Santé : Vers une culture de conformité étendue aux tiers

1 Le risque tiers, porte d'entrée numéro un de la corruption dans la santé

Le tiers, un maillon incontournable

Le secteur pharmaceutique et celui des dispositifs médicaux n'ont pas fini d'externaliser. Sociétés de recherche contractuelle (CRO), fabricants sous contrat (CMO), distributeurs, agents locaux, intermédiaires réglementaires… Tous sont devenus incontournables. Cette tendance ne va pas s'inverser. Elle va se poursuivre et, avec elle, une surface de risque que l'entreprise ne pilote pas directement.

Le mécanisme est toujours le même : le CRO recrute les patients, le CMO sous-traite la production et le distributeur rémunère ses commerciaux sur le terrain. Leur point commun ? Chacun agit au nom de l'entreprise et engage la responsabilité de la personne morale, sans nécessairement en comprendre les implications pratiques ni partager sa culture de conformité.

Cette dilution structurelle de la responsabilité explique pourquoi le risque tiers est devenu la porte d'entrée privilégiée du risque de corruption dans le secteur de la santé, avec un poids plus lourd que celui de la fraude interne ou des malversations classiques. De simples contrôles ponctuels ne suffisent plus à le réduire de manière significative.

> « *Le risque tiers est devenu la première porte d'entrée du risque de corruption dans le secteur de la santé, devant la fraude interne.* »

Une réglementation qui vise désormais vos partenaires

À cela s'ajoute un véritable millefeuille réglementaire.

Le FCPA s'applique dès qu'un lien avec les États-Unis existe. L'UK Bribery Act, dès qu'un lien britannique apparaît. Sapin II, pour toute entreprise française ou opérant en France. Et plus récemment, la Directive anticorruption de l'Union européenne, qui harmonise ces obligations à l'échelle du marché intérieur.

Cette architecture ne vise plus seulement à dicter la conformité interne. Elle vise, de plus en plus explicitement, à ce que cette conformité s'imprègne chez les tiers. Ces textes ne sont pas seulement déclaratifs.

Chiffres clés — Entre 2010 et 2020, les autorités américaines ont conclu des transactions de 25 à plus de 500 millions de dollars avec plusieurs laboratoires pharmaceutiques dans le cadre de faits de corruption impliquant des intermédiaires ou des professionnels de santé étrangers. Novartis, Sanofi, Teva, SciClone, Eli Lilly, Pfizer… Aucun grand nom du secteur n'y a échappé [1]. En 2025, l'application du FCPA a toutefois marqué une pause, avec une suspension en février [2], puis de nouvelles lignes directrices en juin recentrant les poursuites sur les affaires les plus graves [3]. Cette évolution ne remet pas en cause l'obligation de vigilance des acteurs de la santé à l'égard de leurs tiers.

En 2026, une entreprise pharmaceutique ne peut plus se contenter de contrôler sa cuisine interne. Elle doit être en mesure de démontrer qu'elle a exercé une diligence raisonnable auprès de ceux qui agissent en son nom, y compris indirectement.

Quand corruption et cybersécurité se rejoignent

Un risque sous-estimé complique encore la situation. Lorsque ces tiers accèdent à des données de santé (dossiers de patients dans le cadre d'essais cliniques, données de pharmacovigilance, empreintes bancaires, informations personnelles), le risque de fuite ou de piratage épouse celui de corruption.

Ce risque ne peut plus être traité comme accessoire. Le secteur de la santé est déjà identifié comme celui où le coût moyen d'une violation de données est le plus élevé, tous secteurs confondus.

7,42 millions $
en moyenne par incident en 2025, et ce pour la 14e année consécutive [4].

Les illustrations récentes ne manquent pas :

- En France, la cyberattaque qui a visé le logiciel médical Cegedim Santé a exposé les données administratives de près de **15 millions de patients** début 2026 [5]
- À l'international, le fabricant de dispositifs médicaux Medtronic a confirmé en avril 2026 avoir été visé par une intrusion ayant touché plus de **3,8 millions de personnes** [6]

Un tiers, non contrôlé ou contrôlé à la légère, vous expose également en matière de protection des données.

