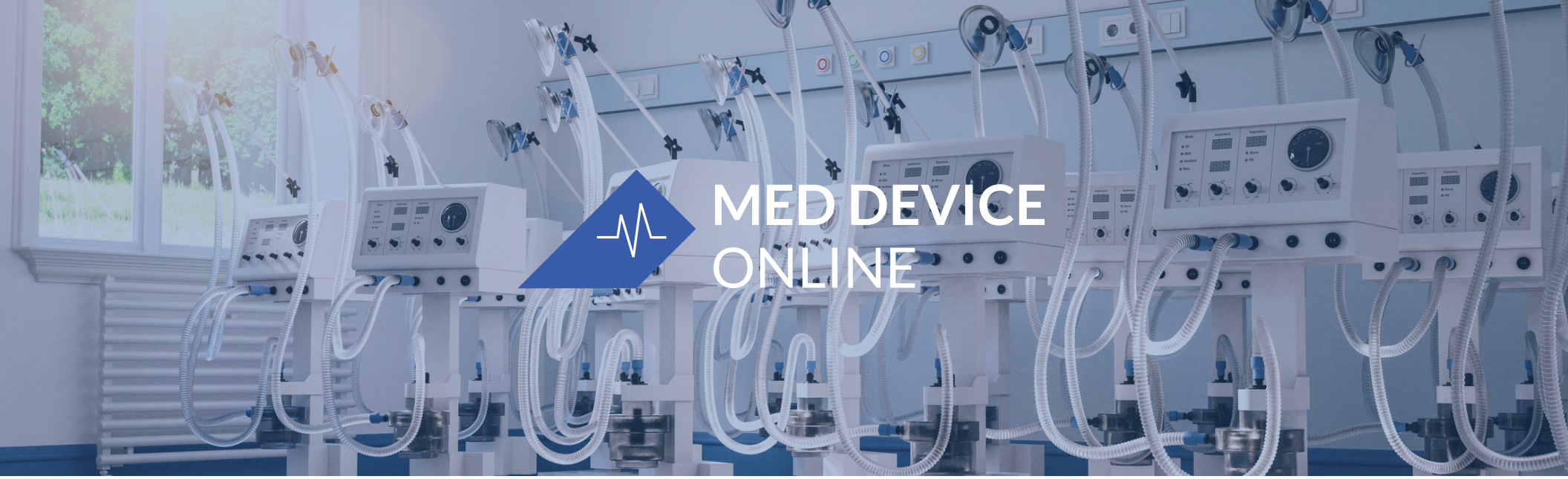
MED DEVICE
ONLINE

NAVIGATING THE NEW LANDSCAPE OF EUROPEAN MEDTECH REGULATIONS



MED DEVICE ONLINE

The EU's Medical Device Regulation (MDR, effective May 26, 2021) and the In Vitro Diagnostics Regulation (IVDR, effective in May 2022) are certainly hurdles for medical device manufacturers to tackle. However, those aren't the only new regulations in Europe to prepare for.

This collection of articles begins with lessons learned regarding economic operator responsibilities, overall quality management system considerations, and common challenges during EU MDR and EU IVDR implementation to ensure a smooth transition and avoid pitfalls during implementation. The second article focuses on typical challenges experienced during the technical documentation assessments conducted by the notified bodies. The e-book then moves on to examine the role of the contract manufacturer under both the MDR and IVDR before explaining how to navigate the MDR's clinical data requirements.

Since Brexit was finalized on January 1, 2021 — due to the pandemic's odd nature of lengthening our view of time, January seems so long ago, doesn't it? — all medical devices must be registered with the Medicines and Healthcare products Regulatory Agency. The next article in this e-book provides 10 actions to prepare for the UK's conformity assessment.

The e-book wraps up with a thorough exploration of the 2020 guide on digital health application requirements from Germany's Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM, or the Federal Institute for Drugs and Medical Devices). You'll need to follow these requirements in order to make your digital health applications available to the more than 73 million participants in the German statutory health insurance. Other nations will likely follow in Germany's footsteps, so it's best to get ahead of these requirements when you can.

MED DEVICE ONLINE

CONTENTS

IMPLEMENTING EU MDR AND IVDR: LESSONS LEARNED, PART 1

Marcelo Trevino

Global VP, Regulatory Affairs & QA, Agendia

The transition to the EU's Medical Device Regulation (MDR) and In Vitro Diagnostic Regulation (IVDR) is not an easy undertaking. As many changes need to be made in the quality system and business processes to meet the new regulations, some organizations are experiencing challenges in implementing and demonstrating compliance to their notified bodies. To start, organizations need to ensure that their devices have the accurate certificate scopes and that current certificates can be maintained until expiration. Several significant important aspects that require sound planning and significant oversight include new quality management system (QMS) and technical documentation requirements.

This is the first article in a two-part series. This article highlights the sections that need close attention regarding economic operator responsibilities, overall QMS considerations, and common challenges during EU MDR and EU IVDR implementation to ensure a smooth transition and avoid pitfalls during implementation. The second article will focus on typical challenges experienced during the technical documentation assessments conducted by the notified bodies.

ECONOMIC OPERATORS' RESPONSIBILITIES ACROSS THE SUPPLY CHAIN

Accountability across economic operators is significantly increased and summarized in the table below:

	Manufacturer	Authorized Representative	Importer	Distributor	Assembler
EUDAMED Registration	X	X	X		
Technical Documentation	X	X	X		X
Design, Development, Manuf, or Assembly	X				X
Handling, Storage, & Distribution	X		X	X	X
Nonconformities	X	X	X	X	X
Field Safety Corrective Actions	X	X	X	X	X
UDI/Labeling	X	X	X	X	X
Complaints	X	X	X	X	X
Post-Market Surveillance	X	X		X	X
Responsible Person	X	X			

Information related to the economic operator (type), contact details, and basic Unique Device Identification-device identifier (UDI-DI) information (risk class, notified body information) must be well defined. EU MDR and EU IVDR require assigning a basic UDI-DI to the device and providing it to the UDI database together with other core elements. Additionally, manufacturers need to verify in the European database on medical devices (EUDAMED) that the information is accurate and up to date.

The new regulations require the European Commission to manage an electronic system to create a single registration number (SRN) that identifies manufacturers, authorized representatives, and importers. The Member States maintain the registration of distributors of devices that have been made available in their territory. Importers are required to verify that the manufacturer or authorized representative has provided the required information to the electronic system and notify the authorized representative or manufacturer of any discrepancies. SRNs are obtained from the competent authorities and are used to apply for conformity assessment with a notified body and to access EUDAMED. Data is accessible by the public and is used by the competent authority to determine required fees. Data must be updated regularly and verified for accuracy to comply with the regulation.

It is also important to keep in mind that initial audits must be done at least partially on-site. This has become challenging due to current COVID-19 restrictions; however, manufacturers need to begin contingency plans and formalize agreement with their notified bodies to address this situation. MDCG 2020-4 provides guidelines on addressing this time-limiting factor; read my article here for discussion on this topic.

QMS REQUIREMENTS THAT REQUIRE CAREFUL REVIEW AND CONSIDERATION

New documentation and record-keeping requirements: Many existing procedures need to be updated, starting with the quality manual, which must reference the new regulations, new common specifications, and standards. If an intended purpose needs to be adjusted, the Medical Device File and other documents will also need to be updated. New record retention requirements shall also be assessed for all devices.

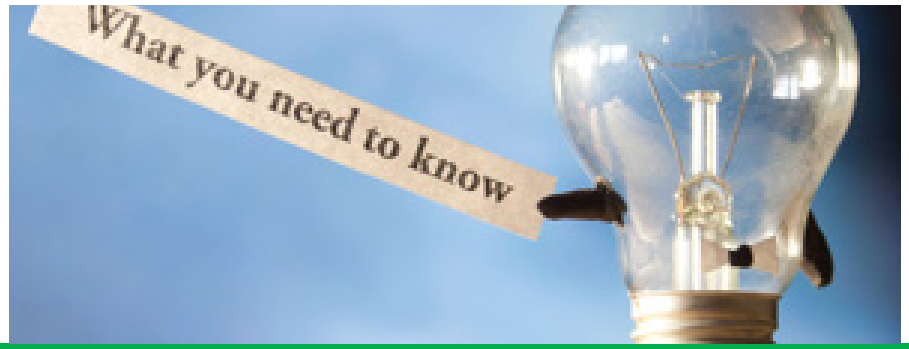
According to Article 10 of both EU MDR and EU IVDR, manufacturers shall keep the technical documentation, the EU declaration of conformity, and, if applicable, a copy of the relevant certificate, including any amendments and supplements — issued in accordance with Article 56 for MDR and Article 51 for IVDR — available for the competent authorities for a period of at least 10 years after the last device covered by the EU declaration of conformity has been placed on the market.

Person responsible for regulatory compliance: Manufacturers and authorized representatives shall have available within their organization at least one person responsible for regulatory compliance who possesses the requisite expertise in the field of medical devices or in vitro diagnostic devices, as applicable. The specific expertise and qualification requirements can be found in Article 15 of EU MDR and Article 15 of EU IVDR.

Strategy for regulatory compliance: A strategy for regulatory compliance that includes how the organization will comply with conformity assessment procedures and how it will manage modifications to the devices must be in place. This strategy shall also include processes for identification of relevant legal requirements, qualification, classification, and handling of equivalence. Quality plans outlining the IVDR transition and the plans for updating the quality system or the technical documentation can demonstrate compliance with this requirement. Establishing continual improvement processes implemented according to Article 10 of EU MDR and EU IVDR should also be taken into consideration as part of the strategy for regulatory compliance.

Implant card: Requirements are outlined in Article 18 of EU MDR.

UDI: Requirements are outlined in Article 27 and Annex VI of EU MDR and Article 24 and Annex VI of EU IVDR.



New plans and strategies: The table below summarizes the plans required by MDR and IVDR that are subject to QMS audits and technical review assessments:

MDR	IVDR
Strategy for Regulatory Compliance – Article 10 & Annex IX	Strategy for Regulatory Compliance – Article 10 & Annex IX
Risk Management Plan – Annex I	Risk Management Plan – Annex I
Clinical Development Strategy – Article 61	
Clinical Evaluation Plan – Annex II, Annex IX, Annex XIV, Annex XV	Performance Evaluation Plan – Annex IX, Annex XIII
Clinical Development Plan – Annex XIV	Clinical Performance Study Plans – Annex XIII, Annex XIV
Clinical Investigation Plan – Annex XV	Clinical Performance Study Plans – Annex XIII, Annex XIV
Post-Market Surveillance Plan – Annex III	Post-Market Surveillance Plan – Annex III
Post-Market Clinical Follow-Up Plan – Annex XIV	Post-Market Performance Follow-Up Plan – Annex XIII

Clinical evaluation applicable to EU MDR: Article 61 indicates that for all class III devices and class IIb devices intended to administer and/or remove a medicinal product, the manufacturer may, prior to clinical evaluation or investigation consult an expert panel about its clinical development strategy. The manufacturer shall give due consideration to the views of the expert panel. This consideration shall be documented in the clinical evaluation report.

