element

EBOOK | 2026

Wireless Medical Devices:

Global compliance and testing considerations

Based on a webinar presented by
Alexander Toohie, Technical Solution Manager, Element

element.com

CONTENTS

EXECUTIVE SUMMARY

Wireless functionality is now standard across a wide range of medical technologies, from diagnostic systems and portable equipment to wearables, implantables and consumables.

As connectivity becomes more common, regulatory and testing requirements become more complex. For manufacturers, the challenge is not simply adding wireless capability, but understanding how the compliance pathway changes once a product is treated as radio equipment for regulatory purposes.

This eBook is based on a webinar[1] presented by Alexander Toohie, Technical Solution Manager at Element, and explores how wireless functionality changes compliance requirements for medical devices in the EU, UK, US and Canada.

Wireless medical device compliance extends well beyond transmitter performance. In the EU, devices with radio functionality generally fall under the Radio Equipment Directive (RED), while in the UK similar requirements apply under the corresponding Radio Equipment Regulations. Together, these frameworks introduce obligations related to product safety, electromagnetic compatibility (EMC) and radio spectrum use.

Manufacturers must therefore consider more than transmitter characteristics such as power, frequency and bandwidth. They also need to address RF exposure, receiver performance, electromagnetic compatibility and select the appropriate conformity assessment route. Under RED, these obligations are set out in Article 3, with safety, EMC and efficient use of radio spectrum forming the main requirements for most wireless medical devices. Other RED provisions, such as cybersecurity and common charger requirements, are generally less relevant to medical devices. RED cybersecurity requirements, for example, do not apply to devices already covered by the Medical Devices Regulation (MDR) or the In Vitro Diagnostic Medical Devices Regulation (IVDR).

In the US and Canada, the regulatory pathway differs from the European model. Products with transmitter functions, such as Wi-Fi, Bluetooth or cellular connectivity, generally require FCC Certification in the US or ISED Certification in Canada. Other electronic functions that do not intentionally transmit, such as certain digital components or receiver-only operations, are typically addressed through a Supplier's Declaration of Conformity (SDoC) rather than full certification.

Compared with Europe, the North American framework places less emphasis on EMC immunity and receiver performance, and more on emissions, transmitter compliance and RF exposure. Testing through accredited laboratories is still required. For devices whose wireless link is essential to clinical performance, wireless coexistence is also an important consideration, particularly in the FDA context, because the device must be shown to operate reliably in the presence of real-world wireless signals.

Test readiness is another critical factor. Before testing can begin, laboratories need specific modes, configurations and documentation,

including transmit and idle modes for EMC, conducted fixtures for radio measurements, companion devices, methods for monitoring radio links, power supply strategies and required declaration forms. Without this preparation, testing delays are likely.

The eBook also examines the role of modular radios. Off-the-shelf radio modules can simplify development, but they do not remove the manufacturer's responsibility for compliance of the finished device. In the US and Canada, a pre-approved module may reduce or eliminate some new certification work, but only if the final product continues to meet the conditions of the original approval.

Even then, the finished product manufacturer should still test the device and confirm overall system compliance. In the EU and UK, the position is more straightforward: there is no legal concept of modular approval under CE or UKCA marking. If the finished product qualifies as radio equipment, the end-product manufacturer remains wholly responsible for demonstrating compliance.

Overall, adding wireless functionality places a medical device within a broader and more technically demanding compliance framework. Early planning and a clear understanding of testing requirements can support a more efficient path to market.

DISCLAIMER:

We have aimed to make this eBook as accurate and complete as possible at the time of publication. However, it should not be relied upon as a substitute for the relevant laws, regulations, standards or formal regulatory guidance. Technologies evolve, products change, standards are updated and regulatory requirements may be amended. In cases of uncertainty, readers should consult the current text of the applicable regulations, standards and official guidance.

INTRODUCTION

Wireless technologies are now embedded across modern healthcare environments, and medical devices increasingly incorporate radio functions for communication, positioning, tracking and power transfer. Wireless is now a defining feature of the medical device landscape.

As shown in **Figure 1**, this shift spans a wide range of products. Laboratory and diagnostic equipment may use Bluetooth to transfer data to nearby computers. Implantable devices are increasingly designed with wireless power transfer to reduce the need for surgical battery replacement. Wearables may combine Bluetooth, Wi-Fi, RFID (radio-frequency identification), NFC (near-field communication), cellular and GNSS capabilities, while portable equipment can rely on wireless connectivity for positioning or data backhaul. Even consumables are becoming part of the connected environment through RFID-based tracking in hospital settings.

Figure 1. Examples of medical device categories and potential wireless applications.

As wireless functionality is added, the regulatory position of a product changes as well. A device that once required only medical device compliance may also qualify as radio equipment, introducing additional obligations tied to radio legislation, testing methods and approval pathways in different regions.

This eBook does not revisit broader medical device regulations. Instead, it focuses on what changes when wireless features are introduced, covering five key areas: wireless technologies used in medical devices, EU and UK requirements, US and Canadian requirements, test readiness for laboratory programs and the opportunities and limitations of modular radios.

CHAPTER 1:
Wireless Medical Devices and Evolving Compliance Requirements

Adding wireless functionality to a medical device does more than expand its capabilities. It changes how the product must be evaluated for compliance.

Once a device includes radio functionality, it is no longer assessed only under medical device requirements. It may also need to meet applicable radio-equipment requirements, adding further regulatory and technical obligations.

In the EU and UK, this can bring the product within radio-equipment legislation and related conformity-assessment requirements. In the US and Canada, it can trigger FCC and ISED Certification requirements, respectively.

WHEN A MEDICAL DEVICE ALSO BECOMES RADIO EQUIPMENT

For manufacturers, the shift is not just technical but conceptual. Wireless connectivity should not be treated as a minor add-on to an otherwise unchanged product. A radio-enabled device enters a broader compliance category, which can affect both product assessment and market access strategy.

In practice, this means the device may become subject to radio-specific legislation alongside the frameworks already applicable to medical devices. The compliance burden expands beyond traditional product safety and device-specific requirements. Teams must consider radio performance, interaction with other electronics, spectrum use and any added RF exposure or interference risks.

A BROADER SET OF TECHNICAL OBLIGATIONS

Wireless compliance is often assumed to focus mainly on transmitter performance, but the scope is much broader. Once radio functionality is added, the assessment can extend into several technical areas.

These include radio spectrum performance, such as frequency, power, bandwidth and efficient spectrum use without harmful interference. They also include electromagnetic compatibility, which may require added monitoring and test conditions when radios are active, even though EMC is already familiar in medical device compliance. RF exposure may also need to be considered, particularly for devices used close to the body, depending on the design and target market. Manufacturers will also need to determine which conformity-assessment or certification routes are allowed in each region.

Taken together, these requirements make wireless compliance more than a narrow technical check. It becomes a broader assessment of how the connected product performs in real operating conditions and whether it can be legally placed on the market in each target region.

WHY EVEN SIMPLE WIRELESS FUNCTIONS MATTER

Not every connected medical product is a complex wearable or multi-radio platform.

Some may include only a simple wireless function, such as tracking or short-range communication. Even so, the presence of that radio function can still have compliance implications.

