ISSUE 9 · FDA HUMAN FACTORS VS CYBER GAP

FDA's cyber guidance keeps pointing at human factors. Human factors never points back.

KEY TAKEAWAYS

- FDA finalized 'Content of Human Factors Information in Medical Device Marketing Submissions' on May 29, 2026, replacing the December 2022 draft, with a town hall set for July 22; read next to the premarket cybersecurity guidance, the two documents describe the same user but only one knows the other exists.
- The premarket cyber guidance (QMSR-aligned version reissued February 3, 2026, superseding the June 2025 final) says risks transferred to the user should be detailed and considered for inclusion as tasks during human factors testing, and its footnote cites the HF guidance directly.
- The new HF guidance has no cybersecurity section: per FDA's Federal Register notice the draft-to-final changes were added risk-based factors, new examples and appendices, and scope clarifications, none of which added cyber, so cyber hands risks to the HF process while the HF process has no idea they are coming.
- Security tasks are user tasks in the exact sense HF means: respond to a detected vulnerability or incident, download version-identifiable authorized software and firmware, act on security event notifications, back up and restore authenticated configurations, make user-configurable changes that could increase security risk, and sanitize the device at decommissioning.
- Run through the HF use-related risk analysis (URRA), several security tasks are candidate critical tasks (a nurse dismissing a security alert that renders like every other alarm, a biomed tech restoring an unauthenticated backup, a user sideloading firmware because the authorized path is stale), yet the author has not seen a URRA that includes them.
- URRA and threat modeling are the same decomposition (interface, failure mode, hazard, harm severity), differing only in accidental legitimate user versus deliberate adversary; AAMI TIR57 already bridges ISO 14971 safety and security risk, but HF and product security file to different sections and usually different reviewers.

> **"The two documents describe the same user, and only one of them knows the other exists."**

(Opening)

FDA finalized the HF marketing-submission guidance on May 29, 2026 with a July 22 town hall, and read beside the premarket cyber guidance the two describe the same user with no cross-reference from HF back to cyber. The cyber guidance explicitly hands user-facing risks to the HF process and footnotes the HF guidance, but the HF final added no cybersecurity section.

Security tasks are user tasks

The cyber guidance enumerates concrete user actions (incident response, authorized firmware download, acting on security notifications, authenticated backup/restore, risky user-configurable changes, decommissioning sanitization) that are user tasks in exactly the HF sense. Run through the URRA's decomposition into use errors, hazards, and harm severity, several are candidate critical tasks, yet the author has never seen a URRA that includes them.

URRA and threat modeling are the same decomposition

The URRA covers accidental legitimate-user error and a threat model covers deliberate adversary action, but both share the skeleton of interface, failure mode, hazard, and harm severity. AAMI TIR57 already bridges ISO 14971 safety and security risk, and a threat model enumerating initial access through the device UI is most of a security-aware URRA in different vocabulary, but the teams file to different sections and reviewers so nobody merges them.

The flowchart pulls cyber work in, both directions

Decision Point B pulls 524B security patches into the HF flowchart because they change authentication flows, add notifications, and rewrite IFU security instructions, generating HF submission-category questions. New Decision Point D lets manufacturers argue against HF validation via UI history, complexity, and existing risk controls, but its 'complex UI' language describes a security management console and 'existing risk control measures' route the argument through the security architecture.

A control the user cannot operate is not a control

Controls that fail human factors get bypassed (shared credentials, the workstation that never locks during a code), so usability failure is security failure, which the phrase 'risks transferred to the user' concedes. Town-hall questions closed June 12 so cyber probably will not come up, but an HF reviewer asking why a patch procedure was never validated with users, or a cyber reviewer asking why the URRA has no security tasks, are both legitimate questions today.

HF guidance finalized May 29, 2026, replacing the December 2022 draft; town hall July 22, with questions closed June 12.

Premarket cyber guidance: QMSR-aligned version reissued February 3, 2026, superseding the June 2025 final.

Verbatim cyber-guidance labeling text: 'Any risks transferred to the user should be detailed and considered for inclusion as tasks during usability testing (e.g., human factors testing)...'

Standards/regulatory hooks: AAMI TIR57, ISO 14971, FDA 524B.

Flowchart mechanics: Decision Point B (modification touches UI/users/uses/environment/training/labeling) and new Decision Point D (argue against HF validation via UI history, complexity, existing risk controls).

Enumerated security user tasks: incident response, authorized software/firmware download, acting on security event notifications, authenticated backup/restore, user-configurable changes, and decommissioning sanitization.