

# Access to Markets:

## Key Differences and Overlaps

Once your UK evidence pack is built, it serves as a platform to build upon to expand into EU or US markets as core documentation and evidence is reusable with minor tailoring.

### What is the crossover?

#### Key:

- ✔ Explicitly required/assessed.
- ⚠ Conditional (depends on product/scenario).
- 📄 Expected evidence (commonly needed to demonstrate conformity).
- ✘ Not specified as an explicit requirement.



Cybersecurity Evidence Area (what to deliver)	DTAC (UK NHS)	EU MDR (with MDCG 2019-16 rev.1)	FDA 510(k) (with 524B for 'Cyber Devices')	Overlap and Practical Notes
<b>Baseline Organisational Assurance (Certifications).</b>	<ul style="list-style-type: none"> <li>✔ Cyber Essentials certificate requested in DTAC (C3.1).</li> <li>✔ Signed Cyber Security Charter for Suppliers to the NHS (C3.2)</li> <li>✔ Software Security Code of Practice confirmation (C3.4)</li> </ul>	<ul style="list-style-type: none"> <li>✘ No specific organisational certification mandated by MDR; focus is device lifecycle risk management and evidence.</li> </ul>	<ul style="list-style-type: none"> <li>✘ No specific organisational certification mandated.</li> <li>📄 QMS-linked cybersecurity processes expected in submissions; 524B focuses on device processes rather than org certification.</li> </ul>	DTAC is uniquely prescriptive about Cyber Essentials. For EU/FDA, certifications can help procurement but are not the regulatory 'core'.
<b>Secure Development Lifecycle (SDLC) and Governance.</b>	<ul style="list-style-type: none"> <li>📄 DTAC v2.0 does not prescribe a named SDLC framework, but C3.4 expects evidence across secure design/development, secure build, secure deployment/maintenance, and customer communication.</li> </ul>	<ul style="list-style-type: none"> <li>✔ MDR Annex I links state-of-the-art development life cycle, risk management including information security, verification and validation (MDCG highlights Annex I 17.2).</li> </ul>	<ul style="list-style-type: none"> <li>📄 FDA guidance recommends using a Secure Product Development Framework (SPDF) within the quality system; scaling with risk.</li> </ul>	EU and FDA both emphasise lifecycle integration of cybersecurity. In practice, IEC 81001-5-1 can anchor your processes (if you adopt it).
<b>System Security Architecture, Boundaries and Data Flows (Device/App/Cloud).</b>	<ul style="list-style-type: none"> <li>📄 Not a named DTAC upload, but strong supporting evidence for C3.4 because it underpins secure design, deployment, maintenance, and customer communication.</li> </ul>	<ul style="list-style-type: none"> <li>📄 Expected as part of technical documentation to demonstrate conformity and justify/verify security solutions; MDCG emphasises architecture as part of evidence.</li> </ul>	<ul style="list-style-type: none"> <li>📄 FDA guidance includes 'Security Architecture' and 'Architecture Views' as submission documentation (Appendix 2 provides diagrams/flows).</li> </ul>	Strong overlap for submission-grade evidence: a clear boundary diagram + trust boundaries reduces assessor friction, especially for connected device + cloud.
<b>Security Risk Management and Threat Modelling (Threats &gt; Controls &gt; Residual Risk).</b>	<ul style="list-style-type: none"> <li>📄 DTAC does not name a standalone threat model upload, but under C3.4 it is strong supporting evidence for secure-by-design development.</li> </ul>	<ul style="list-style-type: none"> <li>✔ Risk management system required (Annex I section 3) and cybersecurity risk should be included; MDCG discusses security risk assessment and threat modelling.</li> </ul>	<ul style="list-style-type: none"> <li>📄 FDA guidance includes Security Risk Management and Threat Modelling; for 524B, processes/procedures for reasonable assurance are required.</li> </ul>	Common core: threat modelling + cybersecurity risk assessment that ties back to safety risk management (and stays maintained as the design evolves).
<b>Third-party Software Components and Dependency Management.</b>	<ul style="list-style-type: none"> <li>📄 Not explicitly named in the DTAC form, but strong supporting evidence for C3.4 because the Code expects component identification, integrity checks, testing, and update management.</li> </ul>	<ul style="list-style-type: none"> <li>📄 Commonly needed to show control of vulnerabilities in libraries, OS components, and other third-party software across the lifecycle.</li> </ul>	<ul style="list-style-type: none"> <li>📄 FDA guidance includes 'Third-Party Software Components'; for 524B cyber devices, SBOM is explicitly required.</li> </ul>	EU/FDA are more explicit on software supply chain; DTAC is lighter, but NHS procurement often still asks. Aligning with SBOM practice reduces rework.

**Important Scope Note:** FDA statutory 524B requirements apply to devices meeting the definition of a 'cyber device'. For other devices, FDA guidance provides nonbinding recommendations on what to include in a 510(k) submission when cybersecurity risk exists.

**Sources (Official):** NHS England DTAC assessed section C; MDCG 2019-16 rev.1 (EU); FDA Cybersecurity FAQs (524B); FDA guidance "Cybersecurity in Medical Devices...", issued 3 Feb 2026.



