Management Gaps of Health Care Software Used in Devices

Karen Flores

University of San Diego

Quality Measure

Table 1. Quality Measures for Monitoring Software for IoT Devices

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Step | Name | Description | Owner | Report to | Calendar Measure |
| 1 | Errors per KLOC | Non-corrected functional errors in code found by quality assurance team per 1000 lines of code. | QA Team | Management Team | At every code release |
| Defect per KLOC | Non-corrected non-functional errors found by quality assurance team per 1000 lines of code. | QA Team | Management Team | At every code release |
| Application Crash Rate | Number of times applications fails after a determined number of uses. ACR = F/U | QA Team | Management Team | At every code release |
| 2 | Risks per Use Case | Number of errors found per use cases reported by QA team at code release. Sum of Errors per KLOC and Defect per KLOC/Use case | Management Team | Company | At every code release |
| Patching Cadence | Amount of time needed in order to respond to incidents and patching cadence | Management Team | Company | At every code release |
| 3 | Non-compliant certification reasons | Enumeration of reasons for not complying with certification models | Company | Regulators & Associations | At every code release |
| Endpoint Incidents | Report of endpoint incidents that had been detected over a period of time | Company | Regulators & Associations | 6 months |
| Mean Time to Repair | Average span of time that involves incident discovery to when a working remedy is deployed. Time line starts at day 0 of suspected incident discovery until code release. | Company | Regulators & Associations | 1 year |
| 4 | Non-compliant certification reasons | General report for reasons detected for non-compliance of certification standards | Regulators & Associations | Government | 6 months |
| Issued Recommendations | General report of issued recommendations | Regulators & Associations | Government | 6 months |
| 5 | Reasons for non-compliance | General report for reasons detected for non-compliance of certification standards | Government |   | 1 year |
| Issued Recommendations | General report of issued recommendations | Government |   | 1 year |

This table contains the recommended quality measures needed to monitor software for IoT devices for health care applications. Measurement are presented in relation to the IoT Medical Devices Software Vigilance Workflow presented in previous sections. Measurements presented for steps 1 through 3 have the main goal to help manufacturers and software developers to identify the *Mean Time Between Failures* and *Mean Time to Recovery/Repair*. These two metrics are useful while assessing reliability and availability of a device and its software (Sandler, Ohstrom, Moy, & McVay, 2010; Siemens, 2011). On the other hand, measurements related to steps 4 and 5 are proposed as a form of monitoring and correlating failures that can be present in one or more manufacturers and have an impact for the whole industry. The main intention of these measurements is to assess the effectiveness of current certification standards and regulations.

# References

Sandler, K., Ohstrom, L., Moy, L., & McVay, R. (2010). *Killed by Code : Software Transparency in Implantable Medical Devices*. *Heart*.

Siemens. (2011). Mean Time Between Failures ( MTBF ) Background information on MTBF, 5.