

Veille Réglementaire et Technologique, Novembre 2025

Date : 2 décembre 2025

Sujet: Analyse de novembre 2025 , La convergence des seuils de conformité et de la consolidation du marché

Résumé

Novembre 2025 marque un tournant décisif pour l'industrie des dispositifs médicaux, caractérisé par la convergence d'échéances réglementaires strictes et d'une restructuration majeure du marché. Tandis que le secteur privé réalisait plus de 30 milliards de dollars d'opérations de fusions-acquisitions stratégiques pour sécuriser les écosystèmes de données de diagnostic, les autorités réglementaires américaines et européennes ont renforcé leurs contrôles sur les systèmes de qualité et la sécurité biologique.

La dynamique déterminante est la « convergence opérationnelle ». L'entrée en vigueur, dans moins de 90 jours, du règlement de la FDA relatif aux systèmes de management de la qualité (QMSR) impose de passer d'une « analyse des écarts » à une « preuve de mise en œuvre ». En Europe, la Commission européenne a officiellement déclaré EUDAMED fonctionnel, lançant ainsi le compte à rebours final avant son utilisation obligatoire, tandis que la Juridiction unifiée du brevet (JUB) a immédiatement exposé les dispositifs portant le marquage CE à des risques juridiques. Par ailleurs, la publication de la norme ISO 10993-1:2025 redéfinit en profondeur les critères de biocompatibilité, faisant passer des tests basés sur une liste de contrôle à une évaluation des risques. Ce rapport synthétise ces mécanismes réglementaires complexes et les évolutions plus larges du marché afin de fournir une vision claire et fiable du contexte.

Résumé exécutif	1
Le noyau réglementaire (MDR et QMSR)	3
FDA QMSR : Le pivot de la responsabilité de gestion	3
EU MDR : EUDAMED et boucles de données cliniques	3
Le paysage normatif (ISO 10993-1:2025)	4
Biocompatibilité : des « tests » à « l'évaluation »	4
La frontière numérique (IA et cybersécurité)	4
Loi européenne sur l'IA : une réalité à haut risque	4
Cybersécurité et systèmes d'exploitation hérités	5
Veille concurrentielle et innovation	5
Fusions et acquisitions stratégiques : la course à la liquidité des données	5
Signaux d'innovation	6
Focus sur les technologies émergentes	6
Interfaces cerveau-ordinateur (ICO) : Le tournant vers les essais pivots	6
Risques juridiques et stratégiques	7
Le « piège à brevets » de l'UPC	7
Mesures exécutives : Priorités intégrées	8
Union européenne (Priorité : Stratégique)	8
États-Unis (Priorité : Opérationnelle)	8
Annexe A : Plan de transition complet pour la fin de vie de Windows 10 pour les dispositifs médicaux	9
1. Résumé : Le moment critique est arrivé	9
2. Exposition réglementaire et de sécurité (situation en novembre 2025)	9
A. Le déficit de vulnérabilité (violation des normes ISO 27001/27002)	9
B. La position réglementaire	9
C. L'intersection de l'IA (dispositifs à haut risque)	10
3. Le plan de transition immédiat : « Contenir et migrer »	10
Phase 1 : Durcissement immédiat (L'état « sans état »)	10
Phase 2 : Isolation du réseau	10
Annexe B : Mise en œuvre technique (script PowerShell)	11
Annexe C : Projet de communication à la clientèle (Avis de sécurité sur le terrain)	13
1. Résumé : Action immédiate requise	13
2. Justification réglementaire et de sécurité	13
3. La solution imposée : le fonctionnement « sans état ».	13
4. Configuration réseau requise	13
5. Plan de mise en œuvre	14

Le noyau réglementaire (MDR et QMSR)

FDA QMSR : Le pivot de la responsabilité de gestion

L'entrée en vigueur de la mesure, prévue le 2 février 2026, étant imminente, la FDA se concentre désormais sur la responsabilité de la direction. Des informations parues en novembre confirment que les enquêteurs examineront attentivement les liens entre l'examen mené par la haute direction et la gestion des risques.

- **Risque d'audit:** Conformément au règlement relatif aux systèmes de management de la qualité (QMSR) (harmonisé avec la norme ISO 13485:2016), les revues de direction doivent examiner explicitement la pertinence, l'adéquation et l'efficacité du système de management de la qualité. Contrairement à l'ancien système QSR, le nouveau régime exige que les processus de gestion des risques ne soient pas des activités de conception isolées, mais qu'ils interviennent « tout au long de la réalisation du produit »..
- **Preuve requise :** Les dirigeants doivent démontrer que les décisions d'allocation des ressources examinées lors des réunions de direction sont directement liées à l'« amélioration ». du système de gestion de la qualité et du produit lié aux exigences du client. Les fichiers de risques statiques qui n'alimentent pas dynamiquement les actions correctives et préventives (CAPA) et les revues de direction sont désormais considérés comme des cibles à haut risque..

EU MDR : EUDAMED et boucles de données cliniques

Le contexte européen s'est durci. Le 27 novembre 2025, la Commission européenne a déclaré les quatre premiers modules d'EUDAMED fonctionnels, fixant ainsi la date limite d'utilisation obligatoire au 28 mai 2026. La phase « volontaire » touche à sa fin.

