein de cette structure se rapportant aux politiques spécifiant les exigences du domaine, telles que les règles de contrôle d'accès et les périodes de validité. Les politiques propres au domaine peuvent être référencées implicitement par l'identification de la source du rapport d'expertise.

0.2 Avantages propres à l'utilisation de la présente Norme internationale

La normalisation des historiques d'expertise concernant l'accès aux dossiers informatisés de santé a deux objectifs:

— assurer que l'information contenue dans le rapport d'expertise est suffisante pour reconstruire clairement la chronologie détaillée des événements ayant conduit au contenu d'un dossier informatisé de santé, et

— assurer que l'historique d'expertise des actions relatives au dossier d'un sujet de soins puisse être suivi de façon fiable, même si elles sont réparties sur différents domaines organisationnels.

La présente Norme internationale est destinée aux responsables de la supervision de la sécurité ou de la confidentialité des informations de santé, aux organismes de santé et aux autres dépositaires d'informations personnelles de santé, qui sont à la recherche de lignes directrices concernant les historique d'expertise, ainsi qu'à leurs conseillers en matière de sécurité, consultants, vérificateurs, vendeurs et prestataires externes de service.

0.3 Comparaison avec les normes relatives aux historiques d'expertise des dossiers informatisés de santé

La présente Norme internationale est conforme aux exigences de l'ISO 27799:2008, dans la mesure où elles font référence à l'expertise et à l'historique d'expertise.

Certains lecteurs peuvent être familiarisés avec le document RFC 3881[13] [Request For Comment (demande de commentaires)] de l'Internet Engineering Task Force (IETF). (Les lecteurs n'étant pas encore familiarisés avec le document RFC 3881 de l'IETF n'ont pas besoin de consulter ce document, car la méconnaissance de ce dernier ne gênera pas la compréhension de la présente Norme internationale). Le document RFC 3881 informatif, daté du mois de septembre 2004 et répertorié comme n'étant plus d'actualité dans la base de données de l'IETF, fut une première tentative utile de spécification du contenu des rapports d'expertise en matière de santé. Dans la mesure du possible, la présente Norme internationale est élaborée sur la base du travail débuté dans le document RFC 3881 concernant l'accès aux DIS et lui est conforme.

0.4 Note concernant la terminologie

Plusieurs termes connexes sont définis dans l'Article 3. Un *rapport d'expertise* est une séquence chronologique d'*enregistrements d'expertise*, chaque enregistrement d'expertise contenant la preuve de son appartenance directe à l'exécution d'un processus ou d'une fonction du système. Dans la mesure où les systèmes de DIS peuvent être des agrégations complexes de systèmes et de bases de données, il peut y avoir plusieurs rapports d'expertise contenant les informations relatives aux événements du système ayant modifié le dossier informatisé de santé d'un sujet de soins. Même si les termes *historique d'expertise* et *rapport d'expertise* sont souvent utilisés de façon interchangeable, dans la présente Norme internationale, le terme *historique d'expertise* fait référence à l'ensemble de tous les enregistrements d'expertise d'un ou de plusieurs rapports d'expertise faisant référence à un sujet de soins, à un dossier informatisé de santé ou à un utilisateur particulier. Un *système d'expertise* fournit toutes les fonctions de traitement de l'information nécessaires à la mise à jour d'un ou de plusieurs rapports d'expertise.

Informatique de santé — Historique d'expertise des dossiers de santé informatisés

1 Domaine d'application

La présente Norme internationale spécifie une structure commune pour les historiques d'expertise des dossiers informatisés de santé (DIS), en termes d'événements déclencheurs d'expertise et de données d'expertise, afin de conserver l'ensemble des informations personnelles de santé pouvant être expertisées sur tous les systèmes et domaines d'information.

Elle s'applique aux systèmes de traitement des informations personnelles de santé qui, conformément à l'ISO 27799, créent un enregistrement d'expertise sûr chaque fois qu'un utilisateur crée des informations personnelles de santé, qu'il y accède, qu'il les met à jour ou qu'il les archive par le biais du système.

NOTE Au minimum, ces enregistrement d'expertise identifient de manière unique l'utilisateur, identifient de manière unique le sujet de soins, identifient la fonction exécutée par l'utilisateur (création d'un dossier, accès à un dossier, mise à jour d'un dossier, etc.) et enregistrent la date et l'heure auxquelles la fonction a été exécutée.

