

UK MHRA Medical Device Cybersecurity Guide

Reviewed 2026-10-18 | Build UK cybersecurity evidence for Great Britain and Northern Ireland, with MHRA registration, current market routes, and postmarket responsibilities.

Define the destination before assembling UK medical device cybersecurity evidence. Great Britain (England, Wales, and Scotland) uses the UK Medical Devices Regulations 2002, as amended. Northern Ireland uses the EU MDR and IVDR framework. Security risk management, lifecycle, testing, deployment information, and vulnerability response should support the applicable conformity route and marketed configuration. There is no universal MHRA cybersecurity certificate that replaces that evidence.

[Download the matching UK cybersecurity PDF.](#)

This guide addresses evidence planning and maintenance, not a complete market-access opinion. Check [MHRA's current market guidance](#) before relying on a route or transition date. [MDC Crosswalk](#) is a companion for multi-market planning, not the authority for UK legal requirements.

Great Britain versus Northern Ireland

Decision	Great Britain	Northern Ireland
Main device framework	UK Medical Devices Regulations 2002, as amended	EU MDR / IVDR under the applicable NI arrangements
Marking route	UKCA or a qualifying recognized CE route	CE, or CE plus UKNI where the relevant UK-body route applies; not UKCA alone
Cybersecurity evidence anchors	Requirements of the chosen route and relevant safety/performance obligations	Applicable MDR or IVDR GSPRs and technical-documentation requirements
Postmarket framework	Part 4A for devices within its scope from June 16, 2025	Applicable EU/NI PMS and vigilance framework; do not substitute GB Part 4A
Local arrangements	MHRA registration and UK Responsible Person requirements where applicable	Check current NI registration and authorized-representative requirements separately

Use [MHRA's NI guidance](#) for that destination. A GB registration plan is not proof of eligibility in NI. If a product is supplied in both, retain two legal-route assessments even when technical evidence is shared.

Registration, local representation, and conformity

MHRA's GB guidance requires medical devices to be registered before placement on the GB market, with applicable arrangements for manufacturers outside the UK to appoint a UK Responsible Person. Confirm the current registration instructions, device category, and representative responsibilities.

Registration does not assess or approve all cybersecurity evidence and must not be presented as an MHRA endorsement. Marking, registration, local representation, technical evidence, and ongoing postmarket responsibilities are different parts of market access.

Current CE recognition: conditional ceilings

The MHRA market-access guidance reviewed on October 18, 2026 describes the following GB arrangements. Use its full route-specific conditions and any valid legal certificate extensions, not only a printed expiry date.

CE route	GB recognition ceiling described by MHRA
General medical devices under EU MDD / AIMDD	Earlier of the relevant certificate expiry or June 30, 2028, subject to qualifying conditions
IVDs under EU IVDD	Earlier of the relevant certificate expiry or June 30, 2030, subject to qualifying conditions
General devices under EU MDR and IVDs under EU IVDR	June 30, 2030 under the applicable recognition arrangements

Self-declared devices, device-specific exceptions, legal extensions, and transition conditions need separate checking. These dates do not authorize every CE-labeled device, and GB ceilings do not determine NI eligibility.

The [MHRA future-regulations implementation page](#) describes a 2026 consultation on indefinite CE recognition and planned premarket reform. Those statements do not, by themselves, establish effective indefinite recognition or a commenced replacement premarket regime. This guide has not established a later commenced instrument superseding the arrangements above. Check current legislation before an actual placement decision.

Cybersecurity evidence for the chosen route

These are recommended working artifacts, not a universal list of legally named UK cybersecurity attachments. For an EU-based route, use the [EU MDR/IVDR evidence crosswalk](#). For a UKCA route, retain the route-specific legal and standards rationale rather than relabeling an FDA package.

Evidence area	Practical records	UK adaptation question
Product and system scope	Intended use, marketed configurations, architecture, interfaces, and connected services	Does the evidence cover the GB or NI configuration and operating environment?
Security and relevant safety risk	Threat model, security risk assessment, control rationale, and links to potential harm	Can the manufacturer explain clinical consequences, limitations, and residual risk decisions?

Evidence area	Practical records	UK adaptation question
Secure lifecycle	Controlled procedures, design reviews, security requirements, and change impact records	Which standards and edition support the actual conformity route?
Components	Build-specific component inventory / SBOM and vulnerability assessment	Can the manufacturer identify affected versions and follow supplier vulnerabilities?
Security testing	Requirement/control traceability, abuse-case and penetration testing where appropriate, findings, and retests	Do scope, test environment, build, and unresolved findings match the supplied product?
Deployment information	Approved installation baseline, access settings, update instructions, support information, and responsibilities	Are instructions consistent with tested assumptions and local deployment?
Postmarket processes	Vulnerability intake, monitoring, risk review, PMS outputs, corrective action, and reporting decisions	Are GB and NI legal assessments separated where their rules differ?