- **Points de blocage liés à la documentation technique :** Les organismes notifiés (ON) appliquent des exigences strictes en matière de documentation technique. Le plan de suivi clinique post-commercialisation (PMCF) ne doit pas être statique ; il doit faire l'objet d'une mise à jour régulière du rapport d'évaluation clinique (CER). Les examinateurs rejettent les dossiers pour lesquels l'interface entre la gestion des risques et l'évaluation clinique n'est pas clairement reflétée dans la liste de contrôle « Exigences générales de sécurité et de performance »..

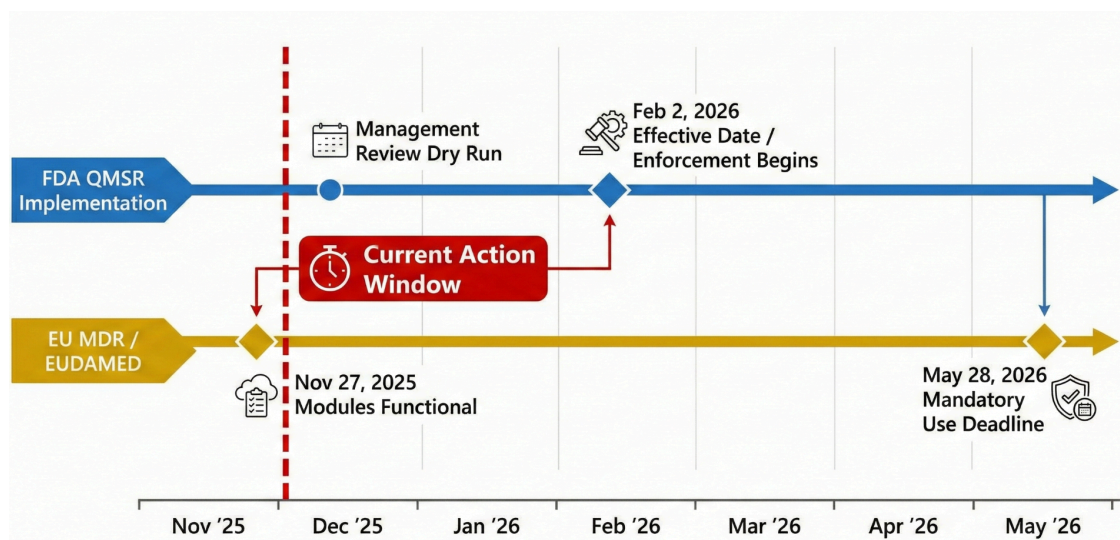


Figure 1: Échéances réglementaires (novembre 2025 - mai 2026)

Le paysage normatif (ISO 10993-1:2025)

Biocompatibilité : des « tests » à « l'évaluation »

La publication de la norme ISO 10993-1:2025 (*Évaluation biologique des dispositifs médicaux*) représente un changement de paradigme. Elle abandonne la mentalité de la « liste de contrôle » au profit d'une approche rigoureuse de la gestion des risques.

- **La justification plutôt que les tests :** Les fabricants ne peuvent plus se contenter d'effectuer des tests basés sur la durée de contact. Les exigences de documentation technique du règlement MDR exigent désormais explicitement une « justification du choix et/ou de la dispense des tests de biocompatibilité ». La nouvelle norme renforce cette exigence en imposant un « plan d'évaluation biologique » (PEB) qui privilégie la caractérisation chimique par rapport aux tests sur les animaux.
- **Évaluation à vie:** Les évaluations doivent désormais démontrer la biocompatibilité « à la fin de la durée de conservation et pendant toute la durée de vie » du dispositif. Cela oblige les fabricants à prendre en compte la dégradation des matériaux et les « utilisations abusives raisonnablement prévisibles » dans leurs évaluations des risques biologiques, conformément aux exigences générales de sécurité.