La présente Norme internationale ne couvre que les actions effectuées sur le dossier informatisé de santé, qui sont régies par une politique d'accès propre au domaine dans lequel s'inscrit le dossier informatisé de santé. Elle ne traite pas des informations personnelles de santé issues de dossier informatisé de santé mais uniquement des identifiants, l'enregistrement d'expertise ne contenant que les liens menant aux segments du dossier informatisé de santé, tel qu'établi par la politique d'accès en vigueur.

Elle ne couvre pas non plus la spécification et l'utilisation des rapports d'expertise dans un but de gestion et de sécurité du système, par exemple pour la détection des problèmes de performance, des failles au niveau des applications, ou en tant que support pour la reconstruction des données, qui sont traitées par les normes de sécurité informatique générales telles que l'ISO/CEI 15408[9].

L'Annexe A donne des exemples de scénarios d'expertise. L'Annexe B donne un aperçu des services de rapport d'expertise.

2 Références normatives

Les documents de référence suivants sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 8601:2004, *Éléments de données et formats d'échange — Échange d'information — Représentation de la date et de l'heure*

ISO 27799:2008, *Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

3.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à l'activité métier et à la sécurité

[ISO/CEI 27000:2009, définition 2.1]

3.2
politique d'accès
définition des obligations concernant l'autorisation de l'accès à une ressource

3.3
responsabilité
principe selon lequel les personnes physiques et morales, ainsi que la collectivité, sont responsables de leurs actions et peuvent être tenues d'en rendre compte

[ISO 15489-1:2001, définition 3.2]

3.4
expertise
examen systématique et indépendant des accès, ajouts ou modifications appliqués aux dossiers informatisés de santé afin de déterminer si les activités ont été effectuées et si les données ont été recueillies, utilisées, conservées ou divulguées conformément aux normes organisationnelles en termes de procédures de fonctionnement, de politiques, de bonnes pratiques cliniques et d'exigences réglementaires applicables

3.5
archive d'expertise
ensemble d'archive d'un ou de plusieurs rapports d'expertise

3.6
données d'expertise
données obtenues à partir d'un ou de plusieurs enregistrements d'expertise

3.7
rapport d'expertise
séquence chronologique des enregistrements d'expertise, chacun contenant les données concernant un événement spécifique

3.8
enregistrement d'expertise
enregistrement d'un événement unique particulier ayant eu lieu au cours du cycle de vie du dossier informatisé de santé

3.9
système d'expertise
système de traitement de l'information permettant de mettre à jour un ou plusieurs rapports d'expertise

3.10
historique d'expertise
ensemble d'enregistrements d'expertise, provenant d'un ou de plusieurs rapports d'expertise, relatifs à un sujet de soins spécifique ou à un dossier informatisé de santé en particulier

3.11
authentification
moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée

[ISO/CEI 27000:2009, définition 2.5]

3.12
autorisation
attribution de privilèges, comprenant la permission d'accès aux données et fonctions

Note 1 à l'article: Adapté de l'ISO 7498-2: l'attribution de droits, comprenant la permission d'accès sur la base de droits d'accès.

3.13
autorité
entité responsable de l'octroi des certificats

3.14
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

[ISO/CEI 27000:2009, définition 2.7]

3.15
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés

[ISO/CEI 27000:2009, définition 2.9]

3.16
temps universel coordonné
UTC
échelle de temps qui constitue la base d'une diffusion radioélectrique coordonnée des fréquences étalons et des signaux horaires, qui a la même marche que le temps atomique international, mais qui en diffère d'un nombre entier de secondes

[CEI 60050-713:1998]

3.17
intégrité des données
propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée

[ISO 7498-2:1989, définition 3.3.21]

3.18
dossier informatisé de santé
DIS
ensemble structuré et complet d'informations cliniques, démographiques, environnementales, sociales et financières inclues dans un formulaire électronique et concernant les soins de santé procurés à un individu

3.19
segment de DIS
partie d'un DIS constituant une ressource distincte pour la politique d'accès

3.20
identification
exécution de tests permettant à un système informatique de reconnaître des entités

[ISO/CEI 2382-8:1998, définition 08.04.12 (validation d'identité)]

3.21
identifiant
élément d'informations utilisé pour déclarer une identité, avant une éventuelle corroboration, par un authentifiant correspondant

3.22
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

[ISO/CEI 27000:2009, définition 2.19]

3.23
intégrité
propriété de protection de l'exactitude et de l'exhaustivité des actifs

[ISO/CEI 27000:2009, définition 2.25]

3.24
identifiant d'objet
OID
identifiant unique à l'échelle planétaire d'un objet d'information

Note 1 à l'article: Les identifiants d'objet utilisés dans la présente Norme internationale correspondent à des systèmes de code. Ces systèmes de code peuvent être définis dans une norme ou peuvent être définis localement par une implémentation. L'identifiant d'objet est spécifié en utilisant la notation de syntaxe abstraite numéro 1 (ASN.1) définie dans l'ISO/CEI 8824-1 et dans l'ISO/ CEI 8824-2.

