Hôpital privé de la Loire : l'éditeur du DPI, tiers non jugé

Le 3 septembre 2026, la CNIL a rendu publique une amende de 500 000 euros contre l'Hôpital privé de la Loire, à Saint-Étienne. Parmi les cinq faiblesses de sécurité que la CNIL sanctionne au titre de l'article 32 du RGPD, selon Caducée.net, figure l'accès permanent dont disposait l'éditeur du dossier patient informatisé (DPI), désormais subordonné à l'autorisation préalable de l'établissement, dans une décision qui restera nominative pendant deux ans. L'acteur qui détient les clés du logiciel n'est pourtant pas partie à la procédure. La régulation corrige ainsi par injonction individuelle ce qui relève d'une propriété du marché des systèmes d'information hospitaliers. L'article lit ce décalage à travers le problème des mains multiples de Dennis F. Thompson et en tire les conséquences pour les groupements hospitaliers de territoire (GHT) publics.

Par Alexandre Berge · 11 octobre 2026 · 17 min de lecture · Analyse

Une sanction exemplaire qui ne désigne qu'un seul responsable

Les faits sont établis par le communiqué de la CNIL et par la délibération de la formation restreinte n° SAN-2026-009 du 21 juillet 2026. Au cours de l'été 2025, un attaquant s'est connecté au DPI de l'établissement, qui appartient au groupe Ramsay Santé, avec les identifiants d'un médecin libéral. Il a accédé aux données de 524 867 patients et de 202 246 personnes désignées comme « tiers de confiance ». Selon Caducée.net, qui cite la délibération, 46 185 des fiches exfiltrées comportaient le recto d'une carte nationale d'identité et 43 des données de santé. La séquence, reconstituée à partir du communiqué et de la presse spécialisée qui cite la délibération, est la suivante.

- 26 juin au 1er juillet 2025 : exfiltration des fiches patients, à un rythme moyen de 73 fiches par minute selon l'analyse des journaux citée par Next et Caducée.net.
- 4 juillet 2025 : notification de la violation à la CNIL, sans manquement retenu au titre de l'article 33 du RGPD selon Caducée.net.
- Septembre 2025 : déploiement de l'authentification multifacteur choisie par le groupe.
- 21 juillet 2026 : délibération de la formation restreinte.
- 3 septembre 2026 : publication de la sanction.

La CNIL retient deux fondements. Au titre de l'article 32 du RGPD (obligation de sécurité), elle relève l'absence de VPN et d'authentification multifacteur pour les utilisateurs externes, une politique d'habilitation qui ignorait la notion d'équipe de soins et l'absence de détection en temps réel d'une activité suspecte, alors que l'analyse post-incident citée par Caducée.net a retrouvé « environ douze heures de reconnaissance avec 665 requêtes » avant l'exfiltration. Selon le communiqué, l'hôpital n'avait pas mis en œuvre « certaines mesures élémentaires de sécurité qui auraient pu rendre l'attaque plus difficile ». Au titre de l'article 34, elle sanctionne l'absence d'information directe des 202 246 tiers de confiance. Le montant tient compte, toujours selon la CNIL, du nombre de personnes concernées, de la nature des données et des capacités financières de l'établissement. La délibération ajoute trois injonctions, dont celle de n'ouvrir l'accès de l'éditeur au DPI que sur autorisation préalable de l'hôpital, dans un délai de trois mois et sous astreinte de 1 000 euros par jour de retard, d'après Caducée.net et Mondaq.

Le mot « tiers » mérite d'être fixé dès maintenant, car la décision l'emploie dans un autre sens. Les « tiers de confiance » de la délibération sont les proches désignés par les patients. Le tiers dont traite cet article est l'éditeur du logiciel, acteur extérieur à la relation entre le régulateur et le responsable de traitement, qui dispose pourtant d'un accès direct aux données. Selon Next, le logiciel en cause est Expert Santé, que l'Agence du numérique en santé (ANS) référence sous la dénomination sociale de Berger-Levrault. La décision, précise Caducée.net, n'attribue l'intrusion ni à une faille du logiciel ni à son éditeur. Elle relève même que la version installée permettait déjà l'authentification multifacteur, l'établissement ayant préféré attendre la solution du groupe. Le cas ne relève donc pas d'une faute de l'éditeur. Il éclaire la position que l'éditeur occupe.