Summary of safety and performance: For implantable devices, class III devices, and in-vitro diagnostic devices class C and class D, manufacturers are required to write up a summary of safety and clinical performance in a way that is clear to the intended user and the patient. Notified bodies are required to review and submit this information to EUDAMED to make it available to the public. There are several requirements to be included by manufacturers in this summary, such as: basic UDI-DI information, SRN, device description and purpose, reference to harmonized standards, a summary of clinical and/or performance evaluation, relevant information on post-market follow-up, suggested training for users and information on residual risks, undesirable effects, warnings, and precautions, among other aspects. For in vitro diagnostic devices, metrological traceability of assigned values is also to be included in this summary.

TYPICAL CHALLENGES WITNESSED DURING IMPLEMENTATION

Organizations must keep in mind that at the time of a QMS assessment to the MDR or IVDR, the quality management systems must be established, documented, and operational (where practical) for all device groups according to EU MDR and EU IVDR Article 10: *General obligations of manufacturers*. There are many requirements that notified bodies must carefully review now that could end up in non-conformances if they are not properly implemented. For example:

A STRATEGY FOR REGULATORY COMPLIANCE, INCLUDING COMPLIANCE WITH CONFORMITY ASSESSMENT PROCEDURES AND PROCEDURES FOR MANAGEMENT OF MODIFICATIONS TO THE DEVICES COVERED BY THE SYSTEM

It is common for organizations to inadvertently define a strategy for regulatory compliance that does not cover all the product types subject to the regulation or all the conformity assessment routes. To avoid a non-conformance here, it is important to conduct a thorough assessment to confirm that the strategy encompasses all applicable products in the scope of certification.

Additionally, being able to demonstrate control and monitoring of economic operators within the entire supply chain can be a regulatory compliance challenge during an audit. This can be successfully accomplished through documented quality agreements that outline new responsibilities for distributors, importers, assemblers, and authorized representatives but it's important that they are formalized prior to an assessment. Each economic operator shall be able to check compliance of all the others involved. For example, distributors must verify the CE mark and EU declaration of conformity, labeling, instructions for use (IFU), and UDI; importers should be able to verify designated authorized representative and maintain details on labeling/packaging, while authorized representatives must verify technical documentation and conformity assessment from the manufacturer and have access to the declaration of conformity and technical documentation.

IDENTIFICATION OF APPLICABLE GENERAL SAFETY AND PERFORMANCE REQUIREMENTS AND EXPLORATION OF OPTIONS TO ADDRESS THOSE REQUIREMENTS

Organizations must conduct an impact assessment of new safety and performance requirements across the entire quality system and not manage them as isolated requirements. For example, risk management documentation must include the impact of these requirements, including mitigation activities.

RESOURCE MANAGEMENT, INCLUDING SELECTION AND CONTROL OF SUPPLIERS AND SUBCONTRACTORS

Qualifications and experience for the person responsible for regulatory compliance must be defined, and records supporting these criteria shall be available. If notified bodies cannot verify this information or conclude that the qualifications/experience are inadequate, the company would not be able to comply with this requirement. In addition to having the documentation available, organizations need to be able to demonstrate that the person responsible for regulatory compliance is permanently and continuously available to support them; this can be managed through a documented agreement in the case of subcontractors, but it is important to not lose sight of this requirement.

Additionally, it is important to show allocation of resources for transition and post-transition requirements in post-market surveillance and to ensure that the legal manufacturer holds all the technical documentation for the devices. This can be demonstrated through quality management review minutes and other records demonstrating resource management is being considered at senior levels in the organization.

RISK MANAGEMENT AS SET OUT IN IN SECTION 3 OF ANNEX I

Risk management cannot be implemented as an isolated process. To successfully demonstrate that risk management is properly implemented, conclusions from risk management must link to clinical performance data. Claims in the IFU must link to the scientific validity and the analytical and clinical performance data, which should also be referenced in the performance evaluation report (PER). It is important that organizations properly address benefit-risk on all hazards and that there is a clear understanding of the concept of hazard vs. harm.

FOR IVDR: PERFORMANCE EVALUATION, IN ACCORDANCE WITH ARTICLE 56 AND ANNEX XIII, INCLUDING POST-MARKET PERFORMANCE FOLLOW-UP (PMPF)

A PMPF is used to confirm safety and validity of a device on the market. If it is confirmed during performance evaluation and risk management activities that the device is safe, PMPF studies are not required, unless issues are revealed from post-market surveillance activities. An important aspect of PMPF is to confirm a benefit-risk ratio for the intended purpose of the device has not been adversely affected.

A performance evaluation should be conducted through an objective review and must consider both favorable and unfavorable data. The depth and extent of the evaluation must be proportionate and appropriate to characteristics of the device, including risks, risk class, performance, and intended purpose. The outputs of the evaluation should lead to a plan for PMPF. If it is concluded that PMPF studies are not needed, this must be justified in the PER.

The performance evaluation shall be a continual process driven by a performance evaluation plan. The intended use is important and critical for setting the clinical evidence required, and scientific validity should link to the claims being made. This is required for all IVD devices, even if devices have been in the market for a long time. Articles 10 and 56 and Annex XIII of the IVDR address all the specific requirements.

VERIFICATION OF THE UDI ASSIGNMENTS MADE IN ACCORDANCE WITH ALL RELEVANT DEVICES AND ENSURING CONSISTENCY AND VALIDITY OF INFORMATION PROVIDED

Organizations need to ensure that the UDI can be verified throughout the supply chain. Additionally, they need to verify that it is included in all the required locations, such as, for example, technical documentation, declaration of conformity, implant card, labeling/packaging, and vigilance reports. A UDI guidance document is available; however, it is mainly focused on medical devices. Therefore, it is important for in-vitro diagnostic manufacturers to assess whether self-tests, near patient tests, companion diagnostics, and class D devices need to implement UDI requirements.

SETTING UP, IMPLEMENTING, AND MAINTAINING A POSTMARKET SURVEILLANCE SYSTEM

Post-market surveillance shall be considered over the full product life cycle, such as design, manufacturing, shelf-life, lifetime, and disposal. Procedures should be implemented for post-market surveillance and post-market performance follow-up (for IVDR), with specific frequency requirements for each device class. Vigilance reporting requirements include implementation of systems for serious incidents, field safety corrective actions, and trend reports.

Organizations must have procedures in place to address reporting requirements, including sound statistical methodologies for monitoring vigilance trends. For example, serious public health threats must be reported within two days, death or unanticipated serious deterioration in the state of health must be reported within 10 days, and any other incidents within 15 days.

Periodic Safety Update Reports (PSURs) and Summary of Safety and Clinical Performance (SSCP) are mandatory reports that must be submitted at different frequencies as summarized below:

Device	Periodic Safety Update Report (PSUR	Summary of Safety and Clinical Performance (SSCP)
Class I	PMS report updated when necessary	
Class IIa	As necessary; at least every 2 years	
Class IIb	Annual	
Class IIb Implantable	Annual to Notified Body through EUDAMED	Annual to Notified Body through EUDAMED
Class III	Annual to Notified Body through EUDAMED	Annual to Notified Body through EUDAMED
IVD A		
IVD B		
IVD C		As soon as possible, where necessary
IVD D		As soon as possible, where necessary

Organizations shall verify that procedures are updated to ensure these activities take place at the required frequencies and that agreements with all applicable economic operators are updated accordingly to avoid potential non-conformances.

Medical device organizations are now required to have several systematic processes that are subject to many new EU requirements, which focus mainly on safety and performance. Economic operators across the entire supply chain must apply faster product development cycles, maintain quality, and remain compliant with industry regulations. While there are many new specific requirements that could be inadvertently missed and a significant number of resources are needed to implement the new requirements, organizations can benefit from following guidelines and by adequately organizing data in their quality management system to provide a clear correlation of the regulation requirements and how the organization complies with them for each device. Additionally, preparing and organizing the technical documentation needed for EU MDR and EU IVDR compliance have their own unique challenges; the next part of this series will explore them, including some considerations to avoid pitfalls during the notified body assessments.

ABOUT THE AUTHOR

Marcelo Trevino is the global vice president, regulatory affairs and quality assurance at Agendia, a molecular diagnostics company focused on breast cancer genomic testing. He has more than 25 years of experience in quality and regulatory affairs, serving in senior leadership roles with different organizations while managing a variety of medical devices: surgical heart valves, patient monitoring devices, insulin pump therapies, surgical instruments, orthopedics, and medical imaging/surgical navigation, amongst others. He has an extensive knowledge of medical device management systems and medical device regulations worldwide (ISO 13485:2016, ISO 14971:2019, EU MDR, EU IVDR, MDSAP). Trevino holds a B.S. in industrial and systems engineering and an MBA in supply chain management from the W.P. Carey School of Business at Arizona State University. He is also a certified Quality Management Systems Lead Auditor by Exemplar Global.

IMPLEMENTING EU MDR AND IVDR: LESSONS LEARNED, PART 2

Marcelo Trevino
Global VP, Regulatory Affairs & QA, Agendia

The first article in this two-part series covered details associated with economic operator responsibilities, overall QMS considerations, and common challenges during implementation of the EU's Medical Device Regulation (MDR) and the EU's In Vitro Device Regulation (IVDR). This article focuses on typical challenges experienced during the technical documentation assessments conducted by the notified bodies.

It is common for organizations to have many legacy devices with long histories under the previous medical device or in vitro diagnostic directives that may have undergone many changes or company acquisitions. Because EU MDR and EU IVDR do not allow grandfathering, all new requirements – including additional information that must be gathered and new required testing – must be presented and explained clearly for the notified body technical reviewers who will be analyzing evidence of compliance in detail. Therefore, proactive preparation is crucial.

Common challenges and key aspects to consider before and during the technical documentation assessments include:

- Tests that were leveraged shall be adequate to comply with current requirements.
- New general safety and performance requirements (GSPRs) that were not in place when the tests or devices were initially launched must be addressed. A GSPR checklist is required and files should provide clear conclusions. The requirements and evidence shall be clearly organized within the technical file (clear data and clear reports).
- Procedures, plans, and templates must be in place even while some EU provisions are not ready, including a plan to monitor the publication of guidance documents and plans in place for implementing all applicable requirements.
- Harmonized standards or common specifications need to be adequately referenced in all applicable documentation, and organizations shall have a system in place to stay up to date with any new revisions to these standards and specifications.