This is especially important for products that may not immediately be seen as connected technology, for example a device without a transmitter but which has an embedded GPS receiver. Once any radio functionality is present, the product may still fall within the scope of radio requirements. Manufacturers therefore cannot assume that a simpler wireless feature carries only minimal compliance consequences. Even relatively straightforward radio functions may lead to added testing, documentation or approval considerations, depending on the product and target market.

WIRELESS INTEGRATION SHAPES THE WIDER COMPLIANCE PROGRAM

A connected medical device cannot move through compliance by addressing radio testing in isolation. Wireless integration can affect multiple parts of the overall assessment program, including safety, EMC, RF exposure and regional approval strategy. This is one reason wireless product development often requires more planning than teams may initially expect.

The compliance pathway may also differ significantly depending on where the device will be marketed. The EU, UK, US and Canada all apply different regulatory frameworks to radio-enabled products. While some technical themes are shared, approval routes, documentation expectations and testing priorities are not identical.

For manufacturers, early planning is critical. Wireless functionality can influence not only what must be tested, but also which regulatory framework and assessment route apply, what evidence must be gathered and which route to market is available. Wireless compliance should therefore be treated as a product-level issue, not a component-level one.

Adding wireless functionality changes the compliance profile of a medical device by bringing radio-equipment requirements into scope alongside medical device requirements.

This introduces added obligations related to spectrum use, EMC, RF exposure and region-specific approval pathways. Just as importantly, it broadens compliance from a narrow focus on transmitter performance to a fuller assessment of how the finished product performs as a connected system.

CHAPTER 2
EU and UK Regulatory Requirements for Wireless Medical Devices

Adding wireless functionality brings medical devices marketed in the EU and UK into a broader regulatory framework beyond core medical device requirements.

In the EU, wireless medical devices may fall within a CE marking framework that can include the Medical Devices Regulation (MDR), the In Vitro Diagnostic Medical Devices Regulation (IVDR), the EMC Directive, the Low Voltage Directive, RoHS and the Radio Equipment Directive (RED), depending on the product.

In the UK, the technical approach is broadly similar, but the legal framework is separate. Following Brexit, the UK retained much of the same structure by transposing EU legislation into domestic law (for example the UK's Radio Equipment Regulations (RER) are a near-identical copy of the EU's RED), and later adapting the terminology through secondary legislation. As a result, technical requirements for wireless products remain broadly aligned across the EU and UK, even though the legal frameworks are distinct.

These legislative frameworks define the legal obligations, while technical standards explain how compliance is demonstrated in practice. Manufacturers should therefore view the EU and UK systems as closely aligned, but not interchangeable.

The core principles are similar, but legislation, marking requirements and standards references must still be confirmed market by market.

RED AS THE MAIN FRAMEWORK FOR WIRELESS COMPLIANCE

Within the EU, RED becomes a central part of the compliance strategy when a medical device includes radio technology. It does not replace MDR or IVDR, but applies alongside them. A wireless medical device may therefore need to satisfy both medical device requirements and the radio-specific obligations introduced by RED.

Adding wireless capability does not create a separate product. It creates a medical device that is also radio equipment. In practice, manufacturers must assess not only intended medical use and core safety, but also radio spectrum use, interaction with other electronics and possible RF exposure.

RED ESSENTIAL REQUIREMENTS: UNDERSTANDING ARTICLE 3

The core EU wireless compliance framework is set out in Article 3 of RED[2].

As shown in **Table 1**, Article 3 defines the essential requirements for radio equipment and provides the main framework for determining what applies once a medical device includes wireless functionality.

This chapter uses RED as the primary reference point, while noting that UK implementation should still be checked separately where needed.

Table 1. Article 3 of the Radio Equipment Directive (RED) 2014/53/EU sets out the essential requirements that radio equipment must meet before it can be placed on the EU market.

Article 3 – Essential Requirements			
Article 3.1	Article 3.2	Article 3.3	Article 3.4
Article 3.1(a)		Article 3.3(a)	
Article 3.1(b)		Article 3.3(b)	
		Article 3.3(c)	
		Article 3.3(d)	
		Article 3.3(e)	
		Article 3.3(f)	
		Article 3.3(g)	
		Article 3.3(h)	
		Article 3.3(i)	

Article 3.1 covers health and safety and electromagnetic compatibility.

Article 3.2 covers efficient and effective use of radio spectrum.

Article 3.3 includes additional requirements for certain categories of equipment, only four of which (articles 3.3(d) through (g)) are currently enacted, including some cybersecurity-related provisions.

Article 3.4 covers common charger requirements for a limited number of product categories.

For most wireless medical devices, the main focus is on Articles 3.1 and 3.2, while Articles 3.3 and 3.4 apply more selectively.

HEALTH AND SAFETY UNDER RED ARTICLE 3.1(A)

Health and safety requirements for wireless products extend beyond conventional electrical safety. In addition to electrical safety, wireless medical devices may raise issues related to magnetic fields, heat, chemical exposure and, most notably, RF exposure. Wireless transmitters can create body-exposure concerns that must be assessed and controlled, so these products must be evaluated across multiple safety considerations.

For lower-power devices or devices used farther from the body, RF exposure can often be assessed by calculation. For products with higher output power, closer proximity to the body or both, Specific Absorption Rate (SAR) testing may be required.

SAR testing places the transmitting device beneath a phantom model representing part of the human body and uses a probe in calibrated tissue-simulating fluid to measure absorbed RF energy.

Figure 2 shows an example of a SAR setup. The goal is to demonstrate that absorbed energy remains below established safe limits.

