CHiME

CIO CHEAT SHEET

FDA Final Guidance on Post-Market Management of Cybersecurity in Devices

Purpose: The purpose of this cheat sheet is to depict all the instances in the Food and Drug Administration's (FDA) final guidance issued December 28, 2016 on post-market management of cybersecurity of devices where the agency calls on manufacturers of these devices to perform certain activities. As the agency notes, however, "FDA's guidance documents, including this final guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word should in Agency guidance means that something is suggested or recommended, but not required."

1. **Introduction:**
    a. This guidance clarifies FDA's postmarket recommendations and emphasizes that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their postmarket management of medical devices.
2. **Background:**
    a. FDA believes that, in alignment with EO 13636 and PPD-21, public and private stakeholders should collaborate to leverage available resources and tools to establish a common understanding that assesses risks for identified vulnerabilities in medical devices among the information technology community, healthcare delivery organizations (HDOs), the clinical user community, and the medical device community.
3. **General Principles:**
    a. An effective cybersecurity risk management program should incorporate both premarket and postmarket lifecycle phases and address cybersecurity from medical device conception to obsolescence It is recommended that manufacturers apply the NIST Framework for Improving Critical Infrastructure Cybersecurity in the development and implementation of their comprehensive cybersecurity programs.
4. **Premarket Considerations:**
    a. Manufacturers should establish design inputs for their device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g).
    b. The approach should appropriately address the following elements:
        i. Identification of assets, threats, and vulnerabilities;
        ii. Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
        iii. Assessment of the likelihood of a threat and of a vulnerability being exploited;
        iv. Determination of risk levels and suitable mitigation strategies;
        v. Assessment of residual risk and risk acceptance criteria.
5. **Postmarket Considerations:**
    a. Cybersecurity risk management programs should emphasize addressing vulnerabilities which may permit the unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient, and may result in patient harm.
    b. Manufacturers should respond in a timely fashion to address identified vulnerabilities. Critical components of such a program include:
        i. Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;
        ii. Maintaining robust software lifecycle processes that include mechanisms for:
            1. monitoring third party software components for new vulnerabilities throughout the device's total product lifecycle;
            2. design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to Off-the-shelf software;
        iii. Understanding, assessing and detecting presence and impact of a vulnerability; · Establishing and communicating processes for vulnerability intake and handling

iv. Note: The FDA has recognized ISO/IEC 30111:2013: Information Technology – Security Techniques – Vulnerability Handling Processes; · Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;

v. Adopting a coordinated vulnerability disclosure policy and practice. The FDA has recognized ISO/IEC 29147:2014: Information Technology – Security Techniques – Vulnerability Disclosure which may be a useful resource for manufacturers; and

vi. Deploying mitigations that address cybersecurity risk early and prior to exploitation.

c. To manage postmarket cybersecurity risks for medical devices, a company should have a structured and systematic approach to risk management and quality management systems consistent with 21 CFR part 820. For example, such a program should include:

i. Methods to identify, characterize, and assess a cybersecurity vulnerability.

ii. Methods to analyze, detect, and assess threat sources. For example:

1. A cybersecurity vulnerability might impact all of the medical devices in a manufacturer's portfolio based on how their products are developed; or
2. A cybersecurity vulnerability could exist vertically (i.e., within the components of a device) which can be introduced at any point in the supply chain for a medical device manufacturing process.

d. Vulnerabilities that do not appear to currently present a risk of patient harm should be assessed by the manufacturer for future impact.

6. Maintaining Safety and Essential Performance.

a. Manufacturers should define, as part of the comprehensive cybersecurity risk management, the safety and essential performance of their device, the resulting severity of patient harm if compromised, and the risk acceptance criteria.

7. Medical Device Cybersecurity Risk Management.

a. As part of their risk management process consistent with 21 CFR part 820, a manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls.

b. This process should include risk analysis, risk evaluation, risk control, and incorporation of production and post-production information.

c. Elements identified in the Appendix of this guidance should be included as part of the manufacturer's cybersecurity risk management program to support an effective risk management process.

d. Manufacturers should have a defined process to systematically conduct a risk evaluation and determine whether a cybersecurity vulnerability affecting a medical device presents an acceptable or unacceptable risk.

e. Such analysis should also incorporate consideration of compensating controls and risk mitigations.

f. Assessing Exploitability of the Cybersecurity Vulnerability

i. Manufacturers should have a process for assessing the exploitability of a cybersecurity vulnerability.

ii. In using any vulnerability scoring system (or tool), weighting of the individual factors that contribute to the composite score should be carefully considered.

g. Assessing Severity of Patient Harm

i. Manufacturers should also have a process for assessing the severity of patient harm, if the cybersecurity vulnerability were to be exploited

h. Evaluation of Risk of Patient Harm

i. For risks that remain uncontrolled, additional remediation should be implemented.

ii. Risk mitigations, including compensating controls, should be implemented when necessary to bring the residual risk to an acceptable level.