- If a performance evaluation plan covers multiple devices, a conclusion of conformity should cover all devices included in the plans and reports.
- Clinical evidence must be available for all legacy devices and data can be obtained from different sources, such as, for example, clinical performance studies, scientific peer-reviewed literature, and published experience gained by routine diagnostic testing. The clinical performance studies shall be linked to the plan for post-market performance follow-up.
- Evidence of the person responsible for regulatory compliance having oversight of the Summary of Safety and Clinical Performance (SSCP) should be readily available.
- Linkage and consistency between the information in declaration of conformity, the Clinical Evaluation Report, the instructions for use, the SSCP, and risk management shall be established.
- Residual risk linkage between adverse events and potential complications shall be included in the instructions for use.
- A complete set of labels and instructions for use in all the languages accepted in the Member States where the device or tests will be sold shall be available for review.
- The SSCP should reflect performance evaluation and must be updated at least annually for class III and implantable devices. This is also a new requirement for in-vitro diagnostic class C and class D devices; therefore, the guidance document MDCG 2019-9 should be carefully reviewed.
- Evidence confirming that the manufacturer has verified that the portions of the SSCP intended for patients can be read and understood by a person without professional or specialized knowledge in the test or device shall be available.
- A device-specific post-market surveillance plan and post-market clinical follow-up plan (if applicable) shall be available. Manufacturers need to demonstrate these elements are designed to proactively collect and evaluate data.
- Manufacturers of class I devices shall prepare a post-market surveillance report summarizing the results and conclusions of the analysis of the post-market surveillance data gathered as a result of the post-market surveillance plan, including CAPAs taken and evidence that the report is updated as needed. The report shall be available to the competent authority upon request.
- A risk management plan shall be established and documented for each device.
- Evidence showing implementation of incoming, in-process, and final inspections and the results of those inspections should be available for each device.
- A clinical evaluation plan as well as a clinical evaluation report (CER) shall be available for each device.
- Design and manufacturing requirements from GSPRs require procedures to be described in the instructions for use addressing safe disposal of the device and related waste substances by the user patient or other person.
- For MDR: Class III medical device implants or IIb medical devices that administer medicines shall undergo additional clinical evaluation requirements that should be in place prior to certification.
- Compliance with all applicable MDCG guidance documents for all the devices subject to certification (some guidances are still in process of being released) will be necessary. The latest MDCG endorsed documents are here.

Requirements are more explicit and prescriptive with respect to what data should be gathered, how it should be gathered, and how it should be used. Even a declaration of conformity must follow requirements identified under Annex IV. Without proper organization, device manufacturers must spend a significant amount of time explaining different versions and justifications, which only slows down the process.

An overview of the technical documentation is provided below; each organization should check Annex II of MDR and IVDR to ensure all requirements are fully addressed and structured appropriately for the notified bodies in their technical documentation. It is also important to review submission guidelines provided by each notified body, which can greatly help to align on expectations.

General information	• Legal manufacturer • Authorized representative within the EU if applicable • Trade name of the device • Existing certification • Declaration from the manufacturer stating that no application has been lodged with other notified body
Description and specification of the device, including variants and accessories	• Intended purpose of the device • Description of the assay method • Class of the device and rationale • Description of the device and its components and specifications • Use of specimen (if applicable) • Instrumentation of automated assays • Description of accessories and combinations • Reference to previous and similar generations of the device • History of changes since placing on the market or last evaluation according to regulation (if applicable)
Information to be supplied by the manufacturer	A complete set of labels and instructions for use in the languages accepted in the Member States where the device will be sold.
Design and manufacturing information	Design information Manufacturing information
General safety and performance requirements	Summary table of Annex I requirements
Benefit-risk analysis and risk management	Risk analysis and risk control methods, including risks associated with usability The documentation shall contain information on: (a) the benefit-risk analysis referred to in Sections 1 and 8 of Annex I, and (b) the solutions adopted and the results of the risk management referred to in Section 3 of Annex I.

Product verification and validation	The documentation shall contain the results and critical analyses of all verifications and validation tests and/or studies undertaken to demonstrate conformity of the device with the requirements of the regulations and, in particular, the applicable general safety and performance requirements. **For MDR:** Preclinical and clinical data and additional information required in specific cases per Annex II **For IVDR:** Information on analytical performance, clinical performance, and clinical evidence according to Annex XIII of Regulation (EU) 2017/746. • Performance evaluation plan • Scientific validity report • Analytical performance report • Clinical performance report • Requirements for class D devices • Requirements for self-testing/near-patient testing devices • Clinical evidence and performance evaluation report • Stability studies • Software verification and validation • Additional info (if applicable) • Draft of the summary of safety and performance
Post-market surveillance	• Post-market surveillance plan • Post-market surveillance data **For MDR:** The technical documentation on post-market surveillance to be drawn up by the manufacturer in accordance with Articles 83 to 86 **For IVDR:** The technical documentation on post-market surveillance to be drawn up by the manufacturer in accordance with Articles 78, 79, 80, and 81
EU declaration of conformity	The EU declaration of conformity shall contain all the following information: 1. Name, registered trade name or registered trademark and, if already issued, SRN as referred to in Article 31 (MDR) and Article 28 (IVDR) of the manufacturer and, if applicable, its authorized representative, and the address of their registered place of business where they can be contacted and their location can be established; 2. A statement that the EU declaration of conformity is issued under the sole responsibility of the manufacturer; 3. The Basic UDI-DI as referred to in Part C of Annex VI; 4. Product and trade name, product code, catalogue number, or other unambiguous reference allowing identification and traceability of the device covered by the EU declaration of conformity, such as a photograph, where appropriate, as well as its intended purpose. Except for the product or trade name, the information allowing identification and traceability may be provided by the Basic UDI-DI referred to in point 3; 5. Risk class of the device in accordance with the rules set out in Annex VIII; 6. A statement that the device that is covered by the present declaration is in conformity with the applicable regulation and, if applicable, with any other relevant Union legislation that provides for the issuing of an EU declaration of conformity; 7. References to any common specifications used and in relation to which conformity is declared; 8. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate or certificates issued; 9. Where applicable, additional information; 10. Place and date of issue of the declaration, name and function of the person who signed it, as well as an indication

The assessment of technical documentation involves a detailed analysis by the notified body's technical reviewers. Data organization is a key element of a successful technical review. The new regulations address the need for this information to be presented in a clear, organized, readily searchable, and unambiguous manner, in a form that can be easily consulted. Technical information is subjected to a preliminary review to verify its content and identify the points to be completed before an assessment is initiated. The assessment is then planned based on the results of this review.

Annex II and Annex III provide a correlation of the required documentation; having information clearly organized to explain all the testing that was performed, including the equivalence of clinical data obtained at different times and all the verification and validation activities associated with each device will help reduce review times and cost.

While this could be particularly challenging for many legacy devices, most companies can contribute to a smooth transition to the new regulations by establishing a standard process to provide all the required information to their notified bodies and by implementing their guidance recommendations.

ABOUT THE AUTHOR

Marcelo Trevino is the global vice president, regulatory affairs and quality assurance at Agendia, a molecular diagnostics company focused on breast cancer genomic testing. He has more than 25 years of experience in quality and regulatory affairs, serving in senior leadership roles with different organizations while managing a variety of medical devices: surgical heart valves, patient monitoring devices, insulin pump therapies, surgical instruments, orthopedics, and medical imaging/surgical navigation, amongst others. He has an extensive knowledge of medical device management systems and medical device regulations worldwide (ISO 13485:2016, ISO 14971:2019, EU MDR, EU IVDR, MDSAP). Trevino holds a B.S. in industrial and systems engineering and an MBA in supply chain management from the W.P. Carey School of Business at Arizona State University. He is also a certified Quality Management Systems Lead Auditor by Exemplar Global.

THE ROLE OF THE CONTRACT MANUFACTURER UNDER THE EU MDR & IVDR

Mark Durivage

Managing Principal Consultant, Quality Systems Compliance LLC

Regulation (EU) 2017/745 Medical Device (EU MDR) of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002, and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC Active Implantable Medical Devices Directive (EU AIMDD) and 93/42/EEC Medical Device Directive (EU MDD) was set for enforcement in May 2020. However, due to the global COVID-19 pandemic, the European Commission extended the date of application for EU MDR by 12 months, meaning medical device companies now have until May 26, 2021 to comply with MDR requirements.

Chapter 1, Scope and Definitions, Article 2, Definitions, of the MDR provides the following:

- Manufacturer - means a natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured, or fully refurbished, and markets that device under its name or trademark.
- Economic operator - means a manufacturer, an authorized representative, an importer, a distributor, or the person referred to in Article 22, Systems and Procedure Packs, requirements (1) and (3).

Other than under the definition of "economic operator" in Article 22, Systems and Procedure Packs, requirements for sterilizers, the MDR does not directly address the definition and requirements of the role of the traditional contract manufacturer.

Regulation (EU) 2017/746 In Vitro Diagnostic Medical Devices (IVDR) of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU In Vitro Diagnostic Medical Devices Directive (IVDD) is set for enforcement on May 26, 2022.

Chapter 1 Scope and Definitions, Article 2 Definitions of the IVDR provides the following:

- Manufacturer - means a natural or legal person who manufactures or fully refurbishes a device or has a device designed, manufactured, or fully refurbished, and markets that device under its name or trademark.
- Economic operator - means a manufacturer, an authorized representative, an importer, or a distributor.

The MDR and IVDR do not directly define or address the role of the traditional contract manufacturer, which is traditionally defined as those that manufacture products for or on behalf of the specification holder.

Before placing a medical device or in vitro diagnostic medical device on the market, manufacturers are required to obtain a single registration number (SRN) and register and input the required information into the required electronic system. There is not a requirement for contract manufacturers to obtain an SRN and register, except those that combine medical devices or in vitro diagnostic medical devices into systems or procedure packs or that sterilize systems or procedure packs.

The most significant requirement for manufacturers (specification holders) is to ensure there are robust quality agreements executed with the contract manufacturers. Some of the items to consider including in the quality agreement are:

- Quality management system
- Unannounced audits
- Availability of records
- Risk management
- Validations
- Change control
- Traceability
- Post-market surveillance support

Although not explicitly required, a functioning quality management system (QMS) should be a primary consideration. Without a QMS (ISO 9001 or 13485), fulfilling the remaining requirements will be difficult, if not impossible, and may hinder the product approval process for manufacturers (specification holders). An effective certified QMS from a reputable registrar should provide the necessary structure required for compliance.