3.25
politique
ensemble d'obligations légales, politiques, organisationnelles, fonctionnelles et techniques destinées à la communication et à la coopération

[ISO/TS 22600]

3.26
privilège
capacité assignée à une entité par une autorité

3.27
gestion des enregistrements
champ de gestion en charge du contrôle efficace et systématique de la création, de la réception, de la conservation, de l'utilisation et du sort final des documents, y compris des processus de recueil et de conservation des preuves et des informations concernant les opérations et les transactions sous forme d'enregistrements

[ISO 15489-1:2001, définition 3.16]

3.28
rôle
ensemble de compétences et/ou de performances, associé à une tâche

3.29
sensibilité
mesure du risque ou du risque perçu qu'un sujet subisse un préjudice associé à ces données ou que celles-ci soient utilisées de manière abusive ou soient mal utilisées

3.30
politique de sécurité
plan ou programme d'action adopté pour assurer la sécurité informatique

[ISO/CEI 2382-8:1998, définition 08.01.06]

3.31
sujet de soins
personne dont il est prévu qu'elle reçoive, recevant ou ayant reçu des soins de santé

[ISO 18308:2011, définition 3.47]

3.32
utilisateur
personne, dispositif ou programme utilisant un système de DIS pour traiter des données ou échanger des informations de santé

4 Symboles et abréviations

EHR Electronic Health Record (Dossier informatisé de santé, DIS)

HL7 Health Level Seven International (Niveau international de santé sept)

OID Object Identifier (Identifiant d'objet)

UTC Coordinated Universal Time (Temps universel coordonné)

5 Exigences et usages des données d'expertise

5.1 Exigences éthiques et formelles

5.1.1 Généralités

Les prestataires de soins de santé ont certaines responsabilités professionnelles et éthiques à assumer, comme entre autres, la protection de la vie privée des sujets de soins ainsi que la documentation des conclusions et des activités de soins. Limiter l'accès aux dossiers de santé et assurer leur utilisation appropriée sont deux conditions essentielles en ce qui concerne les soins de santé et sont imposées par la loi dans de nombreuses juridictions.

Les historiques d'expertise sécurisés concernant les accès aux dossiers informatisés de santé peuvent appuyer la conformité avec l'éthique professionnelle, les politiques organisationnelles et la législation, mais ils ne sont pas suffisants en eux-mêmes pour évaluer la totalité d'un dossier informatisé de santé.

5.1.2 Politique d'accès

Une organisation responsable de la mise à jour d'un rapport d'expertise doit identifier la politique d'accès régissant tous les accès enregistrés.

La politique d'accès doit être conforme à l'ISO 27799:2008, 7.8.1.2.

NOTE 1 La politique d'accès est censée définir la structure d'un segment de DIS.

NOTE 2 Dans l'enregistrement d'expertise, la politique d'accès est identifiée par la source du rapport d'expertise.

5.1.3 Identification sans équivoque des utilisateurs du système informatique

Les historiques d'expertise doivent fournir suffisamment de données pour identifier sans équivoque tous les utilisateurs autorisés du système d'informations de santé. Les utilisateurs du système d'informations peuvent tout aussi bien être des personnes ou d'autres entités.

Les historiques d'expertise doivent fournir suffisamment de données pour déterminer quel utilisateur autorisé ou système externe a accédé à ou a reçu des dossiers de santé de la part du système.

5.1.4 Rôles des utilisateurs

L'historique d'expertise doit présenter le rôle de l'utilisateur ayant effectué l'action enregistrée sur les informations personnelles de santé.

Il convient que les systèmes d'informations traitant des informations personnelles de santé soient pourvus d'un contrôle d'accès spécifique selon le rôle qui soit en mesure de mettre en correspondance chaque utilisateur à un ou plusieurs rôles et chaque rôle à une ou plusieurs fonctions du système, comme recommandé dans l'ISO 27799:2008, 7.8.2.2.