L'accès de l'éditeur n'est pas un détail technique mais une main de plus dans la chaîne

Le point le moins commenté de la délibération est aussi le plus structurel. Next rapporte que la rapporteure reprochait à l'hôpital d'avoir laissé à la société éditrice un accès permanent aux données des patients. L'hôpital invoquait le besoin d'un support rapide et efficace. L'autorité répond que cet accès permanent et sans contrôle « n'est pas nécessaire au regard de la mission d'assistance technique et de maintenance de la société éditrice du logiciel ». Elle ajoute que « les salariés de l'éditeur du logiciel auraient dû systématiquement solliciter l'autorisation préalable de l'hôpital ». Caducée.net précise que l'établissement faisait valoir le passage ultérieur par un serveur bastion (point d'accès unique et contrôlé), et que la CNIL a jugé que ce dispositif sécurise le chemin d'accès sans remplacer l'autorisation de l'établissement.

> **Un chiffre structurant**
>
> Selon Caducée.net, qui cite la délibération, environ 450 utilisateurs externes se connectaient au DPI par Internet avec un simple identifiant et un mot de passe. Parmi eux

> figuraient des praticiens libéraux, leurs secrétariats et certains salariés de l'éditeur. Environ 40 salariés disposant d'un accès distant passaient, eux, par un VPN. Les comptes de l'éditeur partageaient ainsi le canal le moins protégé du système.

Le fait empirique précède ici le mécanisme. L'intrusion de juin 2025 mobilise au moins six contributeurs distincts. Le médecin libéral dont les identifiants ont été compromis, l'établissement qui définit les habilitations, le groupe qui pilote le calendrier de l'authentification forte, l'éditeur qui conçoit le logiciel et y accède en permanence, le centre des opérations de sécurité (SOC) qui collecte des traces sans les analyser, et le président de la commission médicale d'établissement, chargé après l'attaque de retransmettre un mot de passe temporaire identique pour tous. Aucun de ces acteurs n'a provoqué seul la fuite. Chacun a contribué à la rendre possible ou plus grave.

> **Concept : le problème des mains multiples (Thompson, 1980)**
>
> Dennis F. Thompson, « Moral Responsibility of Public Officials: The Problem of Many Hands », *American Political Science Review*, vol. 74, n° 4, 1980, p. 905-916. Lorsque de nombreux agents contribuent de multiples façons aux décisions et aux politiques d'une organisation, il devient difficile, même en principe, d'identifier qui est responsable de leurs résultats. Thompson récuse les deux réponses commodes, la responsabilité purement collective et la responsabilité purement hiérarchique, qui bloquent selon lui l'enquête sur la contribution réelle de chacun. Dans un article de 2014, il propose d'y répondre par la conception des processus, en désignant des responsables de la surveillance de la structure elle-même.

Opérationnalisé sur le cas, le concept produit une observation précise. La chaîne de sous-traitance ne dilue pas la responsabilité juridique, qui reste entière sur le responsable de traitement. Elle dilue la responsabilité pratique, c'est-à-dire la capacité de chaque maillon à se représenter sa propre contribution au risque. L'éditeur assure une maintenance, l'hôpital assure des soins, le groupe assure une trajectoire de conformité. L'accès permanent est le point où ces trois logiques se rencontrent sans qu'aucune ne le possède. Le praticien observe que la télémaintenance ouverte en continu n'est presque jamais une décision explicite. Elle résulte d'un contrat de support, d'une habitude d'exploitation et d'une contrainte de délai, ce que Thompson décrit précisément comme le terrain où les excuses individuelles prospèrent.

La CNIL pratique une responsabilité d'organisation qui laisse le marché hors champ

Le droit applicable explique en partie ce choix. L'hôpital est responsable de traitement, il définit les finalités et les moyens essentiels du DPI, et la délibération le traite comme tel. L'injonction relative à l'éditeur est donc adressée à l'hôpital, qui doit mettre en place les mesures techniques empêchant tout accès non autorisé du prestataire. Aucune des sources consultées ne mentionne une qualification de l'éditeur comme sous-traitant au sens de

l'article 28 du RGPD, ni une procédure distincte le visant.

Mark Bovens, dans *The Quest for Responsibility: Accountability and Citizenship in Complex Organisations* (Cambridge University Press, 1998), donne le vocabulaire pour qualifier ce geste. Il distingue la responsabilité passive (rendre des comptes après coup) de la responsabilité active (se conduire de manière responsable au sein de l'organisation), et décompose la première en plusieurs modèles : la *responsabilité de l'organisation* traitée comme une personne, la responsabilité hiérarchique, la responsabilité collective et la responsabilité individuelle. Bovens défend la voie individuelle, à la condition que les individus aient effectivement la possibilité de se conduire de façon responsable. La sanction de la CNIL relève du premier modèle. Elle vise une personne morale et la contraint à réorganiser ses relations avec ses fournisseurs.