Ces deux vulnérabilités, la corruption et la protection des données personnelles, se renforcent mutuellement et aggravent les répercussions financières et réputationnelles de l'entreprise mandataire.

2 La conformité ne suffit plus

Les entreprises sanctionnées ne sont presque jamais celles qui n'ont rien fait. Ce sont celles dont le dispositif n'a pas évolué depuis sa création.

Contrairement à un vieux poncif, le véritable obstacle à la prévention des risques éthiques n'est pas réglementaire. Les textes, aussi cumulatifs soient-ils, sont connus et maîtrisés par les équipes juridiques internes et régulièrement commentés afin de faciliter leur mise en œuvre.

Le nerf de la guerre est ailleurs. Il est méthodologique. Les entreprises qui ont structuré la gestion du risque tiers au cours des quinze dernières années ne sont pas toujours à la page face à un risque qui, lui, évolue en continu.

Quatre angles morts reviennent systématiquement :

Angle mort n° 1 — la photographie figée

Les entreprises sanctionnées ne sont pas celles qui n'ont pas cartographié leurs tiers. En réalité, ce sont très souvent celles dont le dispositif n'a pas bougé d'une ligne depuis sa création.

Un tiers évalué comme « sain » à T0 devient un risque réel à T+24 mois : l'actionnariat change, un nouvel intermédiaire s'insère dans la chaîne d'exécution, une alerte remonte d'un commercial sur le terrain, sans que l'outil interne ne l'ait pris en considération.

À l'instar d'une cartographie des risques figée au moment de sa réalisation, un dispositif d'évaluation des tiers immobile ne capture aucun de ces changements. Il se contente de fournir une photographie rassurante d'un paysage qui, en réalité, continue de bouger sans lui.

Angle mort n° 2 — l'uniformité qui masque le risque

Le deuxième obstacle est encore plus structurel : les organisations évaluent leurs tiers selon une attention à géométrie variable.

D'une part, elles s'intéressent en priorité aux tiers qui semblent représenter une réelle menace : une approche cohérente, dans une logique de priorisation des ressources. D'autre part, pour réduire ce biais, les entreprises optent souvent pour l'uniformisation de leur approche : un questionnaire unique, la même fréquence de contrôle, le même niveau de vigilance, qu'il s'agisse d'un grossiste établi depuis vingt ans dans un pays jugé à risque par le GAFI ou d'un nouvel agent local dans une zone plus rassurante.

Cette uniformisation donne la fausse impression d'une couverture exhaustive des risques. En réalité, elle affaiblit durablement la vigilance.

Angle mort n° 3 — la conformité de papier

Le principal écueil de toute démarche de conformité reste le plus rarement assumé : trop de programmes anticorruption poursuivent l'objectif d'être « conformes sur le papier », en produisant de la documentation afin de pouvoir prouver, en cas de contrôle, qu'une procédure existait. Cette raison d'être est légitime. Elle est insuffisante face aux risques qui surviennent dans la vraie vie.

Ce qui devrait guider la structuration d'un programme anticorruption, ce sont la mise en cause personnelle des dirigeants et des responsables, ainsi que le risque très concret d'exclusion des marchés publics à la suite d'une condamnation. Ce basculement n'est plus hypothétique.

Signal fort — Le 9 juillet 2026, la commission des sanctions de l'Agence française anticorruption a prononcé sa toute première sanction pécuniaire sur le fondement de l'article 17 de la loi Sapin II assortie, pour la première fois également, d'une mise en cause personnelle du dirigeant : **350 000 € pour la société, 60 000 € pour son président** [7].

Raisonner en coûts réels plutôt qu'en simple obligation documentaire permet au sujet de changer de nature. Il passe d'un exercice de conformité formelle à un enjeu de pilotage des risques à fort enjeu, au même titre qu'un risque financier ou opérationnel.