Les rôles fonctionnels et structurels sont documentés dans l'ISO/TS 21298[4]. Des lignes directrices supplémentaires sur la gestion des privilèges dans le domaine de la santé sont données dans l'ISO/TS 22600 (toutes les parties)[6].

5.1.5 Enregistrements d'expertise sécurisés

Des enregistrements d'expertise sécurisés doivent être créés à chaque fois que des informations personnelles de santé sont consultées, créées, mises à jour ou archivées, conformément à l'ISO 27799:2008, 7.7.10.2. Les enregistrements d'expertise doivent être conservés par le biais d'une gestion sécurisée des enregistrements.

5.2 Usages des données d'expertise

5.2.1 Gouvernance et supervision

Les historiques d'expertise doivent fournir des données permettant aux autorités responsables d'évaluer la conformité avec la politique de l'organisation et son efficacité.

Ceci implique

— la détection des accès non autorisés aux dossiers de santé,

— l'évaluation des accès d'urgence,

— la détection d'abus de privilèges,

et le support de

— la documentation des accès entre les domaines, et

— l'évaluation des politiques d'accès.

NOTE Une évaluation complète de la conformité avec la politique organisationnelle peut nécessiter des données complémetaires qui ne sont pas contenues dans l'enregistrement d'expertise, telles que des informations relatives à l'utilisateur, des tableaux ou des enregistrements de permission sur une entrée physique dans des salles sécurisées. Voir Annexe B en ce qui concerne les services de rapport d'expertise.

Les historiques d'expertise doivent fournir suffisamment de données pour déterminer tous les accès aux dossiers de sujets de soins, ayant eu lieu au cours d'une période déterminée et effectués par un utilisateur donné.

Les historiques d'expertise doivent fournir suffisamment de données pour déterminer tous les accès aux dossiers ayant eu lieu au cours d'une période déterminée et considérés comme représentant un risque élevé de violation de la vie privée.

5.2.2 Sujets de soins exerçant leurs droits

Les historiques d'expertise doivent fournir suffisamment de données pour permettre aux sujets de soins

— d'évaluer quel ou quels utilisateurs ont eu accès à leur dossier de santé et quand,

— d'évaluer la responsabilité concernant le contenu du dossier,

— de déterminer la conformité avec les directives de consentement du sujet de soins concernant l'accès aux données le concernant ou leur divulgation, et

— de déterminer les accès d'urgence au dossier de santé du sujet de soins (le cas échéant) octroyés par un utilisateur, y compris l'identification de l'utilisateur, l'heure d'accès et l'endroit à partir duquel a eu lieu l'accès.

5.2.3 Preuve d'action éthique ou légale du prestataire de soins de santé

Les historiques d'expertise doivent fournir des données permettant de fournir aux prestataires de soins de santé des preuves documentées concernant quelles informations ont été consultées et quelles actions ont été effectuées (création, consultation, lecture, correction, mise à jour, extraction, exportation, archivage, etc.) sur ces informations, quand et par qui.

Il convient d'aligner la conservation des enregistrements d'expertise sur les conditions légales de responsabilité en vigueur au sein de la juridiction.

Voir HL7 EHR Records Management and Evidentiary Support (RM-ES) (Gestion des enregistrements et preuves venant à l'appui).

6 Événements déclencheurs

6.1 Généralités

Les événements d'expertise (événements déclencheurs) qui sont à l'origine de la génération par le système d'expertise d'enregistrements d'expertise sont définis conformément à chaque envergure et objectif des systèmes d'informations de santé et au contenu des politiques de confidentialité et de sécurité. Le domaine d'application de la présente Norme internationale étant limité à l'accès aux informations personnelles de santé, seuls les événements déclencheurs relatifs à l'accès y sont spécifiés.

Afin de générer les enregistrements d'expertise qui satisfont aux exigences de l'Article 5, c'est-à-dire «quand», «qui», «de qui», les deux événements suivants sont obligatoires:

a) les accès aux informations personnelles de santé;

b) les requêtes concernant les informations personnelles de santé.