[IEC 81001-5-1](#) can support lifecycle organization. Do not describe it as universally compulsory for all UK devices or equate a table with certification. Software safety and functional verification/validation remain manufacturer responsibilities; Blue Goat Cyber's work is cybersecurity support and security testing.

GB postmarket duties from June 16, 2025

[SI 2024/1368](#) introduced strengthened GB requirements through Part 4A. MHRA's [scope guidance](#) states that they apply to devices placed on the market or put into service in GB from June 16, 2025, whether CE- or UKCA-marked. Do not apply that statement indiscriminately to every earlier fielded device or to NI.

The cybersecurity contribution should connect to:

- A proportionate PMS system and plan, including relevant security information.
- Vulnerability and complaint intake, affected-build identification, and safety-impact assessment.
- Trend identification, corrective action, and updated risk and technical records.
- The applicable PMS report or PSUR, based on the device and rules.
- Vigilance decisions, field safety corrective action assessment, and customer communications where required.

Use the [Part 4A legislation](#) for controlling requirements and [MHRA vigilance guidance](#) for interpretation. Guidance is not a substitute for legislation.

Vulnerability-to-action workflow

- Record the report, awareness time, reporter, component, device/build, and available evidence.
- Establish whether the product is affected, including the UK configuration and deployed environment.

- Assess exploitability and relevant safety/performance consequences. CVSS alone cannot decide clinical risk.
- Make and record separate GB and NI reportability assessments where both markets are involved.
- Determine corrective measures, field safety action, user communication, and applicable notification timing with the manufacturer regulatory function.
- Verify the corrective action, update controlled records, and feed results into PMS and risk review.

Do not wait for complete root-cause analysis if an applicable reporting deadline is running. Not every CVE is a reportable serious incident, and not every software patch is a field safety corrective action. Keep the rationale and awareness timestamps instead of assuming an automatic classification.

Worked example: remote-service vulnerability

This is fictional. A CE-marked connected device is supplied in GB and NI, and a service-software vulnerability may permit unauthorized configuration changes.

Work item	Evidence and decision
Confirm affected products	Match component versions, service configuration, deployed access, and device build to the report
Assess consequences	Link realistic misuse to intended performance and possible harm; do not accept risk from a severity score alone
Route legal assessment	Check GB Part 4A applicability for relevant placements and the separate NI/EU vigilance framework
Plan mitigation	Manufacturer approves the action and appropriate customer/authority communication; retain configuration and safety impact analysis
Close the evidence chain	Security testing confirms the fix for the supported configuration; risk, component, release, and PMS records are updated

One technical investigation can support both markets, but a single unexamined reporting conclusion cannot replace two applicable legal assessments.

Readiness checklist

- Define GB, NI, or both and identify the product-specific conformity route.
- Verify valid marking and any transition eligibility against current MHRA guidance.
- Establish registration and local representation responsibilities.
- Index security evidence to the marketed configuration and applicable requirements.
- Confirm manufacturer approval of residual risk, labeling, and release decisions.

- Connect vulnerability monitoring to PMS, corrective action, and vigilance.
- Track proposals separately from commenced legislation.

How Blue Goat Cyber helps

We support threat modeling, security risk assessment, SBOMs, penetration testing, and cybersecurity evidence mapping. The manufacturer retains QMS ownership, clinical risk decisions, labeling approval, registration, and regulatory reporting responsibilities. [Book a discovery call](#) to scope the evidence work.

FAQ

Does MHRA registration approve cybersecurity?

No. Registration is not cybersecurity certification, conformity assessment, or endorsement. Maintain evidence for the actual route and ongoing responsibilities.

Can I use UKCA alone in Northern Ireland?

No. Check the applicable CE or CE-plus-UKNI arrangements in MHRA's NI guidance. GB and NI marking routes differ.

Did June 2025 introduce a universal cybersecurity premarket checklist?

No. It introduced strengthened GB postmarket requirements. Cybersecurity evidence must still support the relevant conformity route and safety/performance obligations.

Does every vulnerability need reporting?

Not automatically. Assess the applicable serious-incident, trend, and field safety action criteria and retain the manufacturer's regulatory decision. Act within applicable timelines where a reporting trigger is met.

Related regional guides

- [EU MDR/IVDR evidence crosswalk](#)
- [Japan PMDA cybersecurity guide](#)
- [IEC 81001-5-1 evidence table](#)

Sources and primary references

- [MHRA: regulating medical devices in the UK](#)
- [UK Medical Devices Regulations 2002, as amended](#)
- [SI 2024/1368: GB postmarket amendments](#)
- [Part 4A provisions introduced by SI 2024/1368](#)
- [MHRA: PMS introduction and scope](#)
- [MHRA: vigilance reporting requirements](#)
- [MHRA: EU medical device regulations in Northern Ireland](#)

- [MHRA: future-regulations implementation and policy status](#)
- [MHRA: registration of certain IVDs and certificate-transition guidance](#)

Current web guide: <https://bluegoatcyber.com/guides/uk-mhra-medical-device-cybersecurity>

Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.