Angle mort n° 4 — la dispersion des responsabilités

Un dernier phénomène, plus insidieux, aggrave les trois précédents : la dispersion de la responsabilité en interne. Un risque tiers peut aussi bien toucher les achats, le juridique, la conformité et les affaires médicales. Dans la plupart des organisations, chacune de ces business units fonctionne en silo, sans vision d'ensemble.

Les organisations résilientes ont, au contraire, un point d'entrée unique pour le risque tiers : une fonction ou un comité qui centralise les outils anticorruption (cartographie des risques, dispositif d'alerte interne, contrôles comptables) afin d'arbitrer les priorités et de porter la responsabilité de bout en bout.

Cette approche s'appuie de plus en plus sur des plateformes intégrées de gestion des risques de tiers, qui rassemblent au sein d'un même environnement les évaluations, les alertes, les contrôles, les diligences et les plans d'action. Des solutions comme NAVEX One Third-Party Risk Management contribuent ainsi à offrir une vision consolidée des risques et à assurer un suivi cohérent tout au long du cycle de vie des tiers.

Sans cette coordination, chaque nouvelle alerte relance l'analyse depuis le début, plutôt que de capitaliser sur ce qui a déjà été identifié [8].

> *« Ce ne sont pas les textes qui font défaut. C'est une gouvernance capable de faire vivre le dispositif dans la durée. »*

3 La méthode des organisations les plus matures

Une organisation mature ne se reconnaît pas à ses outils. Elle se reconnaît à sa méthode.

Elle découle d'une méthode appliquée, étape par étape, aux données provenant de son propre programme anticorruption. Trois briques structurent l'approche des entreprises les plus avancées du secteur.

Brique 1 — Segmenter par exposition réelle

La première brique est la segmentation par niveau de risque.

Elle vise à trier les tiers non pas selon leur ancienneté ou leur taille de marché, mais selon des critères découlant de leur exposition réelle : durée de la relation, exposition géographique, proximité avec les prescripteurs ou les décideurs de santé, volume des transactions.

C'est cette approche qui permet ensuite d'allouer les moyens de manière prioritaire plutôt que de manière uniforme.

L'intelligence artificielle peut intervenir à ce stade, non pas pour remplacer les équipes, mais pour accélérer et fiabiliser l'analyse. Elle permet d'agréger et de croiser des données en source ouverte (listes de sanctions internationales, articles de presse, structures actionnariales publiques, rapports d'audit publics) qui sont autrement laborieuses à rassembler manuellement pour chaque tiers.

L'appréciation qualitative et la granularité des contrôles à déployer restent entre les mains du chargé de conformité.

Brique 2 — Coter et prioriser

La deuxième brique est la cotation et la priorisation.

Cette logique reprend le même principe brut/net et probabilité/impact que la cartographie des risques Sapin II, déclinée cette fois au registre des tiers. L'IA peut, là encore, jouer un rôle stratégique en identifiant, à partir de critères prédéfinis, les tiers à évaluer en priorité, ce qui permet à l'équipe conformité de concentrer ses efforts là où elle apporte le plus de valeur ajoutée.

Brique 3 — Surveiller en continu, avec assistance

La troisième et dernière brique est la surveillance continue « assistée ».

L'idée est de passer d'un audit ponctuel tous les deux ans à un système de détection de signaux faibles en continu. C'est dans cette phase que l'IA est la plus stratégique : elle sert à qualifier ces signaux, à détecter des anomalies dans les comportements déclaratifs et à fournir une aide à la décision à l'équipe conformité.

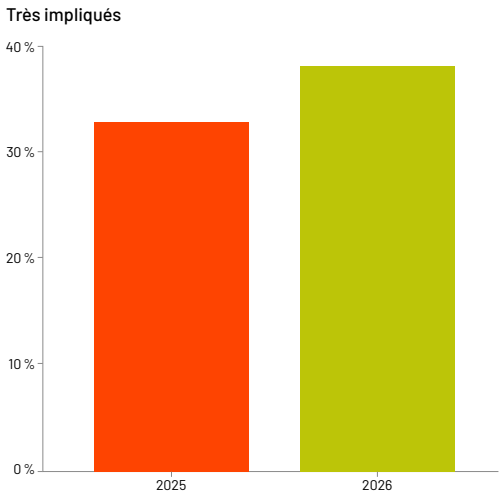
Gouvernance — L'outil signale. L'humain qualifie et décide. La gouvernance reste humaine à chaque étape du circuit, et pas seulement au stade de la surveillance continue.