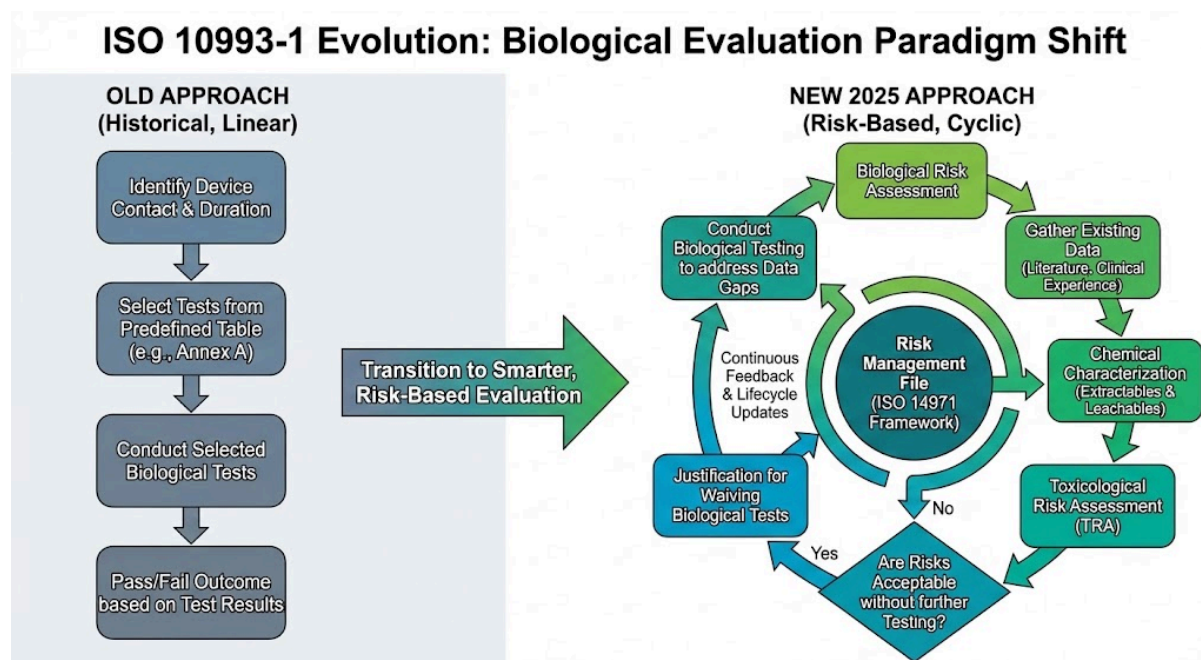


Figure 2:Diagramme d'évolution ISO 10993-1

La frontière numérique (IA et cybersécurité)

Loi européenne sur l'IA : une réalité à haut risque

La loi européenne sur l'IA est désormais applicable aux pratiques interdites, et des obligations à haut risque se profilent à l'horizon.

- **Classification:** Les dispositifs où l'IA est un « composant de sécurité » ou est couverte par la législation d'harmonisation de l'Union (comme le règlement MDR) sont classés comme systèmes d'IA à haut risque..
- **Le mandat d'exploitation forestière** Une exigence essentielle est l'article 12, qui stipule que les systèmes d'IA à haut risque « permettent techniquement l'enregistrement automatique des événements (journaux) ». Ces journaux doivent identifier les situations susceptibles d'engendrer un risque pour le système. Ainsi, les journaux système d'un service informatique deviennent des documents réglementaires soumis à audit..

Cybersécurité et systèmes d'exploitation hérités

Avec la fin du support de Windows 10, les autorités réglementaires émettent des alertes de sécurité. Conformément au règlement MDR, les fabricants doivent fournir une « vérification et une validation du logiciel, incluant des informations sur toutes les configurations matérielles et, le cas échéant, les systèmes d'exploitation ». Le 24 novembre, l'agence australienne TGA a publié une alerte de sécurité spécifique concernant Windows 10, classant le recours à un système d'exploitation non pris en charge comme un manquement aux principes essentiels.

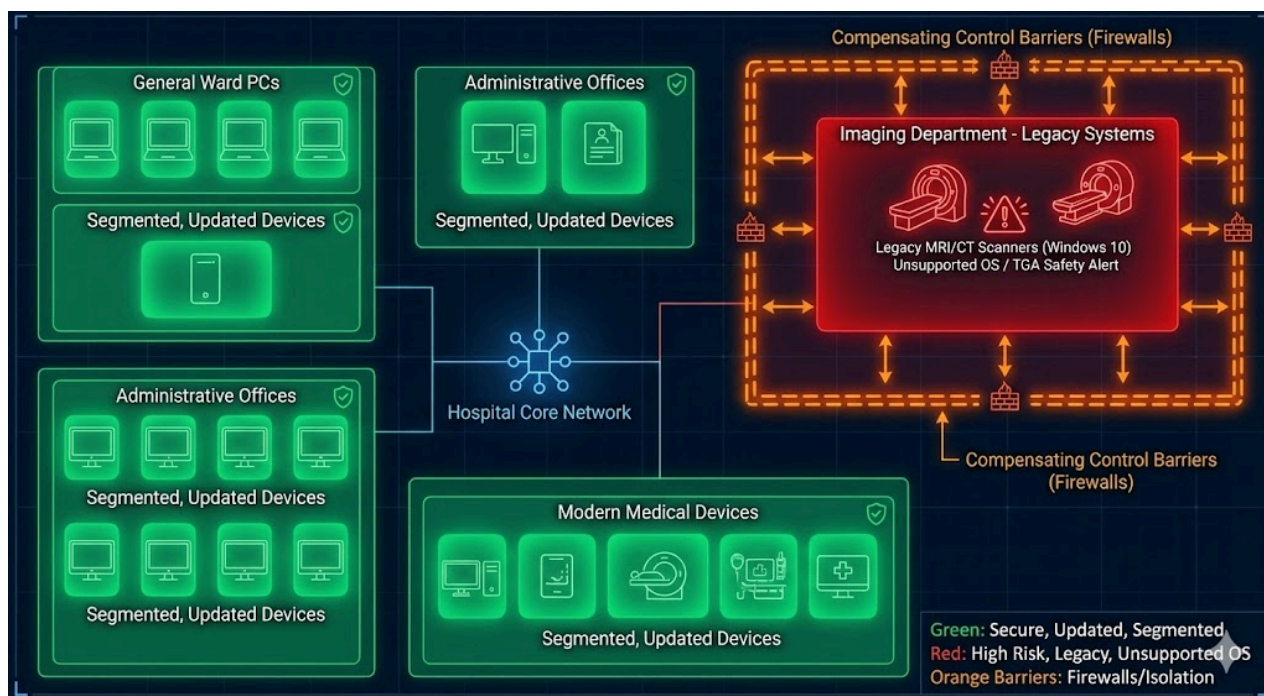


Figure 3: Carte thermique de la surface de risque de cybersécurité

Veille concurrentielle et innovation

Fusions et acquisitions stratégiques : la course à la liquidité des données

En novembre 2025, plus de 30 milliards de dollars ont été enregistrés dans le cadre de transactions, ce qui indique que la valeur migre des matériels autonomes vers des écosystèmes de diagnostic intégrés.