8. Remediating and Reporting Cybersecurity Vulnerabilities

a. When determining how to manage a cybersecurity vulnerability, manufacturers should incorporate already implemented compensating controls and risk mitigations into their risk assessment.

b. In addition, manufacturers should:
    i. Adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the initial vulnerability report to the vulnerability submitter
    ii. Proactively practice good cyber hygiene, reassess risk assessments regularly, and seek opportunities to reduce cybersecurity risks even when residual risk is acceptable;
    iii. Remediate cybersecurity vulnerabilities to reduce the risk of patient harm to an acceptable level;
    iv. Conduct appropriate software validation under 21 CFR 820.30(g) to assure that any implemented remediation effectively mitigates the target vulnerability without unintentionally creating exposure to other risks;
    v. Properly document the methods and controls used in the design, manufacture, packaging, labeling, storage, installation and servicing of all finished devices as required by 21 CFR part 820;
    vi. Identify and implement compensating controls to adequately mitigate the cybersecurity vulnerability risk, especially when new device design controls may not be feasible or immediately practicable. In addition, manufacturers should consider the level of knowledge and expertise needed to properly implement the recommended control;
    vii. Provide users with relevant information on recommended device and compensating controls and residual cybersecurity risks so that they can take appropriate steps to mitigate the risk and make informed decisions regarding device use; and
    viii. Recognize that some changes made to strengthen device security might also significantly affect other device functionality (e.g., use of a different operating system) and assess the scope of change to determine if additional premarket or postmarket regulatory actions are appropriate.

c. Controlled Risk of Patient Harm
    i. For premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84, newly acquired information concerning cybersecurity vulnerabilities and device changes made as part of cybersecurity routine updates and patches should be reported to FDA in a periodic (annual) report. See Section VIII for recommended content to include in the periodic report.

d. Uncontrolled Risk to Safety and Essential Performance
    i. In assessing risk, manufacturers should consider the exploitability of the vulnerability and the severity of patient harm if exploited.
    ii. If the risk of patient harm is assessed as uncontrolled, additional risk control measures should be applied.
    iii. Manufacturers should remediate uncontrolled risks as quickly as possible. (see page 21 for more details)

e. Uncontrolled Risk to Safety and Essential Performance
    i. In assessing risk, manufacturers should consider the exploitability of the vulnerability and the severity of patient harm if exploited.
    ii. If the risk of patient harm is assessed as uncontrolled, additional risk control measures should be applied.
    iii. Manufacturers should remediate uncontrolled risks as quickly as possible. (see page 21 for more details)

9. Recommended Content to Include in PMA Periodic Reports

a. For PMA devices with periodic reporting requirements under 21 CFR 814.84, information concerning cybersecurity vulnerabilities, and device changes and compensating controls implemented in response to this information should be reported to FDA in a periodic (annual) report.

10. Appendix: Elements of an Effective Postmarket Cybersecurity Program

a. Identify

i. Maintaining Safety and Essential Performance

1. Manufacturers should define, as part of their comprehensive cybersecurity risk management plan, the safety and essential performance of their device,

the resulting severity of patient harm if compromised, and the risk acceptance criteria

- **ii. Identification of Cybersecurity Signals**
  1. Irrespective of the originating source, a clear, consistent and reproducible process for intake and handling of vulnerability information should be established and implemented by the manufacturer.
  2. Vulnerability Handling Processes that may be useful resources for manufacturers. Manufacturers should develop strategies to enhance their ability to detect signals (e.g., participating in an ISAO for medical devices).

b. Protect/Detect

- **i. Vulnerability Characterization and Assessment**
  1. When characterizing the exploitability of a vulnerability, the manufacturer should consider factors such as remote exploitability, attack complexity, threat privileges, actions required by the user, exploit code maturity, and report confidence.
- **ii. Risk Analysis and Threat Modeling**
  1. Risk analyses and threat modeling should aim to triage vulnerabilities for timely remediation.
  2. For each vulnerability, a summary report should be produced that concisely summarizes the risk analysis and threat modeling information. Due to the cyclical nature of the analyses, the information should be traceable to related documentation.
- **iii. Incorporation of Threat Detection Capabilities**
  1. Manufacturers should consider the incorporation of design features that establish or enhance the ability of the device to detect and produce forensically sound postmarket evidence capture in the event of an attack

c. Protect/Respond/Recover

- **i. Compensating Controls Assessment (Detect/Respond)**
  1. Manufacturers should assess and provide users with compensating controls such that the risk of patient harm is further mitigated.
  2. Manufacturers should also adopt a coordinated vulnerability disclosure policy and practice that includes acknowledging receipt of the vulnerability to the vulnerability submitter within a specified time frame.

d. Risk Mitigation of Safety and Essential Performance

- i. Once the preceding information has been assessed and characterized, manufacturers should determine if the risk of patient harm presented by the vulnerability are adequately controlled by existing device features and/or manufacturer defined compensating controls (i.e., residual risk levels are acceptable).
- ii. Actions taken should reflect the magnitude of the problem and align with the risks encountered.
- iii. Manufacturers should also include an evaluation of residual risk, benefit/risk, and risk introduced by the remediation.
- iv. Manufacturers should design their devices to ensure that risks inherent in remediation are properly mitigated including ensuring that the remediation is adequate and validated, that the device designs incorporate mechanisms for secure and timely updates.