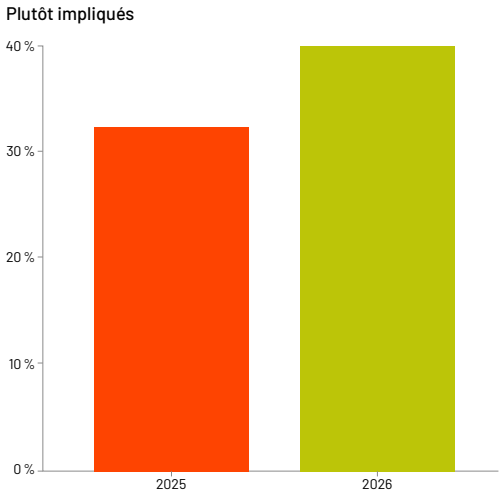
Données NAVEX — L'adoption de l'IA en conformité progresse plus vite que sa gouvernance, même si l'écart tend à se réduire.

En 2026, 38 % des professionnels de la conformité se disent **très impliqués** dans les décisions liées à l'IA au sein de leur organisation, contre 33 % un an plus tôt. Ils sont aussi 40 % à se déclarer **plutôt impliqués**, contre 32 % en 2025.

Cette progression est réelle, mais la gouvernance reste en retrait par rapport aux usages. L'IA est désormais présente dans la quasi-totalité des programmes de conformité : seuls 4 % des professionnels déclarent ne l'utiliser pour aucun cas d'usage.

En clair, les outils se déploient encore plus vite que les mécanismes de gouvernance et la place structurée de l'humain dans la boucle. [9]





Vos données internes valent plus qu'un archivage

Un enjeu reste souvent sous-exploité au sein des entreprises : les évaluations de tiers ne sont pas seulement un output de la gestion interne dont la finalité s'arrête à l'archivage. Agrégées dans le temps, elles constituent une base de données interne permettant de détecter des tendances inquiétantes avant qu'elles ne deviennent des incidents, puis des crises :

- Une concentration de signaux faibles sur une même zone géographique ou un même type d'intermédiaire, indétectable si chaque dossier est traité séparément
- La récurrence du même motif de non-conformité, comme la non-déclaration de cadeaux et avantages accordés à des prescripteurs chez plusieurs tiers d'un même secteur, qui suggère une pratique plutôt qu'un cas isolé, à l'image de l'affaire qui a conduit environ **8 000 pharmaciens**, soit près de 40 % de la profession officinale, à être individuellement mis en cause pour avoir accepté des avantages en marge du dispositif anti-cadeaux [10]
- La détection d'une dérive progressive du profil de risque d'un tiers, qui repose sur la conservation et la comparaison des évaluations successives plutôt que sur le traitement de chaque évaluation comme une photographie indépendante

Ce virage, qui consiste à considérer les données internes comme un actif de pilotage, et non plus seulement comme un « tampon de conformité », est celui qu'opèrent les organisations les plus avancées dans des secteurs à risque tels que le secteur médical et le secteur pharmaceutique.

> « Une organisation bien préparée ne collecte pas les évaluations. Elle les fait parler. »

4 Cas pratique — Le distributeur qu'on n'a pas vu venir

Note : Le scénario suivant est fictif et présenté à des fins pédagogiques uniquement ; il ne représente aucune entreprise réelle. Les prénoms sont également fictifs.

Le siège social se trouve en banlieue parisienne. Le terrain, lui, est à quatre mille kilomètres, dans un pays d'Afrique de l'Ouest où l'entreprise, fabricant de dispositifs médicaux de taille intermédiaire, vend ses produits depuis six ans.

Céline dirige la conformité depuis Paris. Sur place, un seul interlocuteur : Ibrahima, distributeur local, qui parle la langue des acheteurs hospitaliers et connaît chaque chef de service par son prénom.