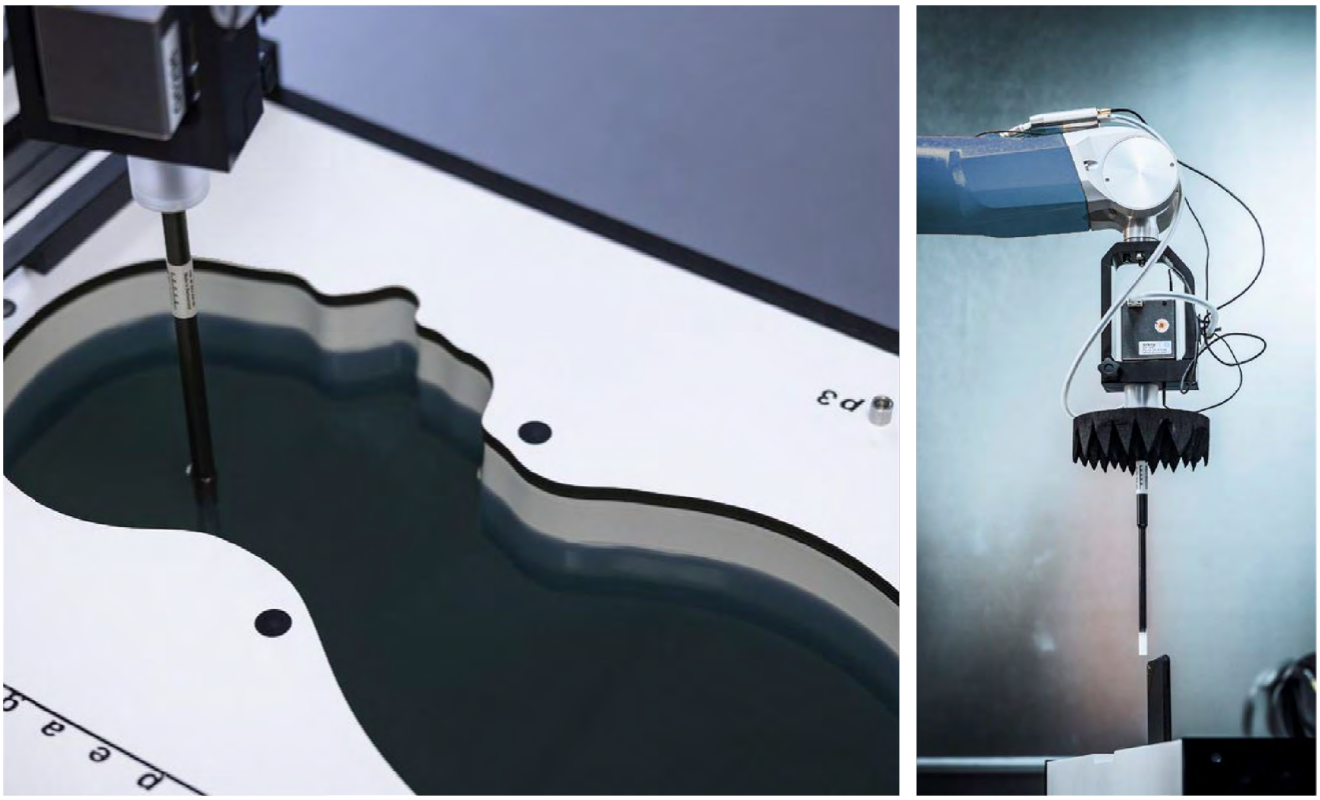

Figure 2. An example of a Specific Absorption Rate (SAR) testing setup.

For wireless medical devices, this is a key distinction from non-radio products: once radio transmission is present, RF exposure becomes part of the safety case.

EMC UNDER RED ARTICLE 3.1(B)

Article 3.1(b) brings electromagnetic compatibility into the RED framework. EMC is not unique to medical devices or wireless equipment; most electrical and electronic products already need to meet EMC requirements. Broadly, EMC includes radiated emissions, conducted emissions, radiated immunity, conducted immunity and electrostatic discharge testing.

What changes with wireless is not the existence of EMC testing, but the complexity of monitoring during that testing.

For non-radio devices, immunity testing mainly checks whether the product continues to function normally under electromagnetic disturbance.

For wireless devices, the lab must also verify that radio links continue operating as intended and that the device does not unintentionally transmit.

As set out in the EN 301 489 series[3], during immunity testing the equipment must continue to operate as intended, must not unintentionally transmit, must not unintentionally change operating state and must not unintentionally alter critical stored data.

This has an important consequence: if the radio is actively transmitting during EMC immunity testing, the lab can confirm that the link remains operational, but cannot confirm that the device is not unintentionally transmitting. For that reason, immunity testing is often performed twice: once with the radio operating normally and again with the radio in idle or receive mode. The second round helps determine whether electromagnetic disturbance causes transmissions that should not occur.

RADIO SPECTRUM REQUIREMENTS UNDER RED ARTICLE 3.2

Article 3.2 addresses the efficient and effective use of radio spectrum. In practice, this includes both transmitter and receiver testing.

Transmitter testing typically examines frequency, output power, bandwidth, band-edge behavior and, depending on the technology, characteristics such as hopping, timing or voltage stability.

These tests help ensure that the radio uses spectrum fairly and does not create harmful interference. Band-edge compliance is especially important where a device is permitted to transmit within one frequency range but adjacent ranges have stricter limits. The signal must fall off sharply at the band edge so that it does not spill into nearby frequencies.

Receiver testing is also an important part of the European framework. These assessments focus mainly on sensitivity and blocking performance. Sensitivity refers to how weak a wanted signal can be while still being received correctly. Blocking refers to how strong an unwanted nearby signal can be before it prevents the receiver from correctly interpreting the wanted signal.

ADDITIONAL RED REQUIREMENTS: CYBERSECURITY AND COMMON CHARGERS

Two areas that often create confusion are RED cybersecurity requirements and common charger requirements.

For Article 3.3 cybersecurity provisions, the key point is that equipment already regulated under MDR or IVDR is explicitly exempt. Because those frameworks already include secure development lifecycle and software-related requirements, RED does not duplicate them. This means RED cybersecurity provisions do not automatically apply to medical devices with internet connectivity or wearable form factors if MDR or IVDR already applies.

Article 3.4, which concerns common charger requirements, is narrower in scope and applies only to 13 specified radio equipment categories: handheld mobile phones, tablets, digital cameras, headphones, headsets, handheld videogame consoles, portable speakers, e-readers, keyboards, mice, portable navigation systems, earbuds and laptops.

There is no blanket medical device exemption: if a medical device falls within one of those categories, the common charger rules apply. In practice, however, overlap between these categories and most medical devices is narrow.

RED CONFORMITY ASSESSMENT PROCEDURES

Another important distinction between RED compliance and the more familiar medical device approval model is the conformity assessment route.

As shown in **Figure 3**, RED provides several conformity assessment routes, and the use of harmonized standards can determine which route is available. This differs from medical device pathways, where manufacturers are often more accustomed to working through a notified body.

For Articles 3.1 and 3.4, manufacturers can generally choose among three routes: Module A, Module B plus C or Module H. Module A is an Internal Production Control route with no notified body involvement.

Under this route, the manufacturer gathers the necessary evidence, usually through testing, prepares the declaration and places the product on the market. Under Module B, a notified body issues an EU-Type Examination Certificate, after which the manufacturer remains responsible for ensuring ongoing conformity to that approved type. Module H is a Full Quality Assurance route involving notified body oversight of quality and production processes.

For Articles 3.2 and 3.3, the available route depends on whether a harmonized standard has been applied in full. If it has, manufacturers may use the same three routes, and many choose Module A because it is the simplest and least costly. If a harmonized standard has not been applied in full, Module A is no longer available and the manufacturer must involve a notified body through Module B or Module H.

