

Medical device cybersecurity risk

Two matrices. One evidence trail. Manufacturer-owned decisions.

SECURITY

Every finding

Exploitability × security impact

SAFETY

Patient-affecting findings only

Exploitability × manufacturer harm severity

Client presentation | 23 October 2026



Classify first. Score from evidence.

01 STRIDE

Classifies threats; never determines a risk score.

02 CVSS v4.0

Record the vector and base score. Read exploitability from AV, PR, and UI.

03 TWO MATRICES

Highest of six CIA impacts for security; manufacturer severity for safety.

04 RESIDUAL REVIEW

Verify controls, re-score, and compare with manufacturer acceptance criteria.

These matrices and action priorities are BGC conventions, not mandated FDA thresholds or deadlines.



Security matrix | every finding

EXPLOITABILITY	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Impact = highest of VC, VI, VA, SC, SI, and SA: H → High; L → Medium; all N → Low.

The CVSS base score is recorded separately, never multiplied into this matrix.



Safety matrix | a separate patient-harm view

EXPLOITABILITY	Negligible	Minor	Serious	Critical	Catastrophic
High	Medium	High	High	Very High	Very High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Low	Medium	Medium

Severity comes from the manufacturer’s ISO 14971 hazard analysis, not a cybersecurity estimate.

Default residual line: Low / Medium controlled; High / Very High uncontrolled. Manufacturer criteria govern.

Security risk | Low

Limited service-log disclosure

A physical service interface exposes a small amount of nonclinical diagnostic data.

Exploitability: Low

Security impact: Medium

Record the finding and supporting evidence.

Fictional review: no clinical data, therapy, alarm, or essential-function pathway.

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Low

SECURITY MATRIX RESULT

Patient-safety rating: not applicable

CVSS base: 2.4 | Recorded only, not the matrix input

Security risk | Medium

Maintenance-record tampering

A physical service interface permits substantial alteration of maintenance records, without a clinical pathway.

Exploitability: Low

Security impact: High

Track remediation or document manufacturer acceptance with a reason.

Fictional review: these records do not drive therapy or clinical decisions.

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

Medium

SECURITY MATRIX RESULT

Patient-safety rating: not applicable

CVSS base: 5.1 | Recorded only, not the matrix input

Security risk | High

Administrative archive loss

A network attacker with high privileges can destroy a nonclinical administrative archive.

Exploitability: Medium

Security impact: High

Fix before release or on a defined postmarket timeline.

Fictional review: the archive is isolated from clinical workflows and device operation.

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

High

SECURITY MATRIX RESULT

Patient-safety rating: not applicable

CVSS base: 6.9 | Recorded only, not the matrix input

Security risk | Critical

Remote identity-store disclosure

An unauthenticated network attack exposes the identity store, without changing clinical functionality in this example.

Exploitability: High

Security impact: High

Fix immediately and recheck the patient-safety gate.

Fictional review: disclosure alone; no demonstrated pathway to patient harm.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Critical

SECURITY MATRIX RESULT

Patient-safety rating: not applicable

CVSS base: 8.7 | Recorded only, not the matrix input

Safety risk | Low

Bedside display interruption

Physical access can briefly interrupt a nonessential display while essential functions remain available.

Exploitability: Low

Manufacturer severity: Negligible

Default residual line: controlled, subject to manufacturer criteria.

Fictional manufacturer evidence: temporary patient inconvenience is possible; independent essential functions remain available.

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

Low

SAFETY MATRIX RESULT

Companion security rating: Low

CVSS base: 2.4 | Recorded only, not the matrix input

Safety risk | Medium

Restricted alarm delay

A privileged network attacker can delay an alarm, with an independent detection path limiting harm.

Exploitability: Medium

Manufacturer severity: Minor

Default residual line: controlled; keep rationale and control evidence.

Fictional manufacturer evidence: delayed detection may cause minor harm under the stated use conditions.

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Medium

SAFETY MATRIX RESULT

Companion security rating: High

CVSS base: 6.9 | Recorded only, not the matrix input

Safety risk | High

Clinical-data alteration

A privileged network attacker can alter clinical data used for a treatment decision.

Exploitability: Medium

Manufacturer severity: Critical

Default residual line: uncontrolled; add controls and reassess.

Fictional manufacturer evidence: altered treatment decisions can cause critical harm.

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:H/SA:N

High

SAFETY MATRIX RESULT

Companion security rating: High

CVSS base: 8.2 | Recorded only, not the matrix input

Safety risk | Very High

Unauthenticated therapy command

An unauthenticated network attacker can alter delivered therapy.

Exploitability: High

Manufacturer severity: Catastrophic

Default residual line: uncontrolled; do not treat a score as acceptance.

Fictional manufacturer evidence: the therapy change can result in patient death.

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H

Very High

SAFETY MATRIX RESULT

Companion security rating: Critical

CVSS base: 9.3 | Recorded only, not the matrix input

Controls change the inputs, not the rules

ILL-HZ-04 | same fictional therapy-command finding

INITIAL

Exploitability High

Security Critical | Safety Very High

RESIDUAL

Exploitability Low

Security Medium | Safety Medium

Fictional verified design: therapy changes require physical clinician confirmation and a privileged service session. Test evidence confirms remote paths are blocked.

Residual safety Medium: controlled under the BGC default line, but it still needs a written manufacturer reason the remaining risk is acceptable. A score is not acceptance.

CVSS:4.0/AV:P/AC:L/AT:N/PR:H/UI:A/VC:N/VI:H/VA:H/SC:N/SI:H/SA:H

Patient evidence and postmarket changes

PATIENT GATE

Document the path to clinical data, therapy, essential function, or alarms. PHI disclosure alone does not pass.

UNCERTAINTY

Treat unclear patient reach as patient-affecting for review; obtain manufacturer hazard and severity evidence.

KNOWN EXPLOIT

Confirm device applicability; record E:A for KEV. KEV alone does not change AV/PR/UI exploitability.

FAILED CONTROL

Re-score if evidence shows a control is defeated. Record the change and manufacturer response decision.

The manufacturer owns the decision

Eliminate → Mitigate → Accept → Transfer

Transfer is a last resort, explicitly justified. Labeling is not proof that a risk is acceptable.

Before scoring

Set acceptance criteria and connect cybersecurity findings to the hazard analysis.

Before acceptance

Review residual risk, control test evidence, and benefit-risk reasoning where applicable.

After release

Track changed evidence, vulnerabilities, failed controls, and required manufacturer actions.

BGC scores and recommends. Device class, software safety class, and cybersecurity risk are distinct.



Source basis and presentation limits

Method basis

Released executive Rev H (BGC-RISK-GUIDE-EXEC-260924) and guide Rev P (BGC-GUIDE-RISK-001): two risk matrices, CVSS v4.0 exploitability, patient gate, and control review.

How to use this presentation

All scenarios, control evidence, and clinical harm severities are fictional teaching examples. Apply the method using evidence from the device being assessed, with manufacturer-owned hazard analysis and acceptance criteria.

The matrices, patient-safety gate, and action priorities are BGC methodology conventions, not universal FDA or standards-mandated thresholds. A rating is not risk acceptance or authorization to release a device.

Present with Blue Goat Cyber attribution. No client data or regulatory outcome promises.