How To Create a Class II SaMD Regulatory Strategy

A winning regulatory strategy for SaMD has five fundamental elements which reflect the key components of your future submission:

1. **The Right Regulation and Predicate**
2. **Risk Management**
3. **Software & Cybersecurity Testing**
4. **Human Factors & Usability Testing**
5. **Clinical Validation Testing**

In this “How To” guide, I have listed a series of questions I would typically ask a client when creating a regulatory strategy with them along with notes throughout to help guide you in the right direction. Here is **STEP 2: RISK MANAGEMENT**. Happy strategy formulating!

STEP 2: RISK MANAGEMENT

Note: If Risk Management were an equation, it would be simplified to this:
Risk Management = Risk Identification + Risk Mitigation

- We will use these three discrete steps during product development to identify and mitigate risks:
  - Crafting a benefit-risk narrative
  - Conducting a Preliminary Hazards Analysis (PHA)
  - Conducting a Failure Modes and Effects Analysis (FMEA)
- This How To will focus on the first two steps as they help guide regulatory strategy and early product design and development.

Note: Start conversational by defining the benefit-risk profile of the device.

- Why are you building this product? What are benefits compared to competitive products? What are the benefits to the user?
- What could go wrong with the device itself? For example, the algorithm could be inaccurate. What could go wrong with the user’s interaction with the device? For example, the user might have a hard time accessing a feature. How could your product get compromised? For example, the wrong people could gain access to sensitive data. What other risks related to device safety, usability, and security might be missing from our existing list?
- Why are the risks we have identified acceptable considering the benefits the device offers?

Note: Risk acceptability is like drawing the line in the sand to delineate what we can tolerate from what requires action. Risk acceptability is not a technical judgement but rather a strategic, ethical and regulatory decision that requires multiple perspectives (such as clinical, engineering, usability, security, and regulatory) to define. Risk acceptability is important to define as we will come back to this during the PHA and FMEA(s) stages.

- Is the benefit-risk profile I have define for my device similar to the benefit-risk profile of my selected predicate(s)? Are there more risks? Are there more benefits? Are there more of both?
  Note: It's fine to have more risks associated with your product compared to your predicate if they are met with more benefits. We want the benefit-risk profile to be leaning in favor of benefits outweighing the risks. This is also a great way to poke holes in your substantial equivalence strategy – does the benefit-risk profile highlight any questions about safety or effectiveness that we wouldn't ask about the predicate.

Note: Now that we have a benefit-risk profile, let's further refine it with a top-down approach that would ultimately generate ***a Preliminary Hazards Analysis (PHA)****. A PHA identifies hazards that could lead to accidents or failures associated with using the device. A PHA is typically created before detailed design or development begins, but they can still be helpful while you're deep into the design and development phases especially if your system scope has changed, if new design features are being introduced, and if you didn't fully consider usability at earlier stages of development.*

Note: Doing a PHA during your regulatory strategy phase may seem too early but you'll see why I think it's helpful at the end of this How To guide. Whether you're developing your device in-house or using a vendor, a PHA helps guide design and development while keeping your team grounded in risk-based decision making.

- Who on your team or in your network of advisors can we assemble to discuss the device's risks?
  Note: Ideally, we would have folks with backgrounds in software engineering, IT and security, regulatory and quality, clinical, and usability/user experience.
- What is the full scope of the device? What is the intended use? What is the use environment? Who are the intended users? What is the workflow which includes physical interactions, decisions the user must make, and the different interfaces the user must navigate?
- Do you know anything about what has gone wrong with previous devices you've released on the market or competitor products that are currently on the market?
  Note: Here is where using FDA's MAUDE database can be helpful. You can search for reported device issues based on product name or product codes and time periods. This isn't the cleanest database because it's solely based on reports received from industry or consumers. It's important to read through all the information provided to decide if it's applicable to your device and if so decide if the complaint is related to use of the

product, a device failure, or a security issue. Store this search and your search criteria in a report – you will want to use this to help comply with IEC 62366 when drafting a "Known use problems report" – more to come on that in STEP 4 of this How To guide.

- OK, the last 3 bullets help to tee up a cross-functional discussion with your team that uses the question: "What if…?" with the goal of identifying **hazards** that could lead to bad scenarios taking place. Here are some examples. *Note: Think about asking these "What if" questions based on specific risk sources – technical/system (includes security), use/user, environmental, and clinical:*
    - What if the battery overheats? [hazard = battery overheats]
    - What if the wireless connection drops during data transmission? [hazard = loss of wireless connection]
    - What if the user clicks the wrong button? [hazard = unintended device function]
- Answer each "what if" question. This will help us define the **hazardous situation**. Let's use the "What if the battery overheats [of a wearable device]?" question as an example. The hazard is the overheating battery. The hazardous situation is when a user is exposed to that hot battery in a wearable.
- What is the **harm** to the user, data, or device if that hazardous situation were to happen? In our overheating battery example, the harm could be a skin burn.
- How severe is each of the harms we identified?
  Note: ISO 14971 defines 5 categories to use. You don't get extra credit for creating your own list. Just go with this one even if your device doesn't have any potential catastrophic risks (that's a good thing).
- What is the likelihood that the hazardous situation would lead to harm?
  Note: I strongly recommend companies use the two-step probability approach (P1 & P2)[1] for FMEAs. But a qualitative score, such as 1-5 or descriptive terms such as "rare, possible, or frequent," is often used at the PHA stage. The goal is to identify risks that cross the line in the sand we drew when defining risk acceptability to support design and development.
- Let's revisit our benefit-risk profile, is there anything we would change now that we have completed the PHA?

[1] Annex C, ISO 14971: 2019