- Abbott et Exact Sciences (21 milliards de dollars) : Abbott a annoncé un accord définitif pour acquérir Exact Sciences, une initiative stratégique dans le domaine du diagnostic moléculaire et du dépistage du cancer afin de dominer la chaîne de valeur des soins « préventifs ».
- GE HealthCare et Intelrad (2,3 milliards de dollars) : GE a entrepris l'acquisition d'Intelrad pour renforcer ses capacités d'imagerie dans le cloud, ciblant spécifiquement le marché ambulatoire où la liquidité des données est essentielle.
- Thermo Fisher et Clario (8,9 milliards de dollars) : Thermo Fisher est entré dans le secteur des essais cliniques numériques en acquérant Clario, dans le but d'intégrer directement les données cliniques pilotées par l'IA dans les flux de travail de recherche.

Signaux d'innovation

Les procédures réglementaires s'accroissent pour les technologies à fort impact.

- Nanopath : Obtention de la désignation de dispositif révolutionnaire de la FDA le 19 novembre pour sa plateforme de biodétection à l'état solide, capable de détecter les infections des voies urinaires en 15 minutes.

- EDAP : A reçu l'autorisation 510(k) de la FDA le 20 novembre pour son système HIFU robotisé Focal One mis à jour, soulignant la confiance du régulateur dans la précision robotique en oncologie.

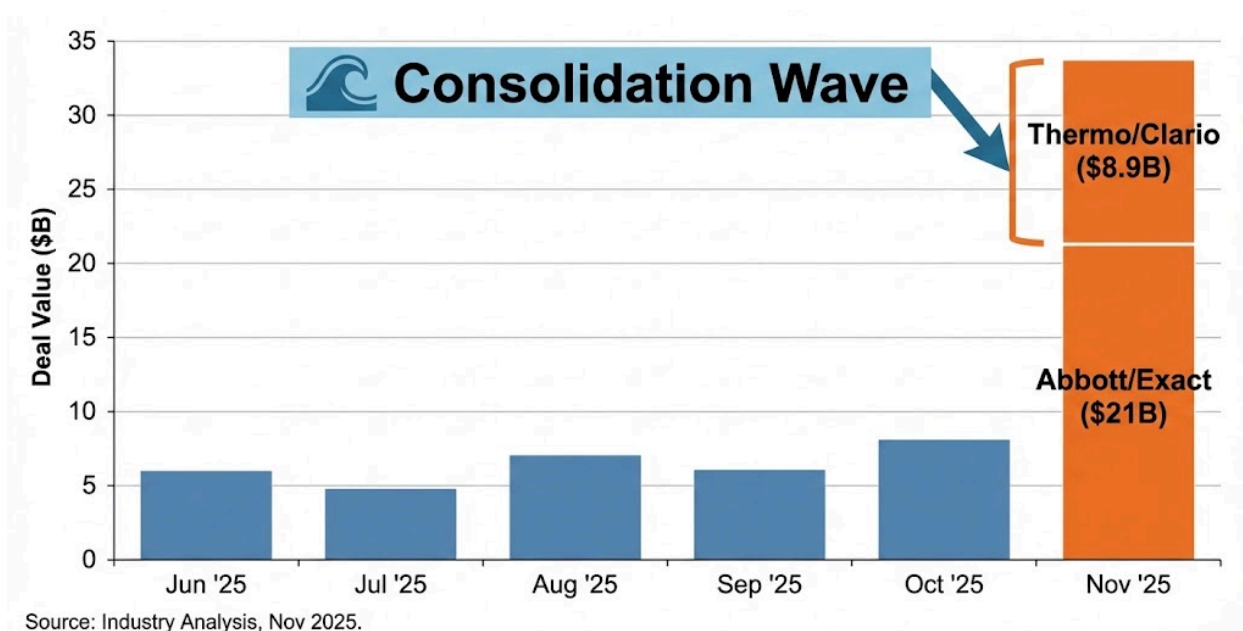


Figure 4 : Volume des opérations de fusions-acquisitions dans le secteur des technologies médicales - novembre 2025

Focus sur les technologies émergentes

Interfaces cerveau-ordinateur (ICO) : Le tournant vers les essais pivots

Novembre 2025 a marqué la transition des interfaces cerveau-machine (ICM) du stade « expérimental » au stade « pré-commercialisation ». Des acteurs comme Paradromics et Synchron progressent vers des essais pivots pour les implants actifs de classe III.