L'injonction prolonge d'ailleurs la piste de Thompson en 2014. Elle fait de l'hôpital le surveillant désigné de l'éditeur, chargé d'ouvrir et de refermer chaque accès. Le dispositif est cohérent avec le droit et loyal envers l'établissement, puisque la formation restreinte a aussi pris acte des mesures correctrices engagées en cours de procédure. Sa limite est ailleurs. Une injonction individuelle ne lie que son destinataire. Le même logiciel, maintenu par la même équipe, peut rester ouvert en permanence dans un autre établissement sans que la délibération SAN-2026-009 n'y change rien. Le groupe Elsan, par exemple, déclarait en 2024 selon CIO Online un déploiement d'Expert Santé sur 21 de ses établissements. Le régulateur traite au cas par cas une configuration qui se reproduit à l'échelle d'une base installée.

Le discours institutionnel comporte ici un non-dit, loyal mais vérifiable. Le communiqué de la CNIL du 3 septembre 2026 détaille l'authentification, les habilitations, la détection et l'information des personnes. Il ne mentionne pas l'accès permanent de l'éditeur, qui figure pourtant parmi les manquements et fonde l'une des trois injonctions. La communication publique, celle que lisent les directions d'établissement, reconduit ainsi le cadrage centré sur l'hôpital. La dimension de marché n'apparaît que dans le texte intégral, et dans la presse spécialisée qui l'a lu. L'article publié le 30 juin 2026 sur IQVIA concluait que la CNIL sanctionne les manquements, pas le modèle. Le cas stéphanois déplace la question. Le modèle en cause n'est pas celui d'une entreprise sanctionnée, mais l'architecture de maintenance d'un secteur entier, dont aucune partie n'est destinataire de la sanction.

Dedalus Biologie montre que l'autre voie existe déjà

Un précédent présente une proximité structurelle maximale avec le cas stéphanois. Le 23 février 2021, CheckNews (Libération) révèle, selon la délibération SAN-2022-009 citée par L'Informaticien, une fuite massive concernant 491 840 patients de 28 laboratoires de biologie médicale (Morbihan, Eure, Loire, Côtes-d'Armor, Loir-et-Cher), tous utilisateurs, selon INCYBER News, du logiciel Mega-Bus de Dedalus Biologie, éditeur de logiciels pour ces laboratoires. Les données comprenaient, selon la CNIL citée par L'Usine Digitale, des

informations médicales très sensibles relatives notamment au VIH, aux cancers, aux maladies génétiques, aux grossesses et aux traitements médicamenteux, ainsi que des données génétiques. Par la délibération SAN-2022-009 du 15 avril 2022, publiée le 21 avril, la formation restreinte inflige à l'éditeur une amende de 1,5 million d'euros.

La comparaison est instructive parce que la configuration est la même et la voie juridique opposée. Dans l'affaire Dedalus, la CNIL qualifie l'éditeur de sous-traitant et le sanctionne directement sur trois fondements, selon le résumé publié par le Comité européen de la protection des données. Lors d'une migration logicielle demandée par deux laboratoires, l'éditeur avait extrait un volume de données supérieur à celui requis, en méconnaissance des instructions du responsable de traitement (article 29 du RGPD). Ses conditions générales de vente et ses contrats de maintenance ne contenaient pas les mentions de l'article 28, paragraphe 3. Ses mesures de sécurité étaient insuffisantes (article 32). La formation restreinte écarte l'argument selon lequel les laboratoires portaient aussi la responsabilité de l'encadrement contractuel, en jugeant que cette obligation partagée est sans incidence sur une responsabilité propre du sous-traitant.

Le parallèle montre que le régulateur dispose déjà d'un outil pour atteindre l'éditeur lorsque son intervention sort de ses instructions. Il montre aussi pourquoi cet outil reste exceptionnel. Dans l'affaire Dedalus, la faute de l'éditeur était active et documentée (une extraction excessive). Dans l'affaire stéphanoise, l'accès permanent est une faculté accordée par le client, non un acte de l'éditeur. La responsabilité retombe alors mécaniquement sur celui qui a ouvert la porte. Le problème des mains multiples se loge exactement dans cet écart. Une même position de marché donne lieu à une sanction du prestataire quand il agit, et à une sanction du client quand il laisse faire. Le marché de la biologie ajoutait une donnée de concentration que l'étude de marché 2023 du GIE SESAM-Vitale permet de mesurer, puisque Dedalus France y détient plus de 80 % des laboratoires équipés. Plus la base installée d'un éditeur est large, plus le choix entre ces deux voies cesse d'être une affaire individuelle. D'autres décisions récentes, comme la sanction de 5 millions d'euros prononcée contre France Travail le 22 janvier 2026 au titre de l'article 32, confirment que la CNIL concentre ses sanctions de sécurité sur le responsable de traitement.