The contract manufacturer should be aware of the possibility of unannounced audits of suppliers and/or subcontractors by notified bodies. Some contract manufacturers, especially smaller organizations, may not be prepared to handle such an audit. In this case, the manufacturer (specification holder) should help the contract manufacturer develop a process and procedures for unannounced audits by notified bodies. A good time for practice could be during a supplier audit.

The quality agreement should ensure that documents and records related to the production of a medical device or in vitro diagnostic medical device should be readily available and must be shared with the manufacturer (specification holder) and/or notified body upon request. This will include device master records (DMRs), device history records (DHRs), policies, standard operating procedures, work instructions, validations, risk management documentation, training records, etc. The documents and records must be readily available for review and stored in a way that minimizes deterioration and prevents loss.

Risk management documentation, usually a process failure modes effects analysis (pFMEA), should be developed and maintained based on the requirements of ISO 14971, *Medical devices - Application of Risk Management*. It is especially important that post-market surveillance data (internal nonconformances and external complaints) are used to update the assumptions for probability of occurrence and probability of detection, as well as to identify new failure modes to demonstrate an active and effective risk management process.

Manufacturers (specification holders) need to ensure contract manufacturers establish and maintain robust risk-based qualification and validation programs, as these documents will be subject to review by notified bodies. Adequate sample size linked to risk is essential to ensure validations demonstrate confidence that the process will produce consistent results that meet predetermined specifications.

Change control processes used by contract manufacturers must ensure there is, at a minimum, a communication and feedback mechanism that allows the manufacturer (specification holder) an opportunity to assess all changes for

potential regulatory impact on the status of the marketing authorization. Preferably, the manufacturer should sign on to any changes affecting its regulated products.

Traceability is essential for all raw materials and components used in the manufacture of regulated medical devices. Manufacturing materials such as mold releases, cutting oils and fluids, and tumbling media should be recorded and subject to change control, as a regulatory assessment will be required by the manufacturer (specification holder). A robust traceability program will aid in the prevention of fraudulent and/or counterfeit raw materials and components entering the systems as well as aid in complaint investigations, field corrections, and recalls.

As part of post-market surveillance support, contract manufacturers will need to ensure that production records as well as nonconformance records are readily accessible and constructed to facilitate review. The internal failure modes of the contract manufacturer must align with the external failure modes of the manufacturer (specification holder) to allow for an efficient review of data regarding complaints and escalation to CAPA as well as the validation of FMEA probability of occurrence and detection assumptions.

CONCLUSION

The relationship between the contract manufacturer and the manufacturer (specification holder) under the EU MDR and IVDR will be much more participatory and engaging than with previous regulations. The EU MDR and IVDR will necessitate a partnership built on a foundation of trust, cooperation, and increased communications.

I cannot emphasize enough the importance of establishing a comprehensive quality agreement outlining the roles and responsibilities of each party as well as the increased expectations and support for unannounced audits, the availability of records, an active risk management and validation program, a robust inclusive system for change control, increased traceability requirements, and post-market surveillance support. The suggestions presented in this article can and should be utilized based upon industry practice, guidance documents, and regulatory requirements.

ABOUT THE AUTHOR

Mark Allen Durivage has worked as a practitioner, educator, consultant, and author. He is Managing Principal Consultant at Quality Systems Compliance LLC, an ASQ Fellow and SRE Fellow. Durivage primarily works with companies in the FDA regulated industries (medical devices, human tissue, animal tissue, and pharmaceuticals) focusing on quality management system implementation, integration, updates, and training. Additionally, he assists companies by providing internal and external audit support as well as FDA 483 and warning letter response and remediation services. He earned a BAS in computer aided machining from Siena Heights University and an MS in quality management from Eastern Michigan University. He holds several certifications, including CRE, CQE, CQA, CSSBB, RAC (Global), and CTBS. He has written several books available through ASQ Quality Press, published articles in *Quality Progress*, and is a frequent contributor to Life Science Connect.

HOW TO NAVIGATE CLINICAL DATA PER EU MDR

Matthias Fink, M.D.
Global Team Leader, TÜV SÜD America

In May 2017, the European Medical Devices Regulation (MDR) 2017/745 was published to replace the current Medical Device Directive (MDD) and the Active Implantable Medical Device Directive (AIMDD). In April 2020, the European Parliament adopted the European Commission's proposal to postpone the Date of Application (DoA) of the MDR by one year, and as such, the new DoA is May 26, 2021. It is worth noting that the end of the transition period for MDD and AIMDD certificates remains May 26, 2024, thus reducing the timeline for manufacturers to get their MDR certificates from four to three years.

The MDR puts a higher emphasis on clinical data for medical devices and calls for increased scrutiny on the duty of manufacturers to continuously collect clinical data in the postmarket setting. Manufacturers are required to proactively collect and evaluate clinical data on the use of their devices. This article highlights some relevant changes during the transition to the MDR and potential challenges manufacturer might face. The MDR requires that medical devices should have sufficient clinical data, but the term "sufficient clinical data" is not defined. Due to the heterogeneity of medical devices ranging from a Band-Aid to a biventricular assist device (artificial heart), it is not feasible to provide a one-fits-all definition.

In general, the definition of clinical data did not relevantly change from MDD/AIMDD to MDR, but due to a more stringent requirement under the MDR, a device with sufficient clinical data under the current directive might need additional clinical data under the MDR. For example, a manufacturer of a legacy device would still rely on clinical data coming from an equivalent device, but that does not fulfill the MDR requirements of demonstrating equivalence.

PREMARKET CLINICAL INVESTIGATIONS

Article 61.4 of the Regulation states that for implantable and class III devices, a premarket clinical investigation shall be performed. Due to more stringent requirements for the equivalence demonstration under the MDR, the number of premarket clinical investigations is likely to increase.

The MDR lays out in several articles and in Annex XV the regulatory requirements for a clinical investigation in the

European Union (EU). The content in Annex XV is aligned with the requirements of the ISO 14155 standard, *Clinical investigation of medical devices for human subjects — Good clinical practice*. The latest revision, ISO 14155:2020, was published last year.

DERIVING CLINICAL DATA FROM PUBLISHED LITERATURE

A relevant source for clinical data under the MDR continues to be published articles in scientific journals. Mantra et al. found in a systematic review that the published literature in the field of orthopedics had doubled between 2000 and 2011. They also saw a tenfold increase in the number of published meta-analyses, with 43.6% of a high quality.[1]

However, despite the increased quantity and quality of published literature, it cannot automatically be concluded that there is sufficient clinical data published for every medical device. In fact, the majority of medical devices are not covered in scientific literature and not every pre- or postmarket clinical study conducted by a manufacturer is published. This is especially true for medical devices with small market shares or for those that are based on an already known design principle that might be of less scientific research interest for a physician.

We also see a focus in research interest on new technologies (e.g., device coatings) or surgical techniques (e.g., minimally invasive procedures), but not every publication contains the clinical data a manufacturer might need to demonstrate conformity with the General Safety and Performance Requirements (GSPRs) laid down in Annex I of the MDR.

Literature data needs to come from a comprehensible and reproducible literature search that will be challenged by the Notified Body. The MEDDEV 2.7/1 (Revision 4) guidance document, published in 2016, provides an up-to-date scientifically valid guidance on how to conduct a literature search in Appendices A4 and A5.

DEMONSTRATION OF EQUIVALENCE

Under the MDD/AIMDD, the majority of medical devices received their initial CE mark via demonstration of equivalence to an already marketed device. Unfortunately, a certain number of devices failed to demonstrate the same level of safety and performance as the claimed equivalent device in the postmarket setting and had to be recalled from the market. A 2016 publication found a higher rate of postmarket safety alerts and recalls for devices first approved in Europe compared to devices first approved in the U.S.[2]

That has led to a more stringent requirement for claiming equivalence in Article 61.5 of the MDR. The equivalence route is still feasible, but it is no longer possible to demonstrate equivalence solely on a descriptive comparison of the two devices. The MDR requires manufacturers to demonstrate a sufficient level of access to the data pertaining to the proposed equivalent device.

For implantable and class III medical devices, a contract is required to allow full access to the technical documentation of the equivalent device. Notified Bodies will challenge manufacturers to provide that in-depth level of access. To clarify some uncertainties in the equivalence demonstration, the MDCG 2020-5 guidance document was published in 2020.

LEGACY DEVICES UNDER THE MDR

Per definition, every medical device marketed under the MDD/AIMDD is considered a legacy device. Since there is no grandfathering, legacy medical devices will need to go through the same initial MDR conformity assessment procedure as novel devices.

In the past, the requirement to collect sufficient clinical data was not always followed strictly, and some devices with long market histories ended up not having sufficient clinical data to make the successful transition to the MDR. To avoid a potential negative impact on the healthcare industry in Europe due to a shortage of medical devices, the MDCG 2020-6 guidance document on sufficient clinical data for legacy devices was published. This guidance includes a definition of devices that could be considered well-established technology that might rely on clinical data from the state-of-the-art to demonstrate conformity with the GSPRs. Corresponding to the equivalence route, a manufacturer would need a specific postmarket clinical follow-up (PMCF) activity to confirm that the device fulfills the GSPRs.

POSTMARKET CLINICAL FOLLOW-UP UNDER THE MDR

The MDR now includes a higher scrutiny of clinical data in the postmarket setting. Depending on the risk class, a manufacturer must provide a summary of the postmarket data and an updated benefit-risk analysis coming from a

partially updated clinical evaluation annually or biannually in a Periodic Safety Update Report (PSUR). For implantable devices, these PSURs shall undergo a mandatory assessment by the Notified Body that issued the EC-Certificate. This higher scrutiny increases the obligations on the manufacturer's side to confirm safety and performance of the devices.

This higher post-market scrutiny, together with the required vigilance system, might provide a tool to detect implantable devices that are not in conformance with the state-of-the-art and recall them from the market earlier. Via the EUDAMED database, Notified Bodies and Competent Authorities will receive regularly updated postmarket data via the PSUR.

The MDR now specifically includes device registries as a source for real-world data in the postmarket setting. Per definition, a registry is a data collection that does not have a specific endpoint and includes all patients treated with a specific medical device or procedure. Since a PMCF study is subject to certain limitations, e.g., a limited number of patients and potential bias by selecting a high-volume hospital, a registry can be a valuable source for long-term clinical data. Sherman et al. stated in 2016 that for medical devices, clinical studies have their limitations compared to the real-world setting.[3]

With the increasing demand for more long-term data from physicians and legislators in Europe, implant registries, like some national joint registries in Europe, started collecting patient-reported outcome measures (PROMs) besides the sole implant survival rates. Even when a medical device is covered in a register, there could still be unanswered questions that might require an additional PMCF study.