# Access to Markets:

## Key Differences and Overlaps

Cybersecurity Evidence Area (what to deliver)	DTAC (UK NHS)	EU MDR (with MDCG 2019-16 rev.1)	FDA 510(k) (with 524B for 'cyber devices')	Overlap and Practical Notes
<b>Cybersecurity Testing Evidence (What was Tested and How Often).</b>	✔ For internet-based / internet-accessible products, must provide an external penetration test summary report from the previous 12 months, including OWASP Top 10 coverage (C3.3).	✔ MDCG states technical documentation should include methods/results of security testing as justification/verification of adopted solutions.	✔ FDA guidance includes 'Cybersecurity Testing' and expects evidence scaled with risk.	All three benefit from a simple 'test evidence index': scope, method, results summary, and follow-up actions.
<b>Minimum IT Requirements, Secure Configuration and User-facing Security Information.</b>	✔ DTAC asks about APIs, interoperability standards, open API practice/documentation, and integration with NHS/local systems where relevant (C4.1-C4.2.6).	✔ MDR Annex I includes minimum IT requirements and protection against unauthorised access; MDCG references minimum IT requirements (Annex I 17.4/23.4).	✔ FDA guidance contains labelling recommendations for devices with cybersecurity risks (secure setup, configuration, maintenance information).	Overlap: publish a one-page 'Secure deployment and operation' note: prerequisites, ports/protocols, roles, update approach, logging expectations.
<b>Post-market Surveillance (PMS) and Ongoing Cybersecurity Monitoring</b>	✔ DTAC does not impose a full PMS regime, but C3.4 strongly supports a lightweight post-release process for vulnerability triage, update decisions, customer communications, and evidence refresh.	✔ MDR includes pre- and post-market aspects; MDCG states technical documentation should be updated with PMS information related to handling/remediation of incidents and vulnerabilities.	✔ ⚠ For 524B cyber devices: must submit a plan to monitor, identify and address postmarket vulnerabilities/exploits. ✔ For other devices: postmarket management is strongly recommended by FDA guidance.	EU MDR is strongest here as a formal lifecycle regime. DTAC is lighter, but no longer silent because C3.4 clearly points to ongoing maintenance and communication.
<b>Coordinated Vulnerability Disclosure (VDP) / Intake Channel</b>	✔ Not a standalone DTAC upload, but strong supporting evidence for C3.4 because the Code expects a published vulnerability disclosure process and confidential reporting route.	✘ Not an explicit MDR requirement as a named artefact in MDCG, though handling vulnerabilities/incidents is part of lifecycle expectations.	✔ ⚠ For 524B cyber devices: postmarket plan must include coordinated vulnerability disclosure and related procedures.	Cross-market best practice: publish a VDP contact channel and triage process. Mandatory for many FDA 'cyber devices' and widely expected by enterprise buyers.
<b>Patching, Updates and Remediation Capability.</b>	✘ Not explicitly required within DTAC but C3.4 now asks suppliers to confirm adherence to the Software Security Code of Practice, including secure deployment and maintenance.	✔ MDCG describes modifying risk control measures/corrective actions/patches and updating technical documentation through PMS.	✔ ⚠ For 524B cyber devices: must make available postmarket updates and patches; processes/procedures for reasonable assurance are required.	Cross-market: a clear 'secure update/patch policy' (delivery method, prioritisation, emergency vs routine cadence) is high leverage.
<b>Software Bill of Materials (SBOM).</b>	✘ Not explicitly named in DTAC v2.0. ✔ Practical way to evidence component control and vulnerability management under C3.4.	✘ Not explicitly required as a named MDR/IVDR artefact, though often useful for component transparency and vulnerability management.	✔ ⚠ For 524B cyber devices: SBOM is explicitly required in premarket submissions.	Treat SBOM as: FDA-required (when applicable), EU-helpful, DTAC/procurement-friendly. Maintaining SBOM per release reduces late-stage submission pain.
<b>Interoperability and Secure Integration Controls.</b>	✔ DTAC interoperability section asks about APIs, applicable interoperability standards, open API practice/documentation, and integration with NHS/local systems (C4.1-C4.2.6).	✔ MDR Annex I includes interaction between software and the IT environment and interoperability/compatibility requirements; MDCG highlights these areas.	✔ FDA guidance includes interoperability considerations and expects interface/connection risks addressed.	Overlap: define scope boundaries and shared responsibilities (device vs app vs cloud vs hospital IT) to avoid gaps in threat modelling and procurement questionnaires.
<b>Privacy/Data Protection Controls (Cyber-adjacent).</b>	✔ DTAC data protection criteria require ICO registration evidence, product DPIA, transparency materials and fair data-use terms, where personal data is processed (C2.2.1-C2.2.6).	✔ MDCG notes privacy/confidentiality may be governed by other legislation (e.g., GDPR) and not explicitly in MDR; cybersecurity connects to confidentiality/integrity/availability.	✘ FDA 510(k) cybersecurity focuses on safety/effectiveness; HIPAA compliance is separate from 510(k) submission requirements.	Include privacy evidence when handling patient data, but keep it distinct from device cybersecurity evidence to avoid conflating regulatory scopes.