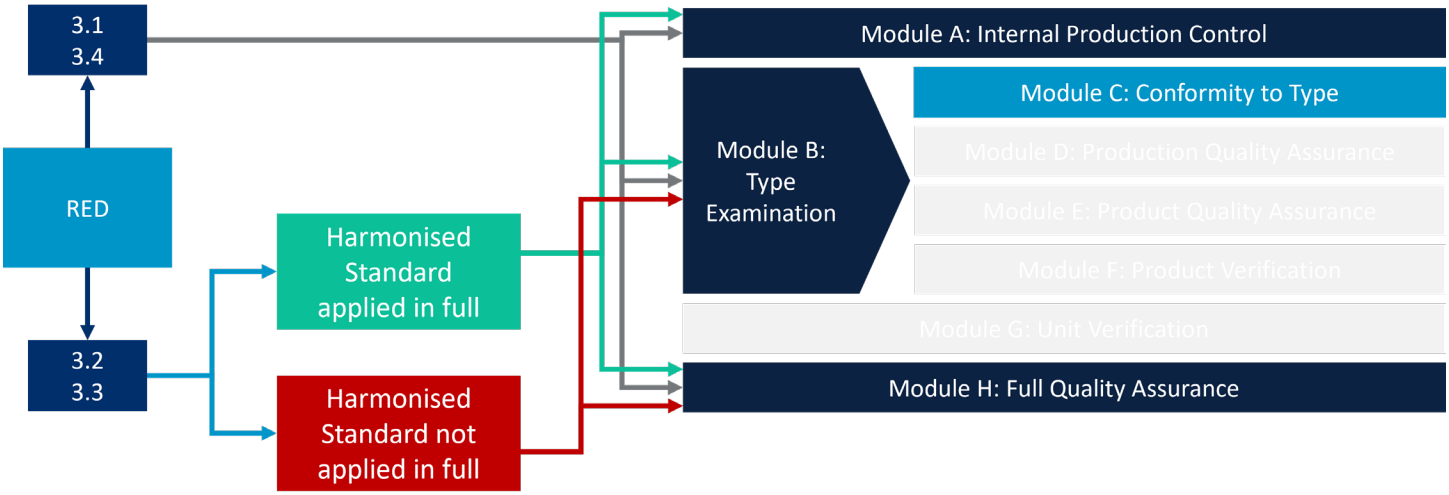

Figure 3. RED conformity assessment procedures.

Although this section uses RED terminology, the same broad conformity assessment logic also applies in the UK, even though the applicable technical standards are designated and maintained separately. This matters because manufacturers need to determine early whether they can apply those standards in full, since that affects whether they can self-declare or must involve a notified body. Note also that the UK equivalent of a notified body is called an approved body, and sometimes bodies who appear on the EU's RED notified body list do not also appear on the UK's RER approved body list; choosing a body able to issue both EU and UK certificates is crucial to avoid missing out on either market.

For wireless medical devices in Europe and the UK, the RED and the closely aligned UK RER requirements create a layered compliance framework built around health and safety, EMC and spectrum use. In practice, most manufacturers need to focus primarily on Articles 3.1 and 3.2, while remembering that cybersecurity and common charger obligations apply more selectively.

A key procedural distinction is that, unlike many medical device pathways, RED may allow manufacturers to use an internal production control route without notified body involvement when harmonized standards are fully applied. That makes selection of standards, evidence gathering and early planning especially important when bringing wireless medical devices to market.

CHAPTER 3:
Wireless Approval Pathways in the US and Canada

The US and Canada take a different regulatory approach from the EU and UK. In North America, wireless functions generally require formal FCC Certification in the US or ISED Certification in Canada. This contrasts with the European model, where compliance is based on declaration, even when a notified body is involved. In the US and Canada, manufacturers are working through formal approval systems tied to radio products. For medtech companies operating globally, that means one connected device may need to follow very different approval pathways depending on the target market.

THE US FRAMEWORK: FCC APPROVAL ROUTES

FCC requirements are set out under Title 47 of the Code of Federal Regulations (47 CFR). As shown in **Figure 4**, products are broadly divided into intentional and unintentional radiators.

Intentional radiators are transmitters, and must meet radio spectrum and RF exposure requirements. Unintentional radiators include digital electronics without transmitter functions, as well as receivers. These products must meet EMC-related requirements, although the FCC's EMC focus is narrower than Europe's because it is concerned mainly with emissions rather than immunity.

This distinction is important because many connected medical devices contain both types of functions. A single product may therefore need to satisfy multiple FCC requirements.

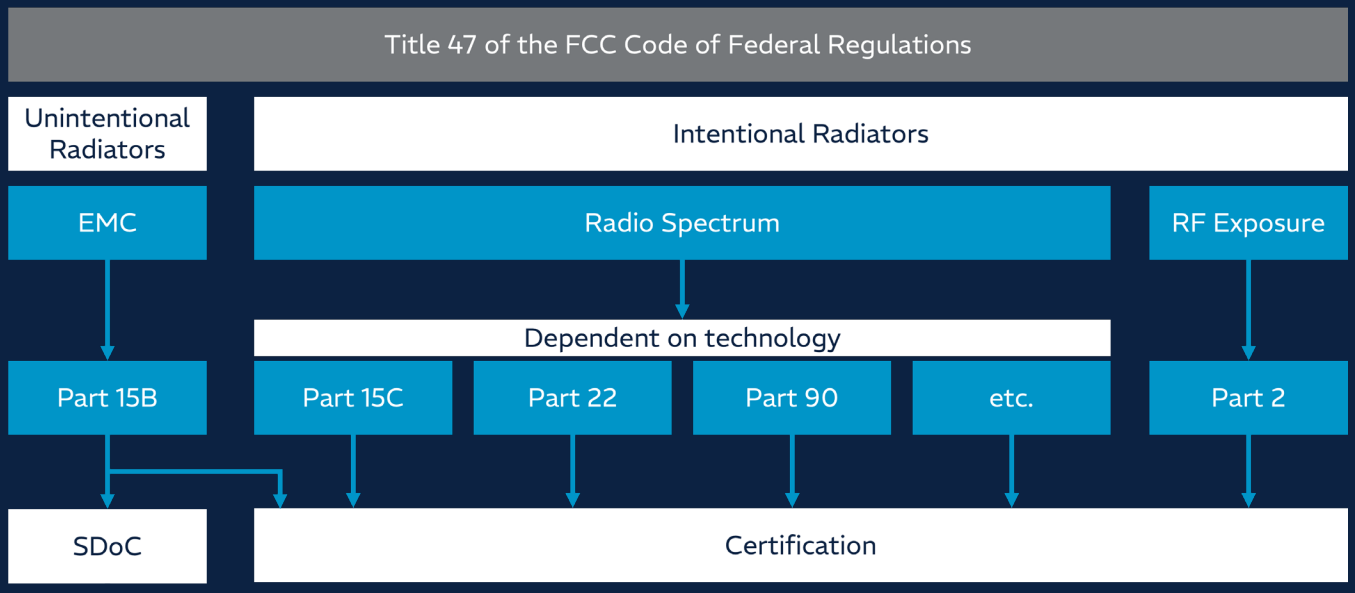

Figure 4. FCC approval routes for wireless devices.

Unintentional radiators are often authorized under Part 15B through a Supplier's Declaration of Conformity (SDoC), while intentional radiators must go through certification.

FCC SDoC should not be confused with the European declaration of conformity. In the US, SDoC is a defined authorization route with specific testing and documentation requirements. Certification, by contrast, results in a formal authorization to market the product based on reviewed evidence submitted through an approved process.

Part 15B EMC requirements can also be routed through certification if desired, although certification is not mandatory for unintentional radiator functions.

Compared with the EU, the FCC places less emphasis on EMC immunity and broad receiver performance. Its framework is more focused on emissions and transmitter-related compliance, though some receiver-related requirements still apply. Even so, product testing remains essential.

THE CANADIAN FRAMEWORK: ISED APPROVAL ROUTES

Canada's ISED framework, shown in **Figure 5**, is structurally very similar to the FCC system. Intentional radiators must meet radio spectrum and RF exposure requirements, while unintentional radiators must meet EMC emissions requirements.

One practical difference is that, in Canada, unintentional radiators cannot go through certification and must use the SDoC route. Otherwise, the overall logic is broadly aligned with the FCC system.

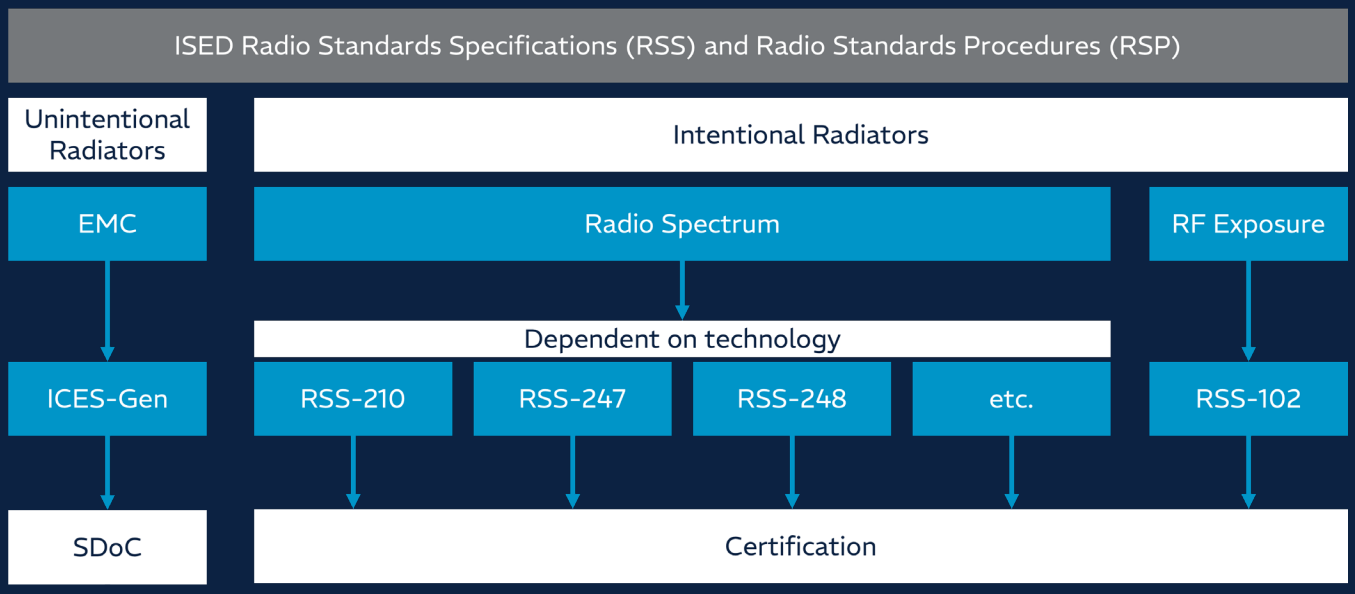

Figure 5. ISED approval routes for wireless devices.

The approval process, however, differs in important ways. In Canada, recognized certification bodies can issue certificates for equipment subject to certification, but a product is not approved for the Canadian market until it appears on ISED's public Radio Equipment List (REL)[4]. This creates a slightly different process flow from the FCC system and often affects timing of a product launch.

For companies planning launches in both countries, these differences can directly affect timelines and market readiness.

WHERE FCC AND ISED ALIGN TECHNICALLY

Despite procedural differences, FCC and ISED requirements often align closely at the technical level. A good example is FCC Part 15.247[5] and Canada's RSS-247[6]. Both apply to products operating in similar frequency bands, including many Wi-Fi-related applications, even if the terminology differs slightly.

In many cases, power limits, band allocations and general technical expectations are closely matched across the two countries. There are still differences to watch for, but from a testing standpoint there is often substantial common ground.

For manufacturers, this can simplify planning and reduce duplication of effort, provided the remaining differences are tracked carefully.

TEST LABS, CERTIFICATION BODIES AND PUBLIC LISTINGS

In both the US and Canada, manufacturers must use recognized or accredited test laboratories, as applicable to the device type and authorization route. FCC[7] and ISED[8] databases identify laboratories recognized for the relevant testing.

Approved certification bodies are also needed for certification work, and likewise there are FCC[9] and ISED[10] databases which may be checked.

Under the FCC system, the certification body issues the certificate on behalf of the FCC. In Canada, a recognized certification body may issue the certificate, while ISED maintains the broader certification framework and public equipment listing requirements. This affects both process flow and timing.

The FCC Grant of Equipment Authorization is the certificate tied to an FCC ID. It identifies the issuing body, applicant, product, applicable rule parts and key operating parameters such as frequency range and output power. It is not just a label; it is the formal evidence that the product may be marketed in the US, provided the stated conditions are met. It may also include notes or restrictions that become especially important later, particularly for modular radios.

In Canada, products appear on the ISED Radio Equipment List. The public listing is an important confirmation of market status, but manufacturers and integrators may still need to review the underlying certification documents to confirm applicable conditions or limitations.

These details may seem administrative, but they have real practical implications. They affect how approval status is verified, how module conditions are interpreted and when a product can actually be marketed.

WIRELESS COEXISTENCE AND FUNCTIONAL WIRELESS PERFORMANCE

For medical devices, one additional North American consideration is wireless coexistence. If a device has functional wireless performance, wireless coexistence testing becomes necessary in the FDA context. Functional wireless performance means the wireless link is essential to the medical function of the device, not simply convenient for data transfer.

A clear example is remote monitoring from a nurse station. If a dropped wireless link prevents critical patient data from reaching clinicians, the wireless function has direct implications for patient safety.

In these cases, wireless coexistence testing evaluates how the device performs in the presence of real wireless signals. Unlike standard immunity testing, which often uses continuous-wave (CW) interferers or interferers with very simple modulation, coexistence testing simulates more realistic radio environments and may even use real products which the device may encounter in practice.

The assessment is tiered according to risk, and manufacturers must define key performance indicators for the wireless link, such as throughput, continuity or other thresholds that determine whether performance remains acceptable under interference conditions.

For connected medical devices, this adds an important layer to North American test expectations and reinforces that regulatory planning must account for the clinical role of the wireless link, not just the presence of radio hardware.

In the US and Canada, wireless medical device approvals rely on formal FCC and ISED processes built around the distinction between intentional and unintentional radiators. Compared with Europe, these systems generally place less emphasis on EMC immunity and broad receiver-performance requirements, but they still rely on accredited testing and structured approval pathways.

At the same time, FCC and ISED requirements often align technically, which can help reduce duplication in test planning. For medical devices with functional wireless performance, wireless coexistence adds an important patient-safety dimension. Overall, while the US and Canadian frameworks may involve less testing in some areas than Europe, they still require careful planning.

CHAPTER 4
Test Readiness and Preparing Wireless Medical Devices for the Lab

Once the regulatory framework is understood, the next step is preparing the product for lab testing. Wireless medical device testing requires specific operating modes, supporting equipment, interfaces and documentation.

If these are not ready at the start of testing, the program can be delayed, and the manufacturer may need to rework the sample, return later and re-enter the queue. Test readiness is therefore a critical part of the overall compliance process.

EMC READINESS: TRANSMIT MODE, IDLE MODE AND LINK MONITORING

For EMC testing, two elements are especially important: firstly having both a transmit mode and an idle mode available; and secondly having a way to monitor the radio link.

Wireless EMC immunity testing must verify both correct operation and the absence of unintended transmission. For that reason, the lab typically needs to test the product in at least two states: an active transmission mode, in which the radio performs its intended function, and an idle or receive mode, in which the radio remains powered and available but is not intended to transmit.

This distinction is important because simply powering down the radio does not show whether unintended transmission could occur. A powered-off radio cannot transmit at all. The lab therefore needs the radio to remain powered, but not intentionally transmitting, in order for any potential unintended transmission to be detected.

A companion device is also required so the lab can verify whether data is still being transmitted or received correctly during immunity testing.

For Bluetooth or Wi-Fi products, this may be relatively straightforward if both the device under test and a companion device can be placed in the test chamber. For cellular devices, the setup is often more complex and may rely on a repeater arrangement, in which a rooftop antenna receives the live cellular network, brings that feed into the test chamber and allows the device under test to communicate with the real network. Performance can then be verified by confirming that data reaches the intended back-end system.

Monitoring criteria must also be defined in advance. If throughput falls below an acceptable level, error rates rise beyond a defined threshold or required performance is otherwise lost, the device may no longer be operating as intended.

TRANSMITTER TEST PREPARATION

Transmitter testing places specific demands on both the sample and its operating controls.

As shown in **Figure 6**, preparation typically depends on six practical requirements.

Figure 6. Key practical requirements for transmitter test preparation.

First, the device should be capable of being fixed to a selectable channel and ideally to maximum power. This is essential for tests such as frequency stability, bandwidth and power spectral density. A radio that continues hopping unpredictably across channels cannot be assessed in a controlled and repeatable way for many of these parameters.

Second, it is highly desirable for the transmitter to support continuous transmission both with and without modulation. Some tests require the device to send realistic or pseudo-random data, while others are better performed using a constant unmodulated tone.

Third, the test strategy must account for all intended antenna configurations. If only one antenna is planned, the scope is simpler. If multiple antenna types or gains will be used, the strategy must reflect that, since changes in antenna type or gain can significantly affect performance. A common approach is to assess one example of each antenna type at the highest intended gain.

Fourth, the lab may need conducted test fixtures. Conducted testing, in which the device is physically connected to the test equipment rather than measured over the air, is often preferred because it is more repeatable, carries lower measurement uncertainty and can be quicker and less expensive, especially for receiver testing. If the product does not have an accessible antenna connector, temporary hardware modification may be required, such as cutting PCB traces and adding a temporary connector.

Fifth, selectable modulation modes and bandwidths are important. A device that supports multiple modes may behave differently depending on the chosen modulation scheme or bandwidth, so the lab needs a way to place the product into each relevant operating state.

Sixth, suitable power supply options must be available. For mains-powered products, this is usually straightforward. For battery-powered devices designed for very low duty-cycle operation, however, the battery may not last if the device is forced into continuous transmission for a long test sequence. In those cases, the manufacturer may need replacement samples, multiple batteries or an alternative powered arrangement, such as a temporary DC supply. Even this can in turn create its own complications, such as potential overheating.

Together, these requirements show that transmitter testing depends on preparation well before the sample reaches the lab.

RECEIVER TEST PREPARATION

Receiver testing adds further requirements beyond those needed for transmitter evaluation and is often performed using conducted test fixtures for repeatability and control.

As with EMC testing, a companion device is required to provide the wanted signal from the other end of the communication link, whether that is a laptop, phone or another system normally used with the device.

The lab also needs a clear indication of whether reception is successful. Many receiver standards quantify success using packet error rate, bit error rate or block error rate. The test setup must therefore allow the lab to determine how many transmissions were correctly received and how many were lost or corrupted.

This indication can take several forms, including direct output of received data, a displayed error count or even a simple visual cue such as an LED response to each successfully received packet. What matters is that receiver performance can be measured quantitatively enough to assess sensitivity and blocking behavior.

DOCUMENTATION AND DECLARATION FORMS

Test readiness is not only about hardware and operating modes. Documentation also matters, including declaration forms required under certain European Telecommunications Standards Institute (ETSI) standards.

Examples include ETSI EN 300 328 V2.2.2 (2019-07)[11] and ETSI EN 301 893 V2.2.1 (2024-11)[12], both of which include annexes requiring the manufacturer or applicant to provide information needed for assessment. Although this is not documentation on the scale of a medical device submission such as a 510(k), it is still material that must be completed before testing can begin properly.

If the hardware is ready but the required declarations are missing, the lab may not be able to proceed. For that reason, documentation should be prepared in parallel with, or even ahead of, the technical test setup.

Preparing a wireless medical device for formal testing requires more than sending a finished sample to the lab. Successful testing depends on how well the product has been prepared in advance, from operating modes and support equipment to interfaces, monitoring methods and required documentation. When these elements are addressed early, the testing process is easier to manage and less likely to be delayed by rework or missing information. Test readiness is therefore a key part of a successful wireless compliance program.

CHAPTER 5:
Modular Radios, Their Advantages and Their Limits

Modular radios are becoming increasingly important for medical device manufacturers.

When a company wants to add wireless functionality to a previously non-wireless medical device, there are generally two options: design the radio in-house as part of the product architecture or integrate an off-the-shelf radio module, such as a Wi-Fi, Bluetooth or cellular module.

For many manufacturers, the second option is appealing. A prebuilt module can reduce the need for in-house radio expertise and lower development effort. Rather than designing every radio parameter from scratch, the manufacturer can integrate a module that already performs much of the radio function and may already have undergone testing.

A module is not the same as a chipset. A chipset is only one component within a radio design and cannot hold approvals on its own. A radio module is a more complete unit of radio equipment and may carry prior assessments or authorizations. Even so, those approvals do not automatically transfer to the finished product.

For that reason, modular radios are often seen as a way to simplify compliance. However, that simplification can be overstated.

WHY MODULE-LEVEL APPROVAL DOES NOT SETTLE PRODUCT-LEVEL COMPLIANCE

A radio module may come with a CE marking, UKCA marking, FCC ID or ISED ID, depending on the market. This can create the impression that most of the compliance work has already been completed and can simply carry over to the host product. That assumption should be treated carefully.

In practice, module-level approval may reduce some work, but it does not remove the manufacturer's responsibility to assess the final product.

FCC AND ISED MODULE CERTIFICATES: WHAT CAN AND CANNOT BE CARRIED FORWARD

In the US and Canada, modular radio authorizations may sometimes be carried forward, but only under defined conditions. A manufacturer using a module should first confirm whether the module has an existing certificate and, if so, whether that existing module certificate remains valid in the host application. **Figure 7** shows the complete decision pathway, from identifying a radio to determining whether additional certification is required.

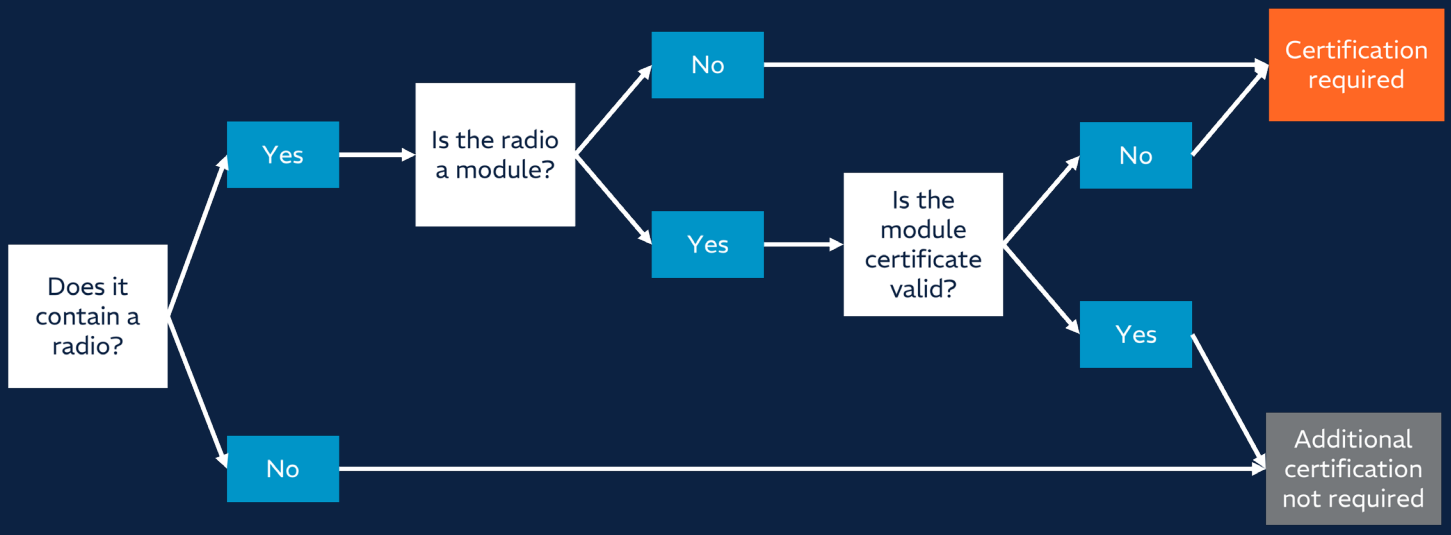

Figure 7. Decision pathway for determining whether additional FCC or ISED certification is required.

If the module certificate remains valid in the host application, additional certification of the host product may not be necessary. If it does not remain valid, further certification work is required. Note that Figure 7 makes no mention of testing. That is because in either case above, end-product testing is always expected.

This is the key distinction which is often misunderstood. Modular approval can reduce administrative burden by avoiding a new certificate for every host configuration, but it does not eliminate the technical responsibility to verify compliance of the finished product through testing.

HOW GRANT CONDITIONS AFFECT END-PRODUCT COMPLIANCE

A key practical issue when integrating a radio module is the set of conditions attached to its original approval. In some cases, a limited modular approval may include requirements such as:

- the antenna must be installed at least 20 cm from all persons
- users must be given instructions needed to maintain RF exposure compliance
- only identical antenna types with the same or lower gain may be used

These are not minor details. They define the valid scope of the approval. If the host application breaks any of these conditions, the answer to the third question in Figure 7 is 'No', and the original module certificate can no longer be relied upon.

For wireless medical devices, this is especially important because the final product may be used close to the body or under operating conditions different from those assumed in the original module approval. A module approved for one RF exposure scenario may not remain valid when integrated into a wearable, portable or patient-facing device.

WHY THE INTEGRATED PRODUCT STILL NEEDS TESTING

FCC guidance (see FCC KDB 996369 D04[13]) strongly recommends that host product manufacturers test the transmitter in the host configuration, even when the module has already been certified. The reason is straightforward: the module was typically tested in isolation, not in the presence of the host product's circuitry, enclosure materials,

PCB structures or antennas. Once integrated, its emissions profile may change.

Host testing is therefore not just about whether the finished product passes or fails. It is also about comparing host behavior with standalone module behavior to determine whether integration has introduced meaningful changes.

In this sense, modular approval may reduce certification administration, but it does not remove the end-product manufacturer's responsibility to verify and demonstrate compliance of the integrated device.

In this sense, modular approval may reduce certification administration, but it does not remove the end-product manufacturer's responsibility to verify and demonstrate compliance of the integrated device.

WHY MODULAR APPROVAL DOES NOT APPLY UNDER CE OR UKCA MARKING

The position in Europe and the UK is in some ways more straightforward. As shown in **Figure 8,** if the end product is radio equipment, RED applies. Whether the radio function comes from a module or is designed directly into the product does not change that legal position.

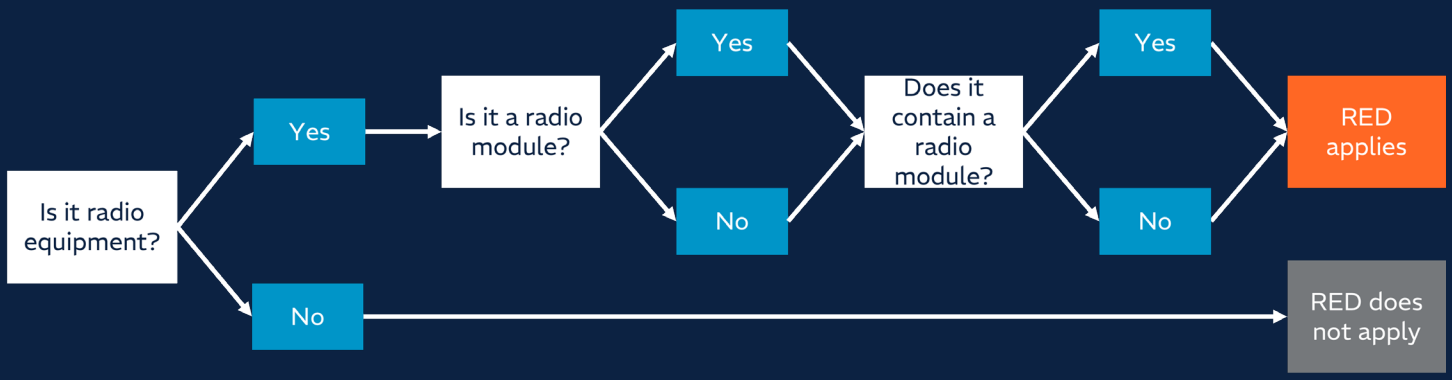

Figure 8. Radio modules for CE/UKCA. RED applicability depends on whether the end product is radio equipment, not on whether the radio function comes from a module.

There is no modular approval concept under CE marking or UKCA marking in the same sense as under FCC or ISED rules. A supplier may claim that a module is CE compliant, but even so no such modular approval mechanism exists. In practice, that claim only means the module was tested and found compliant under its own assessment conditions.

For the manufacturer of the finished product, there is therefore no legal approval to carry forward. The end-product manufacturer remains fully responsible for demonstrating compliance of the radio equipment placed on the market.

WHY MODULE TEST REPORTS STILL MATTER IN EUROPE

Although there is no modular approval route to carry forward under CE or UKCA, module test reports are still highly valuable. Manufacturers should obtain these reports rather than relying only on a supplier's statement that the module was tested.

These reports provide the baseline evidence for assessing the integrated host product. European guidance, including ETSI Guide 203 367[14], supports reassessment of the combined equipment against Article 3.2 of RED when the conditions of use differ from the original assessment conditions. The guidance in this document also closely aligns with the FCC's guidance document linked above.

This allows the host integrator to take a pragmatic, evidence-based approach. Rather than starting over, the manufacturer can compare performance in the host environment with the original module data. If the results align closely, there may be a reasonable basis to conclude that the original test evidence remains representative. If not, additional reassessment is needed.

Again, the core principle is that the manufacturer of the finished product owns the compliance decision.

Modular radios can simplify wireless product development, but they do not remove responsibility for end-product compliance. In the US and Canada, existing module certificates may sometimes be carried forward if all approval conditions remain valid, but host testing is still strongly recommended and may be critical in practice.

In the EU and UK, there is no legal modular approval concept to carry forward. In all cases, the manufacturer of the finished medical device remains responsible for demonstrating that the integrated product is compliant.

KEY TAKEAWAYS

Wireless functionality is redefining medical devices across the healthcare ecosystem, from implantables and portable systems to wearables and hospital consumables. As radio technologies become more embedded in these products, manufacturers face a broader set of regulatory and testing obligations.

Adding wireless capability does more than introduce a few additional radio tests. It can change the product's regulatory status, bringing new requirements related to safety, RF exposure, EMC, spectrum use and, in some cases, coexistence or other market-specific considerations.

In the EU and UK, compliance is generally shaped by RED and related legislation. In the US and Canada, it follows FCC and ISED approval pathways. While the frameworks differ, the practical lesson is consistent across regions: early regulatory planning is critical.

Test readiness is just as important. Manufacturers must prepare test modes, companion devices, antenna configurations, power strategies and documentation before lab work begins. These are essential requirements that can determine whether testing proceeds efficiently or is delayed.

Modular radios may simplify development and reduce some certification burden, but they do not remove responsibility for the final product. Under FCC, ISED, CE and UKCA frameworks, the manufacturer placing the device on the market remains accountable for demonstrating compliance.

For medtech companies, the main lesson is clear: wireless functionality should be treated as a strategic compliance decision from the earliest stages of design. When regulatory planning, engineering and test preparation are aligned early, connected medical devices are far more likely to reach market efficiently and confidently.

REFERENCES

1. Xtalks. *Understanding the testing and compliance requirements for wireless medical devices.* Xtalks webinar. Accessed March 30, 2026.

2. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC. (2014). *Official Journal of the European Union, L* 153, 62–106.

3. European Telecommunications Standards Institute. *Electromagnetic compatibility (EMC) standard for radio equipment and services (EN 301 489 series)*. ETSI.

4. Title 47 of the Code of Federal Regulations, § 15.247. *Operation within the bands 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz.* Electronic Code of Federal Regulations.

5. Innovation, Science and Economic Development Canada. (2023, August). *RSS-247, issue 3: Digital transmission systems (DTSs), frequency hopping systems (FHSs) and licence-exempt local area network (LE-LAN) devices.* Government of Canada.

6. Innovation, Science and Economic Development Canada. *Radio equipment list (REL).* Government of Canada.

7. Federal Communications Commission. *Equipment authorization system test firm search.* Office of Engineering and Technology. FCC.

8. Innovation, Science and Economic Development Canada. *Wireless device testing laboratories.* Government of Canada.

9. Federal Communications Commission. *Telecommunications certification body search.* Office of Engineering and Technology. FCC.

10. Innovation, Science and Economic Development Canada. *Certification bodies.* Government of Canada.

11. European Telecommunications Standards Institute. (2019, July). *EN 300 328 V2.2.2: Wideband transmission systems; Data transmission equipment operating in the 2.4 GHz band; Harmonised standard for access to radio spectrum.* ETSI.

12. European Telecommunications Standards Institute. (2024, November). *EN 301 893 V2.2.1: 5 GHz WAS/RLAN; Harmonised standard for access to radio spectrum.* ETSI.

13. Federal Communications Commission. *996369 Modules, Module Certification, 15.212.* Office of Engineering and Technology Knowledge Database. FCC.

14. European Telecommunications Standards Institute. (2016, January). *EG 203 367 V1.1.1: Guide to the application of radio and EMC tests to multi-radio and combined radio and non-radio equipment.* ETSI.

HOW CAN ELEMENT HELP?

With combined capabilities in electrical safety, EMC, radio and RF exposure testing, medical software, risk management, and clinical evaluation, Element delivers a unified testing experience. A single technical partner reduces complexity, improves coordination across disciplines, and accelerates time-to-market for connected medical devices.

Element can help in three main ways:

1. COMPREHENSIVE COMPLIANCE ACROSS CONNECTED MEDICAL TECHNOLOGIES

We have an Advisory Services department which can help you to understand the challenges facing a manufacturer of radio equipment.

Element provides integrated support across IEC 60601 electrical safety, EMC, wireless and radio compliance, software, usability, and clinical validation. By addressing safety, essential performance, connectivity, and real-world use in parallel, manufacturers can reduce risk, avoid re-testing, and maintain compliance as devices become increasingly connected.

2. SUPPORTING GLOBAL MARKET ACCESS

Element helps manufacturers access markets across Europe, North America, Asia, and beyond through globally coordinated testing, certification, and regulatory strategy. Support includes EU MDR and RED pathways, FDA and Health Canada submissions, FCC and ISED approvals, and the IECEE CB Scheme to reduce duplicate testing across international markets. By aligning regional requirements early, Element helps manufacturers scale efficiently and confidently into new geographies.

Our labs in the USA, EU, UK and Korea have ISO 17025 accreditation for a wide range of RED test standards but we also understand that new standards, such as those which are often listed with restrictions, require deviations and testing outside of the normal accreditation scope.

3. ACCREDITATIONS, EXPERTISE, AND REGULATORY PATHWAY ACCELERATION

We are an ISO 17065 accredited Notified Body to the RED.

Element operates a global network of ISO 17025 accredited laboratories, NRTL facilities, FCC and ISED certification bodies, and Notified Body capabilities for RED, supporting comprehensive and recognized conformity assessments. With experienced technical specialists and regulatory teams, Element accelerates approvals through EU MDR, FDA pathways including ASCA-supported testing, and other global schemes. This depth of accreditation and expertise enables faster regulatory acceptance, fewer submission delays, and a more reliable route to global commercialization.

RELATED SERVICES

- Advisory services
- Pre-compliance testing
- Safety testing (IEC 60601 & 61010)
- Wireless medical testing
- EMC testing
- Battery testing
- Medical software testing
- Clinical Validation
- Certification (FDA ASCA, FCC, Health Canada, ISED, MDR)
- NRTL accredited laboratories (US and UK)
- Global Market Access

element

Scan to find out more.

WHY CHOOSE ELEMENT?

Element Connected Technologies & Mobility, is a leading provider of testing, inspection, and certification services for connected devices and mobility solutions.

We provide comprehensive testing and certification services that ensure products meet international standards for connectivity, interoperability, and safety.

CONTACT

Our LinkedIn

Telephone: +44 (0) 808 234 1667 Web: element.com Email: contact.us@element.com

Making tomorrow safer than today.

CONNECTED TECHNOLOGIES