Dans les GHT, la convergence transforme un accès éditeur en accès territorial

L'Hôpital privé de la Loire est un établissement privé, mais le mécanisme ne s'arrête pas à la frontière entre les deux secteurs. L'article 107 de la loi n° 2016-41 du 26 janvier 2016 confie à l'établissement support de chaque GHT « la stratégie, l'optimisation et la gestion commune d'un système d'information hospitalier convergent, en particulier la mise en place d'un dossier patient ». La Cour des comptes, dans un rapport d'octobre 2020 cité par APMnews, jugeait cette convergence « inaboutie » et relevait que seuls 45 % des GHT allaient déployer une solution de DPI unique. Le raisonnement suivant est une inférence de l'article, non une constatation d'un rapport public. Là où la convergence aboutit, un DPI unique couvre

plusieurs établissements, et l'accès de maintenance de son éditeur devient un accès au territoire de santé entier. La politique publique qui réduit l'hétérogénéité des SI concentre du même coup le point d'entrée tiers.

> **Le plan d'action CaRE (décembre 2023)**
>
> « Le nombre important de fournisseurs nécessitant des liens avec les solutions déployées au sein des établissements de santé (plusieurs dizaines pour certains établissements de santé) induit un risque important d'intrusions d'attaquants via ces « portes ouvertes ». » Le programme fixe l'ambition de « portes sécurisées, maitrisées et exploitées » pour ces liens.

Les pouvoirs publics ont donc nommé le risque. Le plan d'action du programme CaRE (Cybersécurité accélération et résilience des établissements), publié par la Délégation au numérique en santé et l'ANS, consacre son objectif 15 à la sécurisation des accès externes, télémaintenance comprise. En décembre 2023, ses actions et indicateurs étaient encore annoncés comme en cours de co-construction. Le même plan prévoit, à son objectif 20, d'intégrer progressivement des exigences de cybersécurité dans les référentiels sectoriels applicables aux solutions, dont les DPI référencés au titre du Ségur. C'est la seule voie qui atteint le produit plutôt que l'établissement.

L'observatoire 2025 du CERT Santé confirme que la question n'est pas théorique. Sur 764 incidents déclarés en 2025, le rapport constate pour les fuites de données que « l'immense majorité des incidents de ce type constatés par le CERT Santé avaient pour origine la compromission du compte d'un professionnel de santé ou d'un prestataire ». Il classe dans une catégorie distincte les compromissions de comptes applicatifs ou de maintenance, qui représentent 25 % des compromissions du SI. Il indique aussi que l'ANS est intervenue en 2025 auprès de 9 prestataires de solutions métier pour des vulnérabilités exposées sur Internet. Le cadre européen pourrait fournir le levier manquant. Selon Solutions Numériques, la commission spéciale de l'Assemblée nationale a adopté le 10 septembre 2025, après l'adoption du texte par le Sénat le 12 mars 2025, une version du projet de loi Résilience qui soumet les éditeurs de logiciels aux obligations de la directive NIS2, aux côtés des établissements de santé classés entités essentielles. Selon Neova, qui cite le dossier législatif de l'Assemblée nationale, le texte n'avait toujours pas été inscrit à l'ordre du jour de l'Assemblée au 16 septembre 2026, malgré la saisine de la Cour de justice de l'Union européenne par la Commission européenne le 8 juillet 2026. Le levier reste donc à l'état de projet.

Ce que la clôture de l'injonction dira de la régulation par cas

Le titre posait l'éditeur du DPI en tiers non jugé. Le cas de l'Hôpital privé de la Loire montre que ce statut n'est ni une omission ni une faveur. Il résulte d'un droit qui attribue la responsabilité au responsable de traitement et d'un régulateur qui, faute de qualification de

sous-traitant fautif, agit par l'organisation qu'il peut atteindre. Le *problème des mains multiples* ne se résout pas en désignant un coupable supplémentaire. Il se déplace selon l'endroit où le régulateur choisit de fixer la surveillance. En faisant de chaque hôpital le gardien de la porte de son éditeur, la CNIL fixe cette surveillance au niveau le plus fragmenté du marché, au moment même où la convergence des GHT la concentre.