In summary, the new EU MDR leads to increased scrutiny to get novel devices CE marked and to keep legacy devices on the market. It is expected that there will be a smaller number of medical devices on the European market due to the obsoletion of devices when manufacturers reassess their portfolios in the transition from the MDD/AIMDD to the MDR. It is expected that the MDR will be an instrument for increased patient safety in Europe due to the imposition of more stringent requirements to collect clinical data and the higher scrutiny in the postmarket setting.

REFERENCES

1. Manta A, Opingari E, Simunovic N, Duong A, Sprague S, Peterson D et al. A systematic review of meta-analyses in orthopaedic surgery between 2000 and 2016. Bone Joint J 2018;100-B:1270–4

2. Hwang TJ, Sokolov E, Franklin JM, Kesselheim AS. Comparison of rates of safety issues and reporting of trial outcomes for medical devices approved in the European Union and United States: cohort study. BMJ 2016;353:i3323

3. Sherman RE, Anderson SA, Dal Pan GJ, Gray GW, Gross T, Hunter NL et al. Real-World Evidence - What Is It and What Can It Tell Us? N Engl J Med. 2016;375(23): 2293-2297

ABOUT THE AUTHOR

Matthias Fink, M.D., is TÜV SÜD America's global team leader for the Ortho, Trauma and Dentistry Team at the Clinical Centre of Excellence as well as team manager of the Clinical Focus Team North America. A board-certified orthopedic and trauma surgeon, he has 17 years of experience in orthopedic, trauma, and reconstructive surgery and extensive training in cardiovascular and thoracic surgery. Prior to joining TÜV SÜD America, he was a clinical reviewer for the Clinical Centre of Excellence at TÜV SÜD Product Service in Germany.

THE 6-STEP CHECKLIST FOR IVDR COMPLIANCE

Hilde Viroux

Management Consultant, PA Consulting

Hans Mische

Managing Consultant - Health and Life Sciences, PA Consulting

The in vitro diagnostic devices industry has until May 25, 2022 to bring products, documentation, and quality management systems into compliance with the new EU Regulation on In Vitro Diagnostic Devices 746/2017 (IVDR). This regulation is a major revision, focusing on patient safety, requiring more clinical evidence, improving traceability in the supply chain, and enforcing a proactive post-market surveillance system to ensure early detection of problems.

The past year presented a challenge in implementing the IVDR while the COVID-19 pandemic forced the industry to focus efforts on bringing COVID-19 tests to the market. The May 2022 deadline is quickly approaching and there is no sign that the EU Commission is considering postponing it. Even if the deadline is pushed back, the expectation is that it would only be for a year, similar to the extension granted for the medical devices regulation. Full compliance programs often take longer than that. Companies that haven't started their compliance journey need to act soon, as the majority of the IVDs currently on the market cannot be sold after May 2022 unless they are in full compliance with the regulations.

CHALLENGES IMPLEMENTING IVDR COMPLIANCE

The challenges of ensuring IVDR compliance are mostly related to products having insufficient design documentation, requiring additional testing and performance evaluations that must include scientific, clinical, and analytical data – the list goes on. Coordinating the documentation updates between the various functional areas and arranging tests while many staff members work from home due to COVID-19 brings an additional layer of complexity. The fact that most IVDs did not involve the oversight of a notified body under the current IVD directive contributes to the product documentation often not being up to par.

This leads to the second challenge for IVD companies: Not only are many companies not used to working with a notified body, but there are still not enough notified bodies designated under IVDR to cover all the IVDs currently on the market in the EU. IVDR will require notified body involvement for about 80% of the IVDs, compared to less than 20% of IVDs under the current directive. As of early February 2021, there

are four notified bodies designated under the IVDR, compared to 23 notified bodies under the IVD directive. The 23 include five notified bodies from the U.K. that have had their designation withdrawn because of Brexit. A simple calculation shows the bottleneck that is coming. The four notified bodies designated under IVDR will be expected to deal with four times as many products as the 23 notified IVD bodies have. And experience from manufacturers dealing with notified bodies for MDR compliance shows that the notified bodies don't have the resources to deal with the increased demand and requirements, which is having a negative effect on delivery of the services and timelines.

In addition, the notified bodies must perform on-site audits to verify the manufacturer's quality management system. The EU Commission has opened the door to remote audits, but the final decision to allow remote audits is with each country overseeing the notified body, which may lead to discrepancies in the approach to remote audits between notified bodies.

WHAT STEPS SHOULD YOU TAKE TO MEET THE IVDR DEADLINE?

1. **Select and contract with an IVDR designated notified body.** Notified bodies are not necessarily designated for all types of IVDs, so the first step should be to compare your product portfolio with the designated scope of the notified body to ensure there is a match. You can search the NANDO website of the European Commission or check directly with the notified body to verify that they will be able to assess all your IVDs.

2. **Assess and prioritize your product portfolio.** With all the work that needs to be done to bring product documentation up to date, it is advisable to look at the total cost of compliance. For some products, the cost of remediation may be higher than the sales value, so you should take a holistic look at the sales and product value before starting remediation efforts. Similarly, bearing a possible bottleneck with the notified bodies in mind, a company may prioritize the remediation of products that deliver the highest sales value to ensure they can stay on the market after May 2022.

3. **Get the necessary tools and communications in place.** Implementing IVDR is a major undertaking, affecting all areas of the business. Managing such a program in a normal pre-pandemic environment was already a challenge. With the majority of the workforce working from home during the pandemic, even more time has to be spent on training, communication, and change management. Change management was important before, as people often resist change. With the physical separation adding to the challenge, it is critical that the necessary tools and communications are in place to get people motivated and aligned to the changes.

4. **Coordinate between your various workstreams to align your activities.** This is vital to ensure that the inputs to the technical documentation, QMS, labeling, etc. are accurate and timely. A dedicated multifunctional team is needed to align the tasks and review the technical documents. In many cases, new processes and procedures will need to be initiated. To increase efficiency and reduce costs, product documentation and labeling updates to IVDR should coincide with scheduled revisions to avoid extra work. Rolling out IVDR compliant labeling needs careful planning between the regulatory function for global registrations, manufacturing, and supply chain for inventory management.

5. **Update your technical documentation,** including additional testing and creation of new reports like Performance Evaluation Plans and Reports, Periodic Safety Update Reports, and Design History File. This represents a significant amount of work, and testing can take a long time to complete.

6. **Establish a compliant supply chain.** This expansion of the scope of the legislation should not be underestimated. For companies with a complex distribution chain, it can already be a challenge to map out the supply chain and product flows to identify the various economic operators. The role of an economic operator can vary on a product-by-product basis. Importers and distributors have to perform checks, but the checks vary with the role of the economic operator. Distributors that translate the instructions for use or repackage products must meet specific requirements and require a notified body inspection for these activities. Adopting economic operator compliance early on as part of the overall compliance program reduces the risk of running out of time toward the May 2022 due date.

IVDR implementation brings many challenges but also gives companies the opportunity to rationalize and optimize their product portfolio, streamline the supply chain, and implement more robust design and QMS processes to ensure safer products and continued sales in the EU.

ABOUT THE AUTHORS

Hilde Viroux is a medtech expert at PA Consulting and a leading expert on the European Medical Devices Regulation. She is a senior leader with a broad experience in regulations, quality, manufacturing, supply chain, and project management in the pharmaceutical and medical device industry. She has an outstanding track record on successful implementation of major projects and building up new capabilities within an organization. She has an MSc in Medical Technology Regulatory Affairs from Cranfield University in the U.K., and a BS in biochemistry engineering.

Hans Mische is a medical devices design and development expert at PA Consulting. He has demonstrated expertise in business development, strategy, upstream marketing, strategic account management, product development, clinical evaluations, manufacturing, and regulatory affairs in multiple markets. Mische has held leadership roles in organizations ranging from start-ups to large multinational corporations, has experience working with all top 10 medical devices companies, and recently led a global IVDR program for a major diagnostics product company. Additionally, he founded or cofounded five medical device companies and is an inventor on 50+ issued patents for various medical device and diagnostic devices, systems, and technologies. He has a BS in Physics from Saint Cloud State University.

10 ACTIONS TO PREPARE FOR THE U.K. CONFORMITY ASSESSMENT PROCESS

Ed Ball
Senior Associate, RQM+

As medical device businesses work on complying with the EU's Medical Device Regulation and In Vitro Diagnostic Regulation, they must now also turn their attention to changing regulatory rules in the U.K. The transition to the U.K.'s new regulatory regime has officially begun as of Jan. 1, 2021. All medical devices on the U.K. market must be registered with the Medicines and Healthcare products Regulatory Agency (MHRA), including CE marked and U.K. Conformity Assessed (UKCA) marked devices, though there are grace periods for this initial registration based on the risk classification of a device.

During the transition period, the U.K. Medical Devices Regulations (U.K. MDR) 2002 will continue to apply in England, Scotland, and Wales, while CE marks will still be accepted up to June 30, 2023. Not to be confused with the EU MDR, the U.K. MDR transposes European directives for medical devices and in vitro diagnostic medical devices into U.K. law. In Northern Ireland, where the rules for placing a device on the market differ, the EU MDR and IVDR will apply in 2021 and 2022 respectively, in line with the EU's implementation timeline.

Every business must begin planning now to make full use of the transition period and actively monitor for new developments. It is critical to understand where the U.K.'s regulatory regime is still a work in progress, where the potential areas of complexity lie, and any unknown factors. This article will highlight key actions that businesses must integrate into their planning to ensure continued access for their medical devices in the U.K.

1. CHECK FOR OVERLAP BETWEEN THE U.K. AND EU MDRS

The medical device industry is under a great deal of pressure due to the pandemic and regulatory deadlines, but their experiences with the MDR and IVDR may place them in good stead for this new compliance challenge. Businesses have already invested resources in complying with the MDR and IVDR, and so they must begin by determining whether their existing compliance efforts can be repurposed for UKCA marking. In this way, they can eliminate any unnecessary duplication of activities and then plan strategically to fill any gaps in data and documentation.

2. CONSIDER RISK-BASED PLANNING

This preparatory activity can help companies to make informed decisions about their product portfolios in the U.K. and EU markets, based on the level of compliance effort required for each device. Businesses should take a holistic view of regulatory requirements across their whole portfolio by building a risk matrix. The matrix should include products by geography, along with current level of preparedness. By building a complete picture of their regulatory status, companies can then analyze compliance effort and cost for each product class.

