King & Spalding

FDANews Inspection Summit: Mock Audit

Steven Niedelman
King & Spalding

Steven Lynn
Lynn Consulting, LLC

David Elder
Greenleaf Healthcare Consulting

Kristen Grumet
Greenleaf Healthcare Consulting

The Scenario — Pancreatix Insulin Company

Pancreatix Insulin Company

A leading edge, international manufacturer of insulin and distributor of supplies to support the diabetic community including test strips and glucometers.

There has been a history of product recalls. Recent FDA inspection has been classified as Voluntary Action Indicated (VAI).

Pancreatix Insulin Company hasn’t any experience with product related software or cybersecurity.

The Scenario — Pancreatix Acquires *Always Accurate* Glucose Monitoring Systems

Always Accurate is a small niche company, that received PMA approval for a implantable glucose monitoring system intended to continuously monitor patient glucose levels and provide results on portable monitoring device. (*i.e., iPhone*)

Approved by FDA for monitoring 'up to 90 days' before replacement. Approved in EU for 180 days.

FDA Pre-Approval inspection did not identify any significant issues. Due for post-approval inspection by FDA.

Device is contract manufactured and sterilized by Alpha manufacturing to *Always Accurate* specifications. Due diligence audit at Alpha revealed that on average there was an 55-60% acceptable yield, and widespread use of deviations to address changes.

Due diligence at both sites focused on QMS processes and product compliance reviews, but due to lack of experience, Pancreatix did not focus on software design controls or cybersecurity.

The Challenges

Software and Cybersecurity

- Unbeknownst to Pancreatix, there had been continuing software updates being made to address complaints and issues that have arisen since product introduction, several of which failed to detect hyper- and hypoglycemia events.
- Only one adverse event was reported to FDA in response to a MedWatch report received from FDA.
- Software updates were not evaluated for PMA Supplements and were not considered as Part 806 Corrections and Removals events.
- No thought given to potential cybersecurity risks.

The Challenges

Reports of devices failing prematurely (40 – 50 days) were not tracked or trended based upon approval language of ‘up to 90 days’.

Premature removals or re-insertions were not evaluated for reportability, as patients were reported to be fine, although there had been reports of surgical difficulties, delays and infections with no permanent injuries.

Three cybersecurity breaches resulted in erroneous patient results; only one reported to FDA in conjunction with one MDR report filed.

The Director of Commercial Product was recently fired. He threatened to go to FDA with information that would be concerning to the firm.

The Challenges

FDA INSPECTION

- FDA investigators show up at Pancreatix unannounced the day after Christmas to investigate the reported complaint and data breach, as well as other reports of devices being implanted that had failed final product clearance.
- Other than a skeleton crew that volunteered to clean up files, the firm is not in operation.
- Employees on site voluntarily acknowledge there were other similar breaches.
- During FDA's walk-through, investigators requested entry to a locked room. They were told it only contained old computers and office furniture; a box containing a printout of complaint logs with their disposition was discovered upon entry.
- Regarding the software updates, the R&D staff present state, "Hey. We were just making patches. We don't need to report those to the FDA."

Questions to Consider

Was Pancreatix obligated to allow FDA to inspect during a "shut down" during holiday break? Is there any significance to FDA showing up unannounced?

Should the individuals at Pancreatix have volunteered information to FDA that there had been other similar events to what they were investigating?

What is the significance or potential implications of finding the printout of complaint logs in the locked room of “old computers”?

Should anything be reported to the FDA retroactively, as it relates to the adverse events or software changes?

Should Pancreatix have taken any action when the Director of Commercial Product was fired?

Questions to Consider

Should Pancreatix submit PMA Supplements based on the software updates and cybersecurity changes made to address the breaches? If yes, does this increase the likelihood of any FDA "action" in combination with the expected MDR filing and potential Part 806 reports?

What needs to happen in the risk analysis space and why?

Do the software arguments hold water? If not, why not?

Is there any remediation of procedures or records that needs to be explored? If so, what and why?

What responses can Pancreatix reasonably expect to prepare, as a result of the surprise FDA inspection?

King & Spalding

Questions?