L'hypothèse de l'article est la suivante. D'ici au 30 septembre 2027, la règle de l'autorisation préalable de l'accès éditeur restera une obligation individuelle issue d'une injonction, sans traduction dans un référentiel opposable aux produits. Elle se vérifie par deux indicateurs observables. Le premier est la publication sur cnil.fr d'une délibération de clôture de l'injonction prononcée contre l'Hôpital privé de la Loire, sur le modèle des clôtures déjà publiées pour Orange ou Solocal, et la question de savoir si son motif mentionne une modification du logiciel ou seulement de la configuration locale. Le second est la présence ou l'absence, dans un référentiel sectoriel publié par l'ANS (référencement Ségur des DPI ou corpus de la PGSSI-S), d'une exigence explicite subordonnant l'accès de télémaintenance de l'éditeur à une autorisation préalable de l'établissement. L'hypothèse est réfutée si une telle clause apparaît avant cette date, ou si la CNIL sanctionne directement un éditeur de DPI pour un accès non autorisé. Dans les deux cas, la régulation aurait cessé de traiter une propriété du marché comme une somme de cas.

Note méthodologique

Sources principales : communiqué CNIL du 3 septembre 2026, résumés EDPB, plan CaRE et observatoire CERT Santé 2025, complétés par Next et Caducée.net pour le contenu de la délibération SAN-2026-009, dont le texte intégral sur Légifrance n'a pu être consulté directement. Les citations de la délibération sont donc reproduites telles que Next les rapporte, et le nom d'Expert Santé (Berger-Levrault) repose sur Next et le référencement ANS, sa présence dans la version publique restant à vérifier. L'auteur a retenu le cadre de Thompson et Bovens proposé dans le brief, après vérification des titres et des thèses, et a écarté la piste NIS2 comme angle dominant faute de texte adopté. Recherche de sources, croisement des données et structuration du raisonnement s'appuient sur une assistance par intelligence artificielle. Le choix de l'angle et du cadre théorique, la vérification des sources, les arbitrages et l'établissement du texte final relèvent de l'auteur.

Sources

Sources primaires institutionnelles

- CNIL, « Violation de données en matière de santé : sanction de 500 000 euros à l'encontre de l'HÔPITAL PRIVÉ DE LA LOIRE », 3 septembre 2026. https://www.cnil.fr/fr/sanction-hopital-prive-loire
- CNIL, formation restreinte, Délibération n° SAN-2026-009 du 21 juillet 2026 concernant la

société HOPITAL PRIVE DE LA LOIRE, publiée le 3 septembre 2026. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000054790100 (lien relevé sur le communiqué CNIL, texte intégral)

- CNIL, page « Sanctions ». https://www.cnil.fr/fr/thematique/cnil/sanctions
- Comité européen de la protection des données, « Health data breach: the CNIL fined Hôpital Privé de la Loire 500 000 EUR », 9 septembre 2026. https://www.edpb.europa.eu/news/health-data-breach-the-cnil-fined-hopital-prive-de-la-loire-500-000-eur_en
- Comité européen de la protection des données, « Health data breach: Dedalus Biologie fined 1.5 million euros », 4 mai 2022 (, la page n'ayant pu être rechargée)
- CNIL, formation restreinte, Délibération n° SAN-2022-009 du 15 avril 2022 concernant la société DEDALUS BIOLOGIE
- Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, article 107. https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000031913559
- Agence du numérique en santé, fiche de référencement « EXPERT SANTE - 2022.03 », éditeur BERGER-LEVRAULT. https://esante.gouv.fr/node/7733

Rapports officiels

- Délégation au numérique en santé et Agence du numérique en santé, « Le plan d'action pour protéger nos établissements face à la menace cyber. Programme CaRE », décembre 2023. https://esante.gouv.fr/sites/default/files/media_entity/documents/doc-programme-care-231214-20h_pap%5B17%5D.pdf
- Agence du numérique en santé et CERT Santé, « Observatoire des signalements d'incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social. Rapport public 2025 », mai 2026. https://esante.gouv.fr/sites/default/files/media/document/ANS_CERTSante_Rapport_Public_Observatoire_Signalements_ISSIS_2025_VF_0.pdf
- Cour des comptes, rapport sur les groupements hospitaliers de territoire, octobre 2020, cité par APMnews le 8 octobre 2020. https://www.apmintelligence.com/deps_libre?id=152
- GIE SESAM-Vitale, « Étude de marché 2023 des entreprises du numérique en santé ». https://www.sesam-vitale.fr/documents/d/sesam-vitale/etude_de_marche_2023_des_entreprises_du_numerique_en_sante
- Sénat, rapport sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. https://www.senat.fr/rap/l24-393/l24-39314.html