3. RATIONALIZE YOUR PORTFOLIO

A thorough assessment of the regulatory status within their portfolio should then help businesses review what their priorities should be, in line with their commercial interests. This means they may need to make decisions on whether to continue product supply or even introduce new products on the U.K. market. In some cases, the regulatory burden may be reduced, since the U.K. MDR is based on the EU directives, and not the recent EU MDR and IVDR. For instance, Class I devices that have been up-classified under the MDR may continue to self-certify for the U.K. market. It must be noted, however, that future U.K. legislation is likely to closely resemble the EU MDR and IVDR.

4. ENGAGE EARLY WITH APPROVED BODIES

Many businesses may be tempted to wait until the middle or end of the transition period to begin their submission. Those devices that would previously have relied upon a Notified Body for their conformity assessment en route to a CE mark will require a conformity assessment by a U.K. Approved Body in order to attain their UKCA mark. As of January 1, U.K. organizations that were acting as Notified Bodies are now Approved Bodies; there are currently only three U.K. Approved Bodies. There is a danger that Approved Bodies may not be able to cope with demand for their services, so as with the MDR and IVDR, it is highly recommended that companies begin preparing as early as possible to enable easy access to an Approved Body and to ensure there is sufficient time to address any concerns.

5. APPOINT A U.K. RESPONSIBLE PERSON

Non-U.K. manufacturers must have a U.K.-based Responsible Person (UKRP), which is the new equivalent to the EU Authorised Representative. The UKRP must have a registered place of business in the U.K. in order to register with the MHRA and must be identified on either the device's labelling or instructions for use (IFU) once the UKCA mark is affixed to the device. Only one UKRP may be appointed, contrary to the EU rules for Authorised Representatives. In Northern Ireland, non-EU businesses will still need a European Authorised Representative to market devices.

Businesses must first understand what will be expected of their representative, and then determine how to source a UKRP who will be able to reliably fulfil these requirements. Next, businesses must establish procedures for managing documentation with the responsible person, so that both parties have all the necessary information at hand and have clear communication channels.

6. COMPLY WITH LABELLING AND IFU REQUIREMENTS

To comply with the new U.K. regulations, medical devices will need to bear a UKCA mark, as well as the name and address of the UKRP for non-U.K. based manufacturers. In Northern Ireland, medical devices must continue to have a CE mark or the UKNI mark in order to remain on the market. Transition to the MDR and IVDR requires many labelling changes, so it is important that manufacturers do not omit labelling updates from their planning and resource allocation.

7. REVIEW PROCEDURES FOR CONDUCTING CLINICAL INVESTIGATIONS

Where investigations are based across multiple sites in and outside the U.K., businesses will need to plan how to implement and manage these investigations, in compliance with local requirements. Manufacturers with ongoing clinical trials in the U.K. must review the procedures for conducting investigations. It is likely that these will change as the MHRA develops its own requirements. The body has already published guidance on submitting safety reports, making substantial amendments to clinical trials, registering trials for investigational medicinal products, and publishing summary results.

8. EDUCATE YOURSELF ON IMPORT/EXPORT MANAGEMENT

Now that the U.K. is outside of the European Union, EU-based manufacturers and U.K. importers must ensure they are aware of new import procedures and controls and assess how this increase in administrative tasks may affect costs. While CE marking and certificates will continue to be recognized by the U.K. until June 2023, import/export administration thereafter may change considerably and become more complex and burdensome. Practical supply chain issues may emerge in practice. Close monitoring of the developing situation and the emerging intentions of the relevant regulatory authorities is essential.

9. COMPLY WITH DATA PROTECTION REQUIREMENTS

Companies must put protocols in place to ensure compliance for the movement of protected data between the U.K. and the EU. Again, this is a situation whose outcome over the next few years is far from certain. The movement of any data that can be classed as "sensitive" is an issue, under the scrutiny not only of the medical device regulators but also subject to any emerging tensions between U.K. data protection rules and the EU's General Data Protection Regulation (GDPR). So far, both the EU and the U.K. seem keen to maintain "equivalency," as evidenced by the European Commission launching a process to adopt adequacy decisions of the U.K. for GDPR. This has to go through a number of further stages and requires close monitoring over time.

10. TAKE INTO ACCOUNT DEVELOPING ISSUES

As businesses begin UKCA submissions, it is likely that the MHRA will identify emerging issues or areas where further clarification is needed. Staying abreast of these developments will help companies learn from the experiences of others and avoid any potential issues in their own submission. As we have seen with the MDR and IVDR, regulations do not necessarily make it clear *how* requirements should be met, and so the guidance available from the MHRA is likely to evolve during the transition period

For example, clarification will be required concerning the list of designated standards for medical devices issued by the U.K.'s Department for Health and Social Care. The published lists are based on the list of harmonized standards published in the Official Journal of the EU, which are only standards harmonized to the MDD, AIMDD, and IVDD. Recently published standards (e.g., ISO 14971:2019) have not been harmonized to the latter European directives and are thus not in the U.K.'s designated list, but they are considered as the state-of-the-art standards. Manufacturers will need to consider how to manage their compliance with applicable standards where different versions are cited in different regulatory jurisdictions.

The new regulatory regime is also an opportunity for the U.K. to address concerns relating to medical device safety, and this may impact the level of scrutiny during the approvals process. For instance, the Independent Medicines and Medical Devices Safety Review (or the Cumberlege review) was published in 2020, and it shone a light on how the English healthcare system had inadequately responded to serious safety concerns around three medical treatments. The report recommends that the MHRA strengthen adverse event reporting and medical device regulation, as well as improve engagement with patients and their outcomes. These recommendations will certainly play a part in revisions of U.K. legislation.

As the U.K. is likely to revise and update its own regulation for medical devices over the next few years, manufacturers will need to regularly review their compliance planning for products on the U.K. market. The pointers above serve to make the planning process as efficient as possible; manufacturers can make sure they are suitably prepared to work through each step, and they can also anticipate any delays along the way, such as finding a U.K. Responsible Person or carrying out administrative tasks for import. The task of attaining UKCA marking may also be facilitated by manufacturers' efforts for EU MDR and IVDR, since data and documentation are likely to be more up to date than would have otherwise been the case. Those businesses that begin the submission process early are likely to lead the way for others, as well as avoid the risk of losing access to the U.K. market.

ABOUT THE AUTHOR

Ed Ball is a senior associate at RQM+. He formerly worked as a medical device specialist at the U.K. Medicines and Healthcare products Regulatory Agency (MHRA), and is currently an active member of the U.K.'s Technical Committees for Medical Device Quality Management and Risk Management standards. He is a medical device specialist and chartered engineer who combines a technical understanding of medical devices with regulatory and quality management experience. Ed has more than 15 years of experience with devices that are EU Class I–III devices, active devices, implantable devices, diagnostic devices, measuring devices, and sterile devices.

GERMANY'S DIGITAL MEDICAL DEVICE REGULATIONS: A FRAMEWORK FOR THE WORLD TO FOLLOW, PART I

John Giantsidis
President & Principal Consultant, CyberActa, Inc.

Germany's Digital Healthcare Act came into effect on December 19, 2019, introducing the "app on prescription" as part of healthcare provided to patients through digital health applications (in German: "digitale Gesundheitsanwendungen," hereinafter DiGA). The Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM, or the Federal Institute for Drugs and Medical Devices) released a new guide in August 2020 detailing the requirements for DiGA manufacturers in order to make your DiGAs available to the more than 73 million participants in the German statutory health insurance. I will give an overview of the situation and will cover the many privacy requirements noted in the new guide in Part 1 of this article series.

Assuming that your digital medical device or software as a medical device (SaMD) can provide a medical benefit, particularly regarding the improvement of the state of health, the reduction of the duration of a disease, the prolongation of survival, or an improvement in the quality of life, BfArM has to assess your DiGA. Likewise, if your digital medical device or SaMD can be considered as part of the detection, monitoring, treatment, or alleviation of disease or the detection, treatment, alleviation, or compensation of injury or disability, BfArM has to assess your DiGA. BfArM also has to assess your DiGA if it supports the health behavior of patients or integrates the processes between patients and healthcare providers, and include in particular the areas of:

1. Coordination of treatment procedures
2. Alignment of treatment with guidelines and recognized standards
3. Adherence
4. Facilitation of access to care
5. Patient safety
6. Health literacy
7. Patient autonomy
8. The coping with illness-related difficulties in everyday life

Reduction of therapy-related efforts and strains for patients and their relatives.

BfArM has to assess your DiGA within a three-month period starting with the filing of the complete application. The clinical evaluation of the Medical Device Directive (MDD)/Medical Device Regulation (MDR) conformity procedure must initially be considered separately from the DiGA Fast Track. The conformity assessment first proves the safety and suitability of the medical device. However, you can cite study results that have been included in the conformity assessment proving positive healthcare effects.

Generally, a digital medical device qualifies as a DiGA if it is a medical device of the risk class I or IIa (according to MDR or MDD as part of the transition regulations until the beginning of the validity of the MDR on May 26, 2021), its medical purpose is achieved through the main digital functions, and the app is used only by the patient or by the patient and the healthcare provider. This means that apps that are only used by the physician to treat patients are not eligible.

A DiGA must meet explicit requirements regarding safety and suitability for use, data protection, and information security and quality, especially interoperability. You as the manufacturer must demonstrate this to BfArM with emphasis on the completed checklists as well as the evidence of compliance with regulatory requirements for medical devices. BfArM can request further evidence on individual quality features during the application assessment and check the accuracy of the information. In any case, you must provide free access (login data) of your DiGA to BfArM.

The essence of the BfArM assessment is a thorough examination of the manufacturer's statements about the product qualities — from data protection to user friendliness — and the examination of the evidence of the positive healthcare effect of the DiGA. Manufacturers must declare compliance regarding data protection regulations and data security requirements. All DiGAs must meet basic requirements, and those deemed requiring a very high protection requirement must meet additional requirements per the required protection requirement analysis. It is important to understand that the processing of personal data by the DiGA and its manufacturer is subject to EU General Data Protection Regulation (GDPR) 2016/679. Beyond privacy and security, manufacturers must also declare the fulfillment of the requirements regarding interoperability, robustness, consumer protection, ease of use, medical content, and patient safety.

The DiGA privacy requirements emanate from the GDPR's data protection framework and are based on the principles of data privacy, data protection, and privacy rights for individuals in the EU:

CONSENT

- A voluntary, specific, and informed consent of the user is to be obtained for data processing before the processing of such personal and related data is taken place.
- The consent and declarations of the user is given consistently expressly, i.e., through an active, clear action.
- The user can revoke their consent easily, barrier-free, at any time and in an easily understandable way with effect for the future.
- The user is informed of the right and options to withdraw consent before giving their consent.
- Before giving consent, the user is informed in a clear, understandable, user-friendly, and target-group-appropriate form about which categories of data are processed by the DiGA or you as the manufacturer.
- The person concerned can access the texts of the consents and declarations given at any time from the DiGA or via a source referenced within it.