Ibrahima n'est pas un simple revendeur. Il est la voix de l'entreprise auprès des hôpitaux de la région. Sans lui, aucun dossier n'avance, aucun marché ne se débloque.

Céline ne parle pas la langue locale. Les rapports qu'elle reçoit sont traduits, résumés et filtrés. Elle sait ce qu'Ibrahima veut bien lui dire, et pas plus. Sur le terrain, les commerciaux d'Ibrahima multiplient les visites auprès des prescripteurs hospitaliers. Leur fréquence augmente, doucement, mois après mois.

Rien d'alarmant sur le papier. Mais leur fréquence et leur nature ne sont ni documentées ni consignées par l'entreprise mandante. Personne ne s'en étonne, après tout : plus de visites, plus de commandes. Céline, elle, ne voit que les chiffres de vente. Ils sont bons. Très bons, même.

Le signal existe pourtant. C'est un signal faible qui passe inaperçu dans l'activité commerciale courante, à quatre mille kilomètres et une barrière de langue pour tout regard extérieur. Puis un signal finit par remonter, tardivement, par le mauvais canal. C'est un audit externe, mené dans le cadre d'une opération de croissance, qui le détecte.

Céline découvre en quelques jours une situation qu'elle aurait pu identifier bien plus tôt si elle avait disposé de bons points de contrôle. La conséquence est directe : ouverture d'un contrôle par les autorités, risque de sanctions financières et un coût réputationnel dont les répercussions dépassent largement le cadre de la seule relation avec Ibrahima.

Ce que la méthode en trois briques aurait changé

Reprenons ce scénario à la lumière de la méthode présentée précédemment.

Une segmentation par exposition réelle aurait immédiatement classé Ibrahima dans la catégorie de suivi prioritaire, en raison de son exposition géographique, de sa proximité directe avec des prescripteurs hospitaliers et d'un volume de transactions significatif. Mais aussi en raison d'une barrière linguistique qui réduisait d'autant la visibilité du siège sur son activité réelle.

Une surveillance continue assistée par l'IA aurait permis de qualifier la fréquence inhabituelle des visites comme un signal à observer en priorité, bien avant qu'il ne devienne une alerte externe. C'est précisément dans cette direction que s'orientent les nouveaux agents d'IA spécialisés en conformité, comme Nira de NAVEX. Ils sont capables de détecter des patterns à travers les dossiers et les données de programme pour faire émerger plus tôt des risques ou des tendances qui échapperaient à un examen manuel, tout en laissant le jugement humain au centre de la décision finale [11].

Enfin, si les données internes avaient pu être comparées à celles d'autres distributeurs opérant dans des contextes similaires, le niveau de visites non documentées et les avantages associés auraient pu être identifiés comme une anomalie structurelle plutôt que comme une pratique isolée propre à Ibrahima. Céline aurait pu poser la question trois mois plus tôt. Pas dix-huit mois plus tard.

À retenir — Cette méthode ne garantit pas qu'un incident soit toujours évité, car le risque zéro n'existe pas.

Mais la différence entre une détection à T-3 mois et une découverte à T+18 mois se mesure directement en termes de risque de sanction et de coût réputationnel.

Conclusion — Piloter votre registre, pas seulement cocher des cases

La bonne nouvelle : cette maîtrise ne demande pas de tout reconstruire, mais de changer de méthode. Les organisations qui l'ont fait en mesurent déjà les bénéfices.