Cadres théoriques

- Dennis F. Thompson, « Moral Responsibility of Public Officials: The Problem of Many Hands », *American Political Science Review*, vol. 74, n° 4, décembre 1980, p. 905-916. https://dft.scholars.harvard.edu/publications/moral-responsibility-public-officials-problem-

many-hands

- Dennis F. Thompson, « Responsibility for Failures of Government: The Problem of Many Hands », *The American Review of Public Administration*, vol. 44, n° 3, 2014, p. 259-273. https://journals.sagepub.com/doi/abs/10.1177/0275074014524013
- Mark Bovens, *The Quest for Responsibility: Accountability and Citizenship in Complex Organisations*, Cambridge University Press, 1998. https://www.cambridge.org/us/universitypress/subjects/politics-international-relations/political-theory/quest-responsibility-accountability-and-citizenship-complex-organisations

Parallèles historiques

- Haas Avocats, « Fuite de données de santé : la CNIL sanctionne le sous-traitant Dedalus », 22 avril 2022. https://www.haas-avocats.com/reglementation/cnil/fuite-de-donnees-de-sante-la-cnil-sanctionne-le-sous-traitant-dedalus/
- Ubiquity Avocats, « DEDALUS BIOLOGIE : sanction CNIL de 1,5 millions d'euros », 23 mai 2022. http://ubiquity-avocats.com/dedalus-biologie-sanction-cnil-de-15-millions-deuros-pour-manquements-au-rgpd-ayant-cause-une-fuite-de-donnees-de-sante-concernant-pres-de-500-000-patients/
- INCYBER News, L'Informaticien et L'Usine Digitale, couverture de l'affaire Dedalus Biologie et de la délibération SAN-2022-009, 2021-2022
- William Laurent, « Obligation de sécurité et responsabilité du responsable de traitement : la CNIL sanctionne lourdement France Travail », 2026. https://consultation.avocat.fr/blog/william-laurent/article-2979116-obligation-de-securite-et-responsabilite-du-responsable-de-traitement-la-cnil-sanctionne-lourdement-france-travail.html

Presse spécialisée

- Martin Clavey, « L'Hôpital privé de Loire sanctionné pour absence de « mesures élémentaires de sécurité » », Next, 3 septembre 2026. https://next.ink/254472/lhopital-prive-de-loire-sanctionne-pour-absence-de-mesures-elementaires-de-securite/
- Caducée.net, « DPI piraté : 500 000 € d'amende CNIL, MFA, habilitations et journalisation en cause », 21 septembre 2026. https://www.caducee.net/actualite-medicale/16977/dpi-pirate-500-000-d-amende-cnil-mfa-habilitations-et-journalisation-en-cause.html
- Mondaq, « L'Hôpital privé de la Loire sanctionné lourdement par la CNIL », septembre 2026. https://www.mondaq.com/france/data-protection/1845488/
- DSIH, « La CNIL n'épargne plus les établissements de santé ! », 2026. https://dsih.fr/articles/6399/la-cnil-nepargne-plus-les-etablissements-de-sante
- CIO Online, « Les cliniques privées Elsan se tournent vers une gestion hospitalière intégrée ». https://www.cio-online.com/actualites/lire-les-cliniques-privees-elsan-se-tournent-vers-une-gestion-hospitaliere-integree-15861.html

- Solutions Numériques, « Le projet de loi NIS2 et DORA est adopté à l'unanimité en commission spéciale », septembre 2025. https://www.solutions-numeriques.com/le-projet-de-loi-nis2-et-dora-est-adopte-a-lunanimite-en-commission-speciale/
- IT Social, « La transposition de NIS2 attendra au plus tôt la rentrée parlementaire de septembre », juillet 2026. https://itsocial.fr/cybersecurite/cybersecurite-actualites/la-transposition-de-nis2-attendra-au-plus-tot-la-rentree-parlementaire-de-septembre/
- Neova, « NIS2 collectivités 2026 : agir avant la loi Résilience », 27 septembre 2026. https://www.neova.tech/blog/nis2-collectivites-2026-loi-resilience-mise-en-conformite