DATA MINIMIZATION AND ADEQUACY

- The personal data processed via the DiGA are appropriate for the purpose and limited to what is necessary for the purposes of processing.
- You have ensured that the purposes of processing personal data through the DiGA cannot reasonably be achieved to the same extent by other, more data-efficient means.
- Health-related data is stored separately from the data required exclusively for service accounting.

- You have ensured that employees entrusted with non-product-related tasks do not have access to health-related data.
- Provided that the DiGA's use is not restricted to a private IT system of the person using it:
  - You have explicitly considered corresponding application scenarios in the data protection impact assessment.
  - You explicitly advise the insured person that the use of the DiGA in a potentially unsafe environment is associated with security risks that cannot be fully addressed by you as the manufacturer.
- When using the DiGA on an IT system that is not only used by the insured person, the storage, even if temporary, of health-related data on this IT system is completely prevented, and data and files stored locally on the IT system used are securely deleted after the end of the usage session of the DiGA, even if the user has not explicitly ended the usage session.

INTEGRITY AND CONFIDENTIALITY

- The DiGA provides appropriate technical and organizational measures to protect personal data against unintentional or impermissible destruction, deletion, falsification, disclosure, or illegitimate forms of processing.
- The exchange of data controlled by the DiGA between the end device of the person concerned and external systems is encrypted according to the state of the art.

ACCURACY

- The DiGA provides technical and organizational measures to ensure that the personal data that it processes are factually correct and up to date.
- You as the manufacturer take all reasonable measures to ensure that incorrect personal data are immediately deleted or corrected.

NECESSITY AND DATA PORTABILITY

- Personal data collected via the DiGA is stored only for as long as it is absolutely necessary for the provision of the promised functionalities or for other purposes resulting directly from legal obligations.
- You must justify separately the purposes of the storage and the maximum storage period, stating the reasons why these purposes represent a legitimation for the further storage of personal data.
- You provide mechanisms via which the data subject can exercise the right to data portability from the DiGA and can retrieve or transfer it to another DiGA.

INFORMATION REQUIREMENTS

- The data protection declaration is easy to find, barrier-free, and freely accessible via the application website.
- The data protection declaration contains all relevant information about the manufacturer and data protection officer, the purpose of the DiGA, the data categories processed for this purpose, your (the manufacturer's) handling of this data, the right to revoke given consent, and the options for exercising the rights of those affected, and you adequately implement additional information obligations according to GDPR Articles 13 and 14.
- The data protection declaration is easy to find even after the installation of the DiGA.
- The user can receive information from you on the personal data stored about them to the extent specified in GDPR Article 15.
- The data protection declaration contains a comprehensible deletion concept that regulates the procedure for withdrawing consent and deinstallation of the DiGA as well as the handling of claims for deletion of data and restriction of their processing per the requirements of GDPR Articles 17 to 19.
- The user can request that you correct incorrect personal data relating to them and to complete incomplete personal data relating to them.
- Before deleting the user account, you need to inform the data subject of any data that may be lost and the right to data transfer in accordance with Article 20 of Regulation (EU) 2016/679.

DATA PROTECTION IMPACT ASSESSMENT AND RISK MANAGEMENT

- You have implemented a procedure for the regular review, assessment, and evaluation of the effectiveness of the technical and organizational

measures to ensure the security of processing, with which all systems and processes used in connection with the DiGA are recorded.

- You have obliged all persons who have access to personal data from their work to secrecy.
- You have carried out a data protection impact assessment for the DiGA and transferred the risk analysis carried out in the documented risk management processes after a continuous reassessment of threats and risks has taken place.
- You can ensure that personal data breaches are reported to the supervisory authority within 72 hours of becoming aware of the breach.
- You have implemented the requirements of GDPR Article 34 on informing those affected in the event of data protection incidents.

EVIDENCE

- You have documented the data protection guidelines applicable to the company and trained your employees in their implementation.
- You have implemented measures to ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed, or removed.
- The DiGA or you as the manufacturer do not pass on personal data at all to processors or exclusively to processors who have sufficient trustworthiness and liability. You have implemented appropriate mechanisms to protect transferred data and have a binding contractual relationship that excludes a weakening of the commitments made to the insured.
- The processing of health data as well as personally identifiable inventory and traffic data takes place exclusively in Germany, in another member state of the European Union, or on the basis of an adequacy decision in accordance with GDPR Article 45.

The DiGA privacy requirements emanate from the GDPR's data protection framework and are based on the principles of data privacy, data protection, and privacy rights for persons in the EU. It is important to analyze what, how, and why you process data. Be prepared to show how data is transferred and processed because you could be asked. Put consent and privacy notes in plain language and be ready to be responsive to requests from individuals and incidents.

ABOUT THE AUTHOR

John Giantsidis is the president of CyberActa, Inc, a boutique consultancy empowering medical device, digital health, and pharmaceutical companies in their cybersecurity, privacy, data integrity, risk, SaMD regulatory compliance, and commercialization endeavors. He is also a member of the Florida Bar's Committee on Technology and a Cyber Aux with the U.S. Marine Corps. He holds a Bachelor of Science degree from Clark University, a Juris Doctor from the University of New Hampshire, and a Master of Engineering in Cybersecurity Policy and Compliance from The George Washington University.

GERMANY'S DIGITAL MEDICAL DEVICE REGULATIONS: A FRAMEWORK FOR THE WORLD TO FOLLOW, PART II

John Giantsidis
President & Principal Consultant, CyberActa, Inc.

Germany's Digital Healthcare Act came into effect on December 19, 2019, introducing the "app on prescription" as part of healthcare provided to patients through digital health applications (in German: "digitale Gesundheitsanwendungen," hereinafter DiGA). The Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM, or the Federal Institute for Drugs and Medical Devices) released a new guide in August 2020 detailing the requirements for DiGA manufacturers in order to make your DiGAs available to the more than 73 million participants in the German statutory health insurance. In this Part 2, I examine the data security requirements.

INFORMATION SECURITY AND SERVICE MANAGEMENT

- You have implemented an information security management system (ISMS) in accordance with ISO 27000 series or a comparable system and can provide a corresponding recognized certificate or comparable evidence.
- You have a structured protection needs analysis considering damage and threat scenarios with your documented output being be a normal, high, or very high protection requirement for the DiGA in accordance with BSI standard 200-2, and you can submit the documentation of the protection requirement analysis at the request of BfArM.
- You have implemented and documented processes of DiGA/software release, change control, and configuration management, taking into account the EU MDR requirements. Ensure that extensions and adjustments to the DiGA, have been sufficiently tested and explicitly approved before they are put into production.

DATA LEAKAGE PREVENTION

- You have ensured that the communication between the DiGA and other services is technically limited to such an extent that no unwanted data communication can take place from the DiGA via which personal data can be sent.
- At least one transport encryption is used for every data communication between different system components of the DiGA via open networks.

- The DiGA checks the authenticity of the services accessed every time it accesses functionalities that can be accessed via the internet before personal data is exchanged with these services.
- You have ensured that the DiGA does not write any unwanted log or auxiliary files.
- You have ensured that the DiGA does not generate error messages that may reveal confidential information.

AUTHENTICATION

- All users must authenticate themselves using a method appropriate to the protection requirements before data on the application can be accessed.
- You have ensured through suitable technical measures that the data used to authenticate a person using the DiGA is never exchanged via unsecured transport connections.
- The DiGA uses or contains a central authentication component implemented with established standard components that are only permitted for the initial authentication and whose trustworthiness can be verified by the DiGA's services.
- The DiGA enforces that a user can only change the data used for their authentication if sufficient information is added to check the authenticity of this person.
- If authentication is carried out using a password:
  - The DiGA forces everyone using it to use secure passwords in accordance with a password guideline which, among other things, specifies a minimum length for passwords and defines limit values for failed login attempts.
  - You have ensured that passwords are never transmitted or saved in clear text.
  - The DiGA logs and informs the user of any changing or resetting of passwords.
- If the DiGA stores authentication data on a terminal device or in a software component located on it, the explicit consent of the user is requested ("opt-in") and advised of the risks of the function.
- If information on the identity or authenticity of the user or on the authenticity of the DiGA's components is shared between components via dedicated sessions:
  - All session data is protected by appropriate technical measures, during both exchange and storage, with the protection requirements. The session IDs used, if applicable, are generated randomly, with sufficient entropy and using established procedures.
  - All sessions are set up in an instance of a DiGA invalidated when its use is aborted or ended, and the user can also force the explicit invalidation of a session.
  - Sessions have a maximum validity period and inactive sessions are automatically invalidated after a certain period of time.
  - The invalidation of a session results in the deletion of all session data and a session that has once become invalid cannot be reactivated even if individual session data is known.

ACCESS CONTROL

- The DiGA ensures that every access to protected data and functions goes through an authorization check ("complete mediation"), for which a dedicated authorization component, including all protected data, is used for access by operating personnel of the manufacturer ("reference monitor" or "secure node/application"), which requires prior secure authentication of the accessing person.
- All authorizations initially and restrictively are assigned by default and authorizations are only extended via controlled procedures that include effective checking and control mechanisms based on a multiple-eye principle when the authorizations for operating personnel of the manufacturer are changed.
- If the DiGA provides for different user roles, each role can only access functions with the rights required to execute the functionalities associated with the role.
- You have ensured that access to functions and data by your operating personnel is only possible via secure networks and access points.
- All errors and malfunctions of the access control result in a denial of access.

INTEGRATION OF DATA AND FUNCTIONS

- Only the insured can move within the trust domain of the DiGA or a trustworthy external content checked by you.
- If the DiGA allows the user to upload files, such function is restricted as much as possible (e.g., excluding active content), a security check of the content takes place, and you have ensured that files can only be saved in the specified path.

LOGGING

- The DiGA can carry out complete, traceable, falsification-proof logging of all security-relevant events, i.e., the secure identification, authentication, and authorization of individuals and organizations.
- Logging data are automatically evaluated by you in order to recognize security-relevant events or to prevent them proactively.
- Access to logging data is secured by a suitable authorization management system and restricted to a few authorized individuals and defined purposes.

REGULAR AND SECURE UPDATES

- You inform the person concerned (e.g., via push mechanisms or before a user starts the DiGA) if a security-relevant update has been made available for installation or carried out.

