



Capsulas

What changes in 2026 for manufacturers in relation to medical device vigilance?

Information Document on the Medical Device Vigilance System and the Role of the Vigilance Officer at Healthcare Institutions

The Spanish Medicines Agency (AEMPS) has published an updated version of its information document on the medical device vigilance system and the role of the vigilance officer. This new version replaces the June 2015 edition and aligns its content with Regulations (EU) 2017/745 (MDR) and 2017/746 (IVDR), as well as with Royal Decree 192/2023 on medical devices and Royal Decree 942/2025 on in vitro diagnostic medical devices. Below, we analyse the changes with the greatest impact on manufacturers of these products.

Investigation of serious incidents

The 2026 document describes in greater detail the process for investigating serious incidents involving medical devices: AEMPS forwards the information received on the incident to the manufacturer, formally requests that an investigation be opened, and may intervene or launch an independent investigation where it considers this necessary.

The concept of a “serious incident” covers death and serious deterioration in a patient’s state of health, and now also includes serious public health threats and incidents that could have had serious consequences. In all such cases, manufacturers must have a clear procedure in place to receive the information, open an investigation, document the conclusions and respond within the applicable deadline. Incomplete or late responses may hinder the assessment and lead the competent authority to adopt additional measures.

The need to maintain complete and traceable product-file documentation and, ultimately, record evidencing that the product has complied with all applicable safety requirements now becomes an essential element in the investigation of serious incidents. It is also key to comply with any request to produce documents and to rebut the presumption that a product is defective under Directive (EU) 2024/2853 on liability for defective products in the EU. Having protocols in place to facilitate this work may prove particularly useful.

Field safety corrective actions and post-market surveillance

A field safety corrective action (FSCA) is redefined as any action taken for technical or medical reasons to prevent or reduce the risk of a serious incident in relation to a device made available on the market, removing the previous reference to the specific risk of death or serious deterioration. By extending the concept to any risk of a serious incident, the range of situations in which manufacturers may be required to implement a corrective action is broadened.

The list of FSCAs now includes two significant additions that did not appear in the AEMPS’s 2015 guidance: (i) updates to the device’s instructions for use and (ii) software updates. The previous version limited this list to the return, modification, exchange, destruction or adaptation of the device, and to recommendations issued by the manufacturer regarding its use. The express



What changes in 2026 for manufacturers in relation to medical device vigilance?

inclusion of software qualifying as a medical device as the subject of a corrective action reflects its growing importance and has direct consequences for manufacturers of digital solutions and connected devices. In this context, each update may constitute an FSCA subject to notification and may even require a formal communication to users or customers (a field safety notice or FSN), for example in the event of cyberattacks that may pose a threat to public health.

Post-market surveillance (PMS) is also expressly identified as a source for detecting situations that may give rise to an FSCA, requiring manufacturers to connect vigilance, complaints and PMS activities. FSCA procedures must therefore cover not only the withdrawal or destruction of the device, but also documentary and software updates as standalone corrective measures.

Market surveillance

The AEMPS information document further develops market-surveillance activities, expanding the possible sources for detecting problems to include conformity checks, quality defects, CE-marking issues, counterfeiting and reports from law-enforcement authorities. The measures contemplated include the cessation of marketing, withdrawal, cessation of use, recall from end users and specific monitoring by healthcare professionals. The document clarifies that manufacturers must be prepared to provide a coordinated response with distributors and customers in any of these situations.

Implant card and information for patients

There are also significant changes for manufacturers of implantable devices. Until now, the implant card operated largely as a three-copy administrative process. The focus now shifts to ensuring that patients receive useful, standardised and traceable information, with the UDI as the key identification

data. Manufacturers must therefore provide, at least in Spanish, an implant card approximately the size of a credit card and containing the harmonised minimum information: the device name and type, serial number, lot number, unique device identifier (UDI) and model, together with the manufacturer's name, address and website. The card must be accompanied by relevant information, including warnings, precautions, interference with reasonably foreseeable external influences, medical examinations or environmental conditions, the device's expected lifetime and any necessary follow-up, as well as information on materials and substances to which the patient may be exposed.

Some recommendations

In light of the document recently published by the AEMPS, medical device manufacturers should prioritise a review of the following three areas:

- (i) the serious-incident investigation procedure, ensuring that it reflects the new process and applicable response deadlines, as well as protocols designed to ensure the availability of complete files and records evidencing that their devices comply with all safety requirements imposed by the applicable legislation;
- (ii) the FSCA/FSN procedure, verifying that software updates and updates to the instructions for use are included as corrective actions and that vigilance is linked to PMS and complaints; and
- (iii) for manufacturers of implantable devices, the implant documentation, in particular the implant card containing the required minimum information, UDI, expected lifetime, follow-up and materials.

♦♦♦♦