- **Défi réglementaire :** Ces dispositifs font l'objet d'un examen rigoureux concernant leur stabilité à long terme. La documentation technique doit décrire les éléments fonctionnels clés et les matières premières utilisées, y compris les informations relatives aux revêtements, afin de prouver leur innocuité neurologique sur plusieurs années d'implantation..
- **Stratégie clinique** Le plan d'évaluation clinique de ces dispositifs est complexe. Les fabricants doivent justifier rigoureusement les allégations d'équivalence ou, plus probablement, fournir des données d'investigation clinique directes compte tenu des caractéristiques novatrices. La consultation de comités d'experts pour les implants de classe III est désormais une étape cruciale..

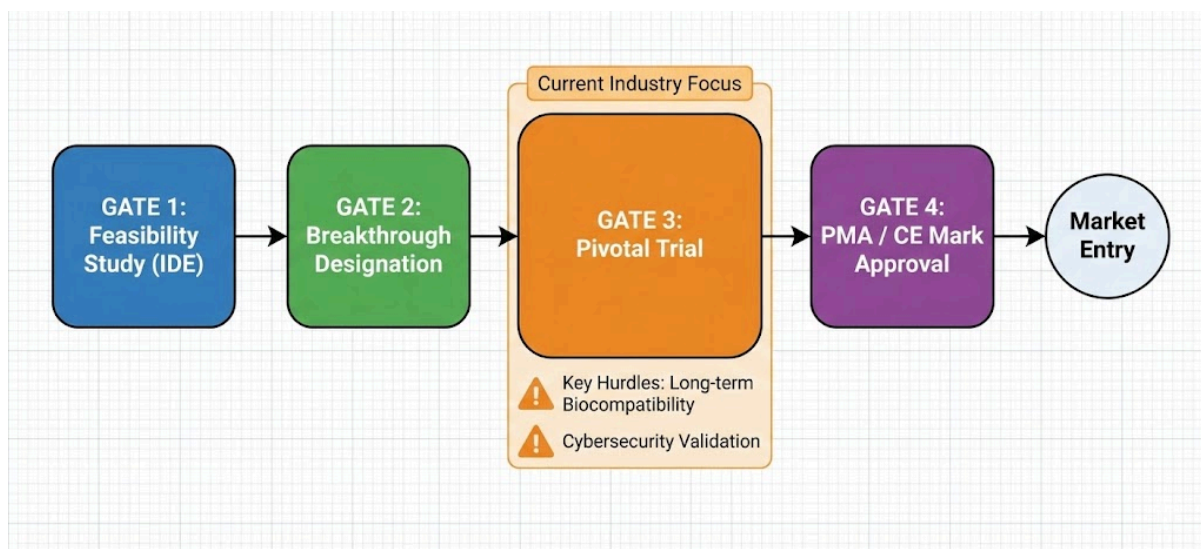


Figure 5: Diagramme du parcours clinique BCI

Risques juridiques et stratégiques

Le « piège à brevets » de l'UPC

Un précédent juridique majeur a été établi ce mois-ci par la Juridiction unifiée des brevets (JUB). La cour a statué que l'obtention et la publication du marquage CE peuvent constituer une preuve de « contrefaçon imminente », permettant ainsi aux titulaires de brevets de demander des injonctions avant la commercialisation d'un produit.

- **Implication stratégique :** La « Déclaration de conformité » Il s'agit désormais d'un signal public susceptible de déclencher un litige. Les équipes juridiques et réglementaires doivent se coordonner afin de garantir la conclusion de l'analyse de la « liberté d'exploitation ». avant que la déclaration de conformité soit signée et le dispositif enregistré dans EUDAMED.

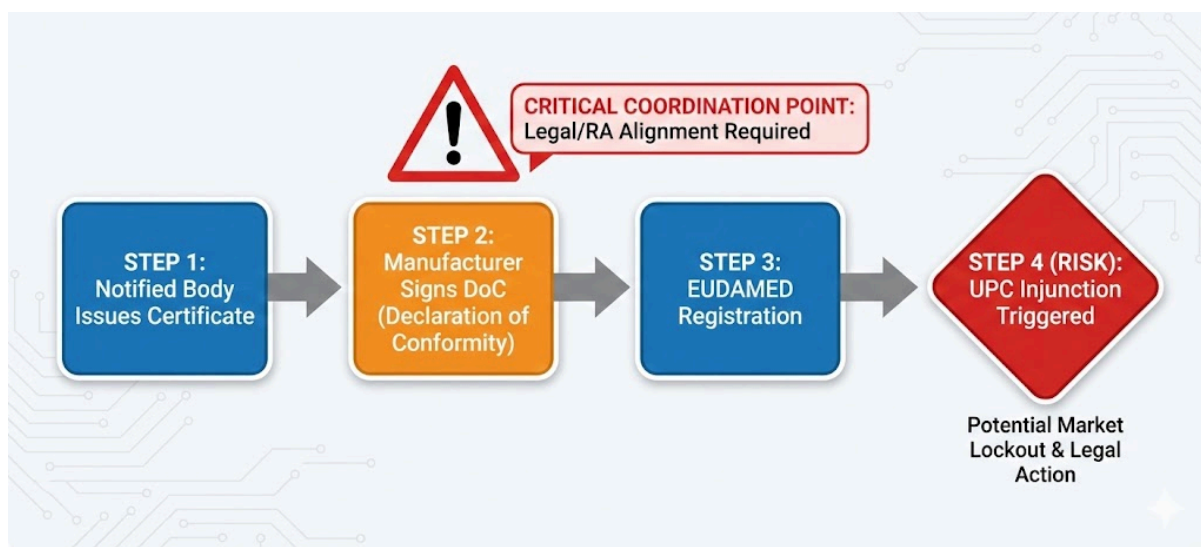


Figure 6 : Flux de travail relatif aux risques liés aux « pièges à brevets »