Des exemples d'événements non couverts sont les suivants:

— démarrage et arrêt de programmes d'application;

— événements d'authentification impliquant l'authentification d'utilisateurs;

— entrée et sortie en provenance/en direction d'un environnement extérieur;

— accès aux informations autres que les informations personnelles de santé;

— alertes de sécurité relatives aux programmes d'application;

— accès au rapport d'expertise contenu dans les programmes d'application;

— événements générés par le système d'exploitation, un logiciel intermédiaire, etc.;

— accès générés par l'utilisation de systèmes utilitaires;

— connexion/déconnexion physique des équipements au réseau;

— démarrage/arrêt des systèmes de protection tels que les systèmes de protection anti-virus;

— mises à jour logicielles impliquant la modification ou la mise à jour de programmes.

6.2 Détails des types d'événements et de leur contenu

6.2.1 Événements d'accès aux informations personnelles de santé

Dans la présente Norme internationale, l'accès aux informations personnelles de santé est considéré comme l'événement d'expertise. Ici «Accès» signifie la création, la lecture, la mise à jour et la suppression

des données. Le rapport d'expertise contient les informations concernant le «quand», «qui» et «de qui» propres à l'accès vers les données à protéger.

Tableau 1 — Événements d'accès

Événement	Contenu
Accès aux informations personnelles de santé	Quand, Qui, De qui

6.2.2 Requêtes concernant les informations personnelles de santé

La requête au niveau de la base de données de DIS formulée dans le but d'obtenir des informations personnelles de santé est considérée comme un événement pouvant être expertisé. La requête représente l'action de requête en elle-même et le référencement aux informations personnelles de santé qui résulte de la requête est considéré comme un événement d'accès. L'enregistrement d'expertise contient les informations concernant la requête «quand», «qui» et «quelles conditions de requête», voir Tableau 2.

Tableau 2 — Requêtes

Événement	Contenu
Requêtes concernant les informations personnelles de santé	Quand, Qui, Quelles conditions de requête

7 Détails des enregistrements d'expertise

7.1 Format d'enregistrement général

Le Tableau 3 décrit le format général des enregistrements d'expertise. Pour le contenu de chaque événement, voir Article 8. Le format d'enregistrement est défini d'après le document RFC3881[13] et le document DICOM[11], avec ajout des champs facultatifs PurposeOfUse et ParticipantObjectPolicySet.

Tableau 3 — Format général des enregistrements d'expertise

Type	Nom du champ	Néces-sité	Description	Info. supplé-mentaire
Relatif à l'événe-ment (1)	EventID	O	ID de l'événement d'expertise	Voir 7.2
	EventActionCode	O	Type de l'opération effectuée lors de l'événement d'expertise	
	EventDateTime	O	Date/heure à laquelle s'est pro-duit l'événement	
	EventOutcomeIndicator	F	Succès ou échec de l'événement	
	EventTypeCode	F	Catégorie de l'événement	
Relatif à l'utilisa-teur (1..2)	UserID	O	ID de la personne ou du proces-sus	Voir 7.3
	AlternateUserID	F	Autre ID pour l'utilisateur ou le processus	
	UserName	F	Nom d'utilisateur ou de proces-sus	
	UserIsRequestor	F	Indicateur précisant si l'utilisa-teur est le demandeur ou non	
	RoleIDCode	F	Spécification du rôle que l'utilisa-teur possède lors de l'événement	
	PurposeOfUse	F	Code stipulant l'objectif de l'utili-sation des données consultées	
	NetworkAccessPointType-Code	F	Type de point d'accès réseau	Voir 7.4
	NetworkAccessPointID	F	ID du point d'accès réseau	
Relatif au système d'expertise (1)	AuditEnterpriseSiteID	F	ID du site au sein de l'organisme expertisé	Voir 7.5
	AuditSourceID	O	ID unique de la source d'expertise	
	AuditSourceTypeCode	F	Code de type de la source d'expertise	

7.2 Identification de l'événement déclencheur

7.2.1 ID de l'événement

Description: Identifiant unique propre à un événement expertisé particulier, par exemple un élément de menu, un programme, une règle, une politique, un code de fonction, un nom d'application ou une adresse URL. Il permet l'identification de la fonction effectuée.

Nécessité: Obligatoire

Format/Valeurs: Valeur codée, définie soit par les implémenteurs du système, soit par référence à un vocabulaire standard. L'attribut «code» doit être sans équivoque et unique, au moins au sein de l'ID de la source d'expertise (voir 7.5). Exemples d'identifiants d'événements: nom de programme, nom de méthode ou nom de fonction.

NOTE Le codage est modélisé selon l'IHE ITI TF-1 et TF-2[12] et l'ISO 12052[1], supplément DICOM 95.