Checklist de la data room

Ce qu'il faut préparer avant une due diligence santé par fovea. Cochez ce qui existe et notez ce qui manque.

Quatre dossiers, un par dimension. Déposez ce qui existe. Une courte note sur ce qui manque aide davantage qu'un document écrit à la hâte.

COMMENT NOUS TRAITONS VOS DONNÉES

Nous n'avons pas besoin d'accès aux systèmes de production.

Nous n'avons pas besoin de données patients identifiables. Pour vérifier la validation d'un modèle, des données anonymisées ou synthétiques suffisent.

Nous travaillons dans votre data room et votre dépôt et ne copions pas de code sur nos propres systèmes.

NDA avant tout accès, et nous n'évaluons pas les concurrents directs des entreprises que nous conseillons.

1. Médecine

	Notes
☐ Rapport et plan d'évaluation clinique	
☐ Plans d'investigation clinique (CIP), plans d'analyse statistique et rapports d'études cliniques	
☐ Publications et enregistrements, par exemple sur ClinicalTrials.gov ou au DRKS	
☐ Notice d'utilisation et parcours clinique prévu	
☐ Plan et rapports de SCAC (PMCF), incidents et registre des réclamations	

2. Technologie

	Notes
☐ Vue d'ensemble de l'architecture, schéma des flux de données et hébergement (fournisseur, région, certifications comme ISO 27001, HDS ou BSI C5)	
☐ Accès en lecture au dépôt, SBOM avec liste des SOUP	
☐ Stratégie de test, couverture de tests et description de la chaîne CI/CD	
☐ Modèle de menaces, rapports de tests d'intrusion et état des corrections, journal des incidents	
☐ Spécifications d'interface (HL7v2, profils FHIR, ISiK) et liste des interfaces en production par client	

- [ ] Pour l'IA : description des données d'entraînement et de validation, model cards, rapports de validation, surveillance et processus de réentraînement

3. Réglementaire

	Notes
- [ ] Destination et justification de la classification, y compris la règle 11 du MDR pour les logiciels	
- [ ] Documentation technique selon les annexes II et III du MDR	
- [ ] Certificats de l'organisme notifié, rapports d'audit et non-conformités ouvertes	
- [ ] SMQ : certificat ISO 13485 et procédures principales	
- [ ] Documentation IEC 62304 avec classe de sécurité logicielle, dossier de gestion des risques ISO 14971, dossier d'aptitude à l'utilisation IEC 62366	
- [ ] AIPD, mesures techniques et organisationnelles, contrats de sous-traitance	
- [ ] Analyse des écarts EU AI Act si le produit utilise l'IA, documents de remboursement comme le dossier DiGA	

4. Go-to-market

	Notes
- [ ] Liste des clients avec valeur du contrat, date de début et de renouvellement	
- [ ] Pipeline avec étape, voie d'achat et date de signature attendue	
- [ ] Prix, contrats types et accords de pilote	
- [ ] Effort d'implémentation par client, résiliations et renouvellements	
- [ ] Deux ou trois contacts de référence que nous pouvons appeler	

Comment se déroule un Red Flag Check

Jour 0	**Accès**	NDA signé. Vous ouvrez une data room en lecture seule et nous donnez un accès en lecture limité dans le temps à votre dépôt de code, avec journal d'accès activé.
Jour 1	**Lancement**	Trente minutes avec le CEO. Nous convenons du périmètre, du calendrier et des interlocuteurs, puis envoyons la liste des documents que nous n'avons pas trouvés.
Jours 1 à 3	**Revue documentaire**	Nous lisons les documents, le code et la configuration. Nous n'exécutons rien sur vos systèmes.

Jours 2 à 4	**Entretiens**	Environ 45 minutes chacun avec le CEO, le CTO et la direction médicale, plus QA/RA si le poste existe. Dans une Full Due Diligence, aussi avec des utilisateurs cliniques, des clients et la DSI hospitalière.
Jour 5	**Vérification des faits**	Vous voyez nos constats factuels avant que l'investisseur reçoive le rapport, et pouvez corriger ce que nous aurions mal compris.