Mesures exécutives : Priorités intégrées



Union européenne (Priorité : Stratégique)

1. Évaluation des écarts selon la norme ISO 10993-1 : Réaliser une analyse des écarts pour tous les rapports d'évaluation biologique. S'assurer que la justification du choix et/ou de l'exemption des essais est explicitement documentée afin de répondre à l'approche fondée sur les risques de la nouvelle norme de 2025..
2. EUDAMED Sprint : Les modules étant fonctionnels depuis le 27 novembre, veuillez vérifier vos données « UDI-DI de base » par rapport à la « Liste des produits et application ». Toute divergence entraînera un blocage de l'accès au marché en mai 2026.
3. Synchronisation PI/Réglementation : Mettre en œuvre une étape obligatoire de « validation juridique » avant la signature de toute nouvelle déclaration de conformité UE afin d'éviter une exposition prématurée à des litiges en matière de brevets en vertu des nouvelles règles de la Juridiction unifiée des brevets (JUB).



États-Unis (Priorité : Opérationnelle)

1. Revue de gestion QMSR : Dans votre revue de décembre, documentez explicitement l'analyse de « l'amélioration du produit liée aux exigences des clients ». Cette formulation précise est une exigence du QMSR que les inspecteurs de la FDA recherchent.
2. Intégration de la gestion des risques : Auditez les validations de vos processus de fabrication. Assurez-vous que, si un processus ne peut être entièrement vérifié, les enregistrements de validation démontrent que les méthodes de surveillance et de contrôle sont documentées., avec un lien direct vers le fichier de gestion des risques.
3. Fin de vie en matière de cybersécurité : Pour les appareils exécutant Windows 10, mettez à jour la documentation technique afin d'inclure une « Évaluation des risques de cybersécurité » spécifique pour le système d'exploitation non pris en charge, détaillant les mesures de contrôle compensatoires (par exemple, l'isolation du réseau) dans le cadre des « Exigences générales de sécurité et de performance »..

Annexe A : Plan de transition complet : Fin de vie de Windows 10 pour les dispositifs médicaux

1. Résumé : Le moment critique est arrivé

À compter du 14 octobre 2025, Microsoft a mis fin au support de Windows **10 Famille et Professionnel**. Pour les fabricants de dispositifs médicaux (MDM) et les organismes de prestation de soins de santé (HDO), les dispositifs fonctionnant avec ces systèmes d'exploitation sont désormais techniquement obsolètes.

Cette obsolescence a une incidence sur la conformité aux exigences de « l'état de l'art » prévues par le règlement européen relatif aux dispositifs médicaux (MDR) et engendre des responsabilités spécifiques concernant loi européenne sur l'IA. Pour les appareils intégrant des composants d'IA, l'article 15 de la loi sur l'IA exige que les systèmes d'IA à haut risque soient résilients face aux tentatives de tiers non autorisés d'en altérer l'utilisation, les résultats ou les performances en exploitant les vulnérabilités du système. Un système d'exploitation non mis à jour constitue une vulnérabilité critique.

L'urgence de votre situation dépend entièrement de la version de Windows 10 que vous utilisez. Microsoft les divise en **Disponibilité générale (GA)** et **Canal de maintenance à long terme (LTSC)**.

- **Windows 10 Famille/Professionnel/Entreprise (Général)** : Fin du support 14 octobre 2025 Si vos appareils utilisent cette technologie, vous vous trouvez dans une période critique.
- **Windows 10 IoT Entreprise LTSC** : Il s'agit de la norme industrielle pour les dispositifs médicaux.
 - **LTSC 2015** : Se termine le 14 octobre 2025.
 - **LTSC 2016** : Se termine le 13 octobre 2026.
 - **LTSC 2019** : Se termine le 9 janvier 2029.
 - **LTSC 2021** : Se termine le 13 janvier 2032.

2. Exposition réglementaire et de sécurité (situation en novembre 2025)

A. Le déficit de vulnérabilité (violation des normes ISO 27001/27002)

Sous **ISO/IEC 27002:2022 Contrôle 8.8 (Gestion des vulnérabilités techniques)** Les organisations sont tenues d'obtenir des informations sur les vulnérabilités techniques des systèmes d'information utilisés, d'évaluer leur exposition et de prendre les mesures appropriées.

- **Statut**: Depuis le 14 octobre, le fournisseur (Microsoft) ne signale plus les vulnérabilités de Windows 10 GA et ne les corrige plus.
- **Impact**: Les fabricants ne sont plus en mesure de satisfaire à l'exigence d'évaluer efficacement l'exposition ni d'appliquer les mesures correctives fournies par le fournisseur.