Trois constats se dégagent de ce livre blanc :

- Le risque tiers, appliqué au secteur de la santé, est devenu le point d'entrée principal du risque de corruption, et il continuera de s'élargir avec l'externalisation du secteur
- La conformité de façade – cartographie figée, traitement uniforme des tiers, audits ponctuels – ne suffit plus face à un risque multifactoriel en constante évolution
- Les organisations les plus robustes s'organisent autour d'une méthode en trois briques (segmentation, priorisation, surveillance continue assistée), appuyée par les données internes et l'IA à chaque étape, mais jamais en substitut de la décision humaine

Cette méthode ne vise pas seulement à réduire le risque de sanctions. Elle produit quatre bénéfices distincts et complémentaires :

- **Conformité** — réduction du risque de sanction et de mise en cause personnelle
- **Efficacité opérationnelle** — allocation des ressources de contrôle sur les tiers prioritaires, plutôt qu'un traitement à l'aveugle de l'ensemble du portefeuille
- **Gain de temps** — une réévaluation continue plutôt que des campagnes d'audit coûteuses et périodiques
- **Gouvernance et visibilité** — une vision consolidée et à jour du registre des tiers à risque, communicable à la direction et, le cas échéant, aux autorités de contrôle

D'ici quelques années, ce qui distinguera les entreprises les plus performantes ne sera plus la taille de leur dispositif de conformité, mais leur capacité à évoluer aussi vite que leurs tiers.

Le risque tiers ne se réduit pas en ajoutant des contrôles, mais en changeant la manière dont l'organisation regarde ses tiers : moins comme une liste à cocher, davantage comme un portefeuille à piloter dans la durée.

> *« Le risque tiers ne se réduit pas en ajoutant des contrôles, mais en changeant de regard. »*

Sources

[1] SEC, *Foreign Corrupt Practices Act — Enforcement Actions* (chronologie des transactions, y compris Teva 2016 à 519 M$ et Novartis 2020) — https://www.sec.gov/enforce/foreign-corrupt-practices-act

[2] Executive Order 14209 — *Pausing Foreign Corrupt Practices Act Enforcement To Further American Economic and National Security*, Federal Register, 14 février 2025 — https://www.federalregister.gov/documents/2025/02/14/2025-02736/pausing-foreign-corrupt-practices-act-enforcement-to-further-american-economic-and-national-security

[3] Todd Blanche (Deputy Attorney General), *Guidelines for Investigations and Enforcement of the Foreign Corrupt Practices Act* (FCPA), mémorandum du DOJ, 9 juin 2025 — https://www.justice.gov/dag/media/1403031/dl

[4] HIPAA Compliant Hosting, « Healthcare Data Breach Statistics 2026 » (données IBM Cost of a Data Breach Report) — https://hipaacomplianthosting.com/blog/healthcare-data-breach-statistics

[5] France 24, « Les données personnelles de 15 millions de patients piratées en France », 27 février 2026 — https://www.france24.com/fr/france/20260227-donn%C3%A9es-m%C3%A9dicales-15-millions-de-fran%C3%A7ais-pirat%C3%A9es-sant%C3%A9-cyberattaque

[6] HIPAA Journal, « Medical Device Maker Medtronic Notifies 3.8M Individuals About April 2026 Cyberattack » — https://www.hipaajournal.com/medical-device-maker-medtronic-data-breach/

[7] Agence Française Anticorruption, communiqué de presse — Commission des sanctions, 9 juillet 2026 — https://www.agence-francaise-anticorruption.gouv.fr/files/2026-07/Communiqu%C3%A9%20de%20presse%20commission%20des%20sanctions%20AFA%20affaire%20Soci%C3%A9t%C3%A9%20V.%20et%20M.%20S.%20.pdf

[8] NAVEX, plateforme NAVEX One — Third-Party Risk Management — https://www.navex.com/fr-fr/plateforme/gestion-du-risque-tiers/

[9] NAVEX (en partenariat avec Alan Agency), *L'état du risque et de la conformité en France 2026* — https://www.navex.com/fr-fr/northstar/etat-des-risques-et-de-la-conformite-en-france-2026/

[10] Village de la Justice / ACG Avocats & Associés, synthèse de l'affaire Laboratoires Urgo (tribunal judiciaire de Dijon, 27 janvier 2023) — https://www.village-justice.com/articles/professionnels-sante-loi-anti-cadeaux-comment-reagir-cas-convocation-dgccrf,48738.html

[11] NAVEX, NIRA, l'agent IA de NAVEX intégré à NAVEX One — https://www.navex.com/fr-fr/gestion-des-risques-et-conformite-assistees-par-l-ia/