Checkliste Datenraum

Was Sie vor einer Healthcare Due Diligence durch fovea vorbereiten. Haken Sie ab, was vorhanden ist, und notieren Sie, was fehlt.

Vier Ordner, einer pro Dimension. Laden Sie hoch, was existiert. Eine kurze Notiz zu fehlenden Unterlagen hilft mehr als ein Dokument, das in Eile entstanden ist.

SO GEHEN WIR MIT IHREN DATEN UM

Wir brauchen keinen Zugang zu Produktivsystemen.

Wir brauchen keine identifizierbaren Patientendaten. Wenn wir die Modellvalidierung prüfen, reichen anonymisierte oder synthetische Daten.

Wir arbeiten in Ihrem Datenraum und Repository und kopieren keinen Code auf eigene Systeme.

NDA vor dem Zugang, und wir prüfen keine direkten Wettbewerber von Unternehmen, die wir beraten.

1. Medizin

	Notizen
☐ Klinischer Bewertungsbericht und klinischer Bewertungsplan	
☐ Prüfpläne (CIP), statistische Analysepläne und klinische Studienberichte	
☐ Publikationen und Registereinträge, zum Beispiel bei ClinicalTrials.gov oder im DRKS	
☐ Gebrauchsanweisung und vorgesehener klinischer Workflow	
☐ PMCF-Plan und Berichte, Vorkommnisse und Beschwerdeprotokoll	

2. Technologie

	Notizen
☐ Architekturüberblick, Datenflussdiagramm und Hosting-Setup (Anbieter, Region, Zertifizierungen wie ISO 27001 oder BSI C5)	
☐ Lesezugang zum Repository, SBOM einschließlich SOUP-Liste	
☐ Teststrategie, Testabdeckung und Beschreibung der CI/CD-Pipeline	
☐ Bedrohungsmodell, Pentest-Berichte und Stand der Behebung, Incident-Log	
☐ Schnittstellenspezifikationen (HL7v2, FHIR-Profile, ISiK) und eine Liste der Live-Schnittstellen pro Kunde	

- [ ] Bei KI: Beschreibung der Trainings- und Validierungsdaten, Model Cards, Validierungsberichte, Monitoring und Retraining-Prozess

3. Regulatorik

	Notizen
☐ Zweckbestimmung und Begründung der Klassifizierung, einschließlich MDR-Regel 11 für Software	
☐ Technische Dokumentation nach MDR Anhang II und III	
☐ Zertifikate der Benannten Stelle, Auditberichte und offene Abweichungen	
☐ QMS: Zertifikat nach ISO 13485 und zentrale Verfahrensanweisungen	
☐ Dokumentation nach IEC 62304 mit Software-Sicherheitsklasse, Risikomanagementakte nach ISO 14971, Gebrauchstauglichkeitsakte nach IEC 62366	
☐ DSFA, technische und organisatorische Maßnahmen, Verträge zur Auftragsverarbeitung	
☐ Gap-Analyse zum EU AI Act, falls das Produkt KI nutzt, Unterlagen zur Erstattung wie der DiGA-Antrag	

4. Go-to-Market

	Notizen
☐ Kundenliste mit Vertragswert, Start- und Verlängerungsdatum	
☐ Pipeline mit Phase, Beschaffungsweg und erwartetem Abschlussdatum	
☐ Preise, Musterverträge und Pilotvereinbarungen	
☐ Implementierungsaufwand pro Kunde, Kündigungen und Verlängerungen	
☐ Zwei oder drei Referenzkontakte, die wir anrufen dürfen	

So läuft ein Red Flag Check

Tag 0	**Zugang**	NDA unterschrieben. Sie öffnen einen Datenraum mit Lesezugriff und geben uns einen befristeten Lesezugang zu Ihrem Code-Repository, mit eingeschaltetem Zugriffsprotokoll.
Tag 1	**Kick-off**	Dreißig Minuten mit dem CEO. Wir einigen uns auf Umfang, Zeitplan und Interviewpartner und schicken eine Liste der Unterlagen, die wir nicht gefunden haben.
Tag 1 bis 3	**Dokumenten-Review**	Wir lesen Dokumente, Code und Konfiguration. Gegen Ihre Systeme lassen wir nichts laufen.

Tag 2 bis 4	**Interviews**	Jeweils etwa 45 Minuten mit CEO, CTO und medizinischer Leitung, dazu QA/RA, falls vorhanden. In einer Full Due Diligence auch mit klinischen Anwendern, Kunden und der Krankenhaus-IT.
Tag 5	**Faktencheck**	Sie sehen unsere sachlichen Befunde, bevor der Investor den Bericht bekommt, und können alles korrigieren, was wir falsch verstanden haben.