B. La position réglementaire

En vertu du règlement (UE) 2017/745 relatif aux dispositifs médicaux (MDR), et plus particulièrement **Annexe I, Exigences générales de sécurité et de performance (EGSP)**:

- **GSPR 17.2** : Vous devrez développer des logiciels conformément aux normes en vigueur. **"État de l'art"** (BAS).
- **GSPR 17.4** : Vous devez gérer le risque d'accès non autorisé.

L'avis du vérificateur : Les organismes notifiés (par exemple, TÜV, BSI) interprètent généralement l'expression « état de l'art » comme désignant un système d'exploitation pris en charge. Si votre système d'exploitation est obsolète, vous n'êtes pas, à proprement parler, conforme à la norme GSPR 17.2, sauf si vous avez mis en place des mesures d'atténuation massives et infaillibles (ce qui est rare).

L'intersection de l'IA (dispositifs à haut risque)

Pour les dispositifs classés comme systèmes d'IA à haut risque, la loi européenne sur l'IA exige que les solutions techniques visant à remédier aux vulnérabilités spécifiques à l'IA soient adaptées aux circonstances et aux risques concernés.

- **Risque** : L'exécution de modèles d'IA sur un système d'exploitation en fin de vie permet aux attaquants d'exploiter des failles au niveau du système d'exploitation pour contourner les garde-fous de l'IA au niveau de l'application (par exemple, l'empoisonnement des données).

3. Le plan de transition immédiat : « Contenir et migrer »

Pour maintenir la sécurité des patients et la conformité réglementaire sans remplacement immédiat du matériel, nous devons mettre en œuvre une défense en profondeur stratégique.

Phase 1 : Durcissement immédiat (L'état « sans état »)

- **Action** : Activez les filtres d'écriture unifiés (UWF). Toute modification effectuée par un logiciel malveillant ou un utilisateur est enregistrée dans la mémoire RAM et effacée au redémarrage.
- **Justification** : Cela répond au besoin de résilience face aux erreurs, aux défauts ou aux incohérences au sein de l'environnement du système, comme le prévoit la loi sur l'IA.

Phase 2 : Isolation du réseau

- **Action** : Mettre en œuvre la ségrégation des réseaux.
- **Justification** : Cela correspond à **ISO/IEC 27002:2022 Contrôle 8.22**, qui stipule que les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés dans les réseaux de l'organisation.

Annexe B : Implémentation technique (script PowerShell)

Artefact:Initialiser-MedicalDeviceUWF.ps1

But: Configurer le système d'exploitation Windows 10 IoT Enterprise en mode « sans état » pour pallier l'absence de correctifs de sécurité.

PowerShell

```
<#
```

.SYNOPSIS

Renforce la sécurité d'un appareil médical d'entreprise Windows 10 IoT en activant le filtre d'écriture unifié (UWF).

.DESCRIPTION

Ce script effectue les actions suivantes pour parvenir à une posture de sécurité « sans état » :

1. Vérifie et installe la fonctionnalité Windows UWF si elle est manquante.
2. Configure la superposition pour utiliser la RAM (essentiel pour effacer les logiciels malveillants au redémarrage).
3. Définit la taille de la superposition (par défaut : 2048 Mo).
4. Ajoute des exclusions critiques pour Windows Defender (afin de permettre la persistance des mises à jour des définitions de sécurité).
5. Protège le volume C:.
6. Active le filtre UWF.

NOTES

- REDÉMARRAGE REQUIS : L'appareil doit être redémarré pour que la protection prenne effet.
- AVERTISSEMENT DE PERTE DE DONNÉES : Une fois activée, TOUT fichier enregistré sur C: disparaîtra au redémarrage, sauf s'il est explicitement exclu.

```
#>
```

```
# Assurez-vous que le script est exécuté en tant qu'administrateur
```

```
si(!(([Security.Principal.WindowsPrincipal][Sécurité.Principal.IdentitéWindows]::GetCurrent()).IsInRole([Sécurité.Principal.RôleIntégréWindows]"Administrateur")) {
```

```
    Erreur d'écriture "Ce script nécessite des privilèges d'administrateur. Veuillez l'exécuter en tant qu'administrateur."
```

```
    Sortie 1
```

```
}
```

```
Écrire-Hôte "--- Démarrage du protocole de durcissement UWF ---" -Couleur de premier planCyan
```

```
1. Installez la fonctionnalité UWF si elle n'est pas présente.
```

```
$uwfFeature=Get-WindowsOptionalFeature -En ligne -Nom de la fonctionnalité "Client-UnifiedWriteFilter"
```

```
si($uwfFeature.État -ne "Activé") {
```

```
    Écrire-Hôte « Installation de la fonctionnalité Unified Write Filter... » -Couleur de premier planJaune
```

```
    Activer-WindowsOptionalFeature -En ligne -Nom de la fonctionnalité "Client-UnifiedWriteFilter" -Tous -NoRestart
```

```

Écrire-Hôte "Fonctionnalité installée. Un redémarrage sera nécessaire à la fin." -Couleur de
premier plan Vert
}autre{
    Écrire-Hôte "La fonctionnalité UWF est déjà installée." -Couleur de premier plan Vert
}

```

2. Réinitialisez l'UWF à son état initial avant la configuration.

Écrire-Hôte "Réinitialisation de la configuration UWF aux valeurs par défaut..."

uwfmgr.exe **filtre** réinitialiser les paramètres

3. Configurer la superposition (mode RAM)

Nous utilisons le mode RAM afin que les données soient stockées dans la mémoire volatile.

AVERTISSEMENT : Si la mémoire tampon est saturée, le système risque de se bloquer.
2048 Mo constituent une taille de tampon standard et sûre pour les appareils modernes.

Écrire-Hôte "Configuration de la superposition de RAM (Taille : 2048 Mo)..."

superposition uwfmgr.exe **type d'ensemble** RAM

superposition uwfmgr.exe **taille de l'ensemble** 2048

superposition uwfmgr.exe **définir le seuil d'alerte** 1500

superposition uwfmgr.exe **seuil critique défini** 1900

4. Protéger le volume système (C:)

Écrire-Hôte "Verrouillage du volume système (C:)..."

uwfmgr.exe protection du volume C:

5. Ajouter des exclusions de sécurité critiques

Nous autorisons Windows Defender à écrire sur le disque afin que les signatures antivirus persistent après un redémarrage.

Écrire-Hôte "Ajout d'exclusions pour Windows Defender..."

fichier uwfmgr.exe **ajouter-exclusion** "C:\ProgramData\Microsoft\Windows Defender"

fichier uwfmgr.exe **ajouter-exclusion** "C:\Windows\WindowsUpdate.log"

registre uwfmgr.exe **ajouter-exclusion**

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender"

6. Activez le filtre

Écrire-Hôte "Activation du filtre d'écriture unifié..."

uwfmgr.exe **filtre** activer

Écrire-Hôte "--- Configuration terminée ---" -Couleur de premier plan Cyan

Écrire-Hôte "AVERTISSEMENT : L'appareil est maintenant pré-verrouillé." -Couleur de premier plan Rouge

Écrire-Hôte "La protection s'activera après le prochain redémarrage." -Couleur de premier plan Rouge

Écrire-Hôte "Pour assurer la maintenance de l'appareil (installation de mises à jour/applications) ultérieurement, utilisez : 'uwfmgr servicing enable'"

Annexe C :Brouillon Communication avec la clientèle (Avis de sécurité sur le terrain)

À: Administrateurs d'hôpitaux, directeurs de la sécurité informatique et services d'ingénierie clinique

Depuis Bureau de la sécurité des produits de [Nom de votre entreprise]

Date: 3 novembre 2025

Sujet : ACTION DE SÉCURITÉ OBLIGATOIRE : Fin de vie de Windows 10 et configuration « sans état »

1. Résumé : Action immédiate requise

À compter du 14 octobre 2025, Microsoft a officiellement mis fin à la prise en charge du système d'exploitation Windows 10 (éditions à disponibilité générale) intégré à votre [Nom du modèle de l'appareil].

Afin de maintenir la conformité aux exigences générales de sécurité et de performance (GSPR) du règlement européen relatif aux dispositifs médicaux (MDR) et de préserver **CE Mark** Compte tenu de l'état de ces appareils, nous exigeons l'activation immédiate de **Profil de sécurité « sans état » (filtre d'écriture unifié)** et strict **Ségrégation du réseau**.

2. Justification réglementaire et de sécurité

Sous la **Loi européenne sur l'IA**, nous devons veiller à ce que les systèmes d'IA à haut risque soient résilients face aux tentatives de tiers non autorisés visant à modifier leur utilisation ou à compromettre leurs propriétés de sécurité. De plus, **ISO/IEC 27001:2022** nécessite la gestion active des vulnérabilités techniques.

Sans prise en charge du système d'exploitation par le fournisseur, il nous est impossible d'évaluer l'exposition aux nouvelles menaces. Par conséquent, nous devons mettre en œuvre des mesures de protection robustes afin de prévenir l'empoisonnement des données et l'exécution non autorisée de code.

3. La solution imposée : le fonctionnement « sans état ».

Avec effet immédiat, toutes les unités fonctionnant sous Windows 10 migrent vers une architecture sans état.

- **Verrouillage du disque** :Le lecteur C: sera en lecture seule.
- **Désinfection lors du redémarrage** :Tout fichier écrit ou logiciel malveillant introduit pendant une session clinique sera redirigé vers la RAM et supprimé au redémarrage.

4. Configuration réseau requise

Conformément à **Contrôle ISO/IEC 27002 8.22**, les groupes de services et de systèmes d'information doivent être séparés dans les réseaux de l'organisation.

Vous devez déplacer ces appareils vers un **VLAN mis en quarantaine** avec la liste de contrôle d'accès (ACL) suivante :

- **REFUSER:**Tout le trafic entrant provenant d'Internet public.
- **REFUSER:**Tout le trafic SMB (partage de fichiers) (Ports 445/139).
- **PERMETTRE:**Trafic sortant TLS 1.2/1.3*seulement* à vos adresses IP PACS/HIS spécifiques.

5. Plan de mise en œuvre

Ci-joint le **Initialiser-MedicalDeviceUWF.ps1** script de durcissement.

- **Action:**Déployez ce script via votre système de gestion des terminaux ou manuellement en **30 novembre 2025**.
- **Vérification:**Les appareils ne présentant pas cette configuration après la date limite seront signalés comme « à risque ».