HARDENING

- If DiGA services can be called up via web protocols:
  - Methods of the protocols used that are not required are deactivated for all services that can be called via open networks.
  - You have restricted the permitted character encodings as much as possible.
  - You have limited values for access attempts set for all services that can be called via open networks.
  - You have ensured that no safety-related comments or product and version information are disclosed.
  - You regularly delete unnecessary files.
  - You have ensured that these services are not recorded by search engines.
  - There is no absolute local path information.
  - You have excluded the retrieval of source texts.
- If the DiGA processes data that is provided by the user or by sources not controlled by the DiGA:
  - You treat this data as potentially dangerous and validate and filter accordingly.
  - You check this data on a trustworthy IT system.
  - Incorrect entries, if possible, are not handled automatically or the relevant functionalities are reliably implemented so that misuse is excluded.
  - This data is encoded in a form that ensures that malicious code is not interpreted or executed.
  - This data is separated from specific queries to data-holding systems (e.g., via stored procedures) or data queries are explicitly secured against attack vectors benefiting from such data.
  - You have consistently ensured that errors in the DiGA are dealt with and lead to the abortion and possibly rolling back of the initiated functions.
  - The DiGA is protected against automated access by suitable protective mechanisms if these are not part of the intended use.
  - Configuration files relevant for secure operation are protected against loss and falsification by suitable technical measures.

USE OF SENSORS AND EXTERNAL DEVICES

- If the DiGA directly accesses the sensors of a mobile device and/or external hardware (e.g., sensors close to the body):
  - You have specified the framework conditions under which sensors or connected devices can be installed, activated, configured, and used and you have ensured the existence of these framework conditions as far as possible before carrying out the corresponding functionalities.

- The DiGA ensures that sensors and connected devices are set to a basic setting during installation or initial activation, which corresponds to a documented safety guideline.
- The user can reset sensors and devices directly controlled by the DiGA to a basic setting that corresponds to a documented safety guideline.
- Data exchange between the DiGA and directly controlled sensors or devices is only possible when the installation and configuration of the sensors or devices has been completed.

- If the DiGA exchanges data with external hardware (e.g., body-hugging sensors):
  - The processes for installing, configuring, activating, and deactivating this hardware are described appropriately for the target group and, as far as possible, secured against incorrect operation.
  - There is a mutual authentication between the DiGA and external hardware.
  - Data between the DiGA and external hardware will only be encrypted after an initial connection.
  - You have ensured that if the DiGA is uninstalled or if its use is ended, all data stored on external hardware will be deleted.
- You have documented how connected hardware can be safely deactivated so that no data is lost and no sensitive data remains on the device.

THIRD-PARTY SOFTWARE

- You must keep a complete list of all libraries and other software products used in the DiGA that were not developed by you as the manufacturer.
- You use suitable methods of market observation to ensure that previously unknown risks for data protection, data security, or patient safety emanating from these libraries or products are identified promptly.
- You have established procedures to take appropriate measures in the event of such identified risks to be able to immediately block the app and notify users.

ADDITIONAL REQUIREMENTS FOR DIGAs WITH VERY HIGH PROTECTION REQUIREMENTS

- Personal data processed on IT systems that are not at the personal disposal of the user are only stored in encrypted form on these systems.
- You have carried out a penetration test for the version of the DiGA to be included in the directory, considering common attack vectors such as clickjacking or cross-site request forgery, among others.
- You have documented the results of the penetration tests and the results of the processing of the measures or recommendations and, if necessary, transferred them to suitable management systems.
- You will enforce a two-factor authentication at least for the initial authentication of all users.
- If the DiGA allows a fallback option to one-factor authentication:
  - The user is made aware of the associated risks and such a relapse is only activated after the user has given their consent, which has been confirmed by an active action.
  - The user can deactivate this relapse option at any time from within the DiGA.
- The DiGA can support authentication of insured persons as the user via an electronic health card with a contactless interface by December 31, 2020, at the latest.
- Messages (XML, JSON, etc.) and data are sent to DiGA services accessible via open networks checked against defined schemes.
- If components are web servers, e.g., for administration or configuration:
  - The web server is configured as restrictively as possible.
  - Only the required components and functions of the web server are installed or activated.
  - The web server is not operated under a privileged account.
  - Security-related events are logged.
  - Access is only possible after authentication.
  - All communication with the web server is encrypted.

It is important to understand that the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, or BSI) which helps organizations identify and implement measures to help secure IT systems has created a baseline set of standards for protecting information technology (in German, IT-Grundschutz). These BSI standards consist of:

- An ISMS based on ISO/IEC 27001 standards (BSI-Standard 100-1)
- The IT-Grundschutz methodology, which describes how to set up and operate an ISMS (BSI Standard 100-2)
- A risk analysis method (BSI Standard 100-3)
- The IT-Grundschutz Catalogues, a standard set of potential threats and safeguards against them for typical business environments.

Also, it is important to note that ISO/IEC 27001 is a security standard that formally specifies an ISMS that is intended to bring information security under explicit management control. As a formal specification, it mandates requirements that define how to implement, monitor, maintain, and continually improve the ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. Certification to ISO/IEC 27001 helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.

ABOUT THE AUTHOR

John Giantsidis is the president of CyberActa, Inc, a boutique consultancy empowering medical device, digital health, and pharmaceutical companies in their cybersecurity, privacy, data integrity, risk, SaMD regulatory compliance, and commercialization endeavors. He is also a member of the Florida Bar's Committee on Technology and a Cyber Aux with the U.S. Marine Corps. He holds a Bachelor of Science degree from Clark University, a Juris Doctor from the University of New Hampshire, and a Master of Engineering in Cybersecurity Policy and Compliance from The George Washington University.

GERMANY'S DIGITAL MEDICAL DEVICE REGULATIONS: A FRAMEWORK FOR THE WORLD TO FOLLOW, PART III

John Giantsidis
President & Principal Consultant, CyberActa, Inc.

This last article in this series has to do with the remaining requirements pertaining to the DiGA application (interoperability, robustness, consumer protection, and patient safety). Emphasis is on the adherence of ISO/IEEE 11073 Health Informatics — Medical/Health Device Communication Standards enable communication between medical, healthcare, and wellness devices and with external computer systems. They provide automatic and detailed electronic data capture of client-related and vital signs information, and of device operational data.

INTEROPERABILITY

- The data processed can be exported by the user in an interoperable format from January 1, 2021, at the latest and made available to the insured person for further use.
- The export takes place in or using an open, recognized international standard or in a profile you have disclosed as using an open, recognized international standard.
- The user can export relevant excerpts from the health data processed via the DiGA for their care, particularly regarding therapy progress, therapy planning, therapy results, and data analyses carried out from the DiGA by January 1, 2021, at the latest. The export takes place in a human-readable and printable format and takes into account the care context in which the DiGA is typically used according to its intended purpose.
- The DiGA must be able to collect data from medical devices used by the user or from sensors worn by the user to measure and transmit vital signs (wearables), and the DiGA supports a published and documented profile from January 1, 2021, at the latest ISO IEEE 11073 standard
- The standards and profiles used to establish the interoperability are published or linked on the application website and can be used without discrimination and implemented in their systems by third parties.

ROBUSTNESS

The DiGA is robust against malfunctions and operating errors by demonstrating that:

- Sudden power failure does not result in loss of data.
- Sudden internet connection failure does not result in data loss.
- The DiGA checks the plausibility of measurements, inputs, and other data from external source.
- The DiGA includes functions for testing and/or calibrating connected medical devices and sensors.

CONSUMER PROTECTION

- The user receives all the information they need to make a usage decision before commitments are made to you or a third party. In the information on the sales platform or on the application website, the range of functions is fully described, and the medical purpose is fully reproduced. The information on the sales platform or the application website clearly shows which features are available with the download or use of the application and which features are available at what price, e.g., can or must be purchased as in-app purchases or function redirects.
- The compatibility with systems and devices is communicated transparently. You have published a list of compatibility commitments regarding operating system versions and mobile end devices or web browsers and web browser versions as well as other required or optionally usable devices on the application website and you are keeping this list constantly up to date.
- You must publish the DiGA's medical purpose.
- The usage conditions are designed in a consumer-friendly manner:
  - The DiGA is ad-free.
  - It does not contain any non-transparent offers such as auto-renewing subscriptions or time-limited specials.
  - It contains measures to protect against unintentional in-app purchases or does not offer in-app purchases
- You have implemented measures to support users by providing free German-language support in operating the DiGA, which answers user inquiries within 24 hours at the latest.

EASE OF USE AND ACCESSIBILITY

- Usability style guides of the respective platform for mobile applications have been fully implemented, or alternative solutions have been implemented for which user-friendliness can be demonstrated.
- Easy and intuitive usability was confirmed in tests with focus groups representing the target group.
- The DiGA offers operating aids for people with disabilities by January 1, 2021, at the latest, or supports the operating aids offered by the platform.

SUPPORT FOR SERVICE PROVIDERS

- You provide information for integrated service providers in which the additional use of the app by a service provider is disclosed and clearly describe the underlying roles for the service provider and patient.
- You provide information for integrated healthcare providers that describes how the DiGA's use can be explained to the insured as part of the therapy.
- The user can activate their own data access for the service providers to be involved or transmit data securely to the service providers.

QUALITY OF THE MEDICAL CONTENT

- The DiGA is built on secured medical knowledge and makes this transparent:
  - The medical content and procedures implemented in the DiGA are based on the generally recognized professional standard.
  - You have established suitable processes to keep the medical content and procedures implemented in the digital health application up to date.
  - The sources for the medical content and procedures implemented, for example, guidelines, textbooks, and studies, are published and named in the DiGA or on a website linked from the DiGA.

- The studies carried out with the DiGA are published and named in the DiGA or on a website linked from the DiGA.

- The health information with which the DiGA supports the user is appropriate:
  - It is based on the generally recognized professional standard, it is tailored to the target group, and it is offered on a case-by-case basis and in the context of the respective use.
  - You have established suitable processes to keep the health information up to date.
  - The sources for the health information are published and named in the DiGA or on a website linked from the DiGA.
  - Didactic procedures are implemented to deepen and strengthen the health knowledge offered.

PATIENT SAFETY

- You clearly state on the sales platform or before the web application is started for which users and indications the DiGA should not be used, if there are restrictions.
- In the DiGA, the user is given context-sensitive information on risks as well as information on suitable measures to mitigate or avoid them.
- In the context of critical measured values or analysis results, the DiGA clearly indicates the need or the usefulness of consulting a doctor or another service provider.
- The DiGA recommends the user to discontinue use of the app or to change the use of the app if a defined state is determined.
- Consistency conditions are defined for all values entered by the user or collected via the connected medical devices or sensors or taken from other external sources, which are checked before a value is used.
- Error messages are designed in such a way that the user can understand where the error was and how they can contribute to avoiding it in the future.

CONCLUSION

A DiGA can be a native app or a desktop or browser application, and can also comprise devices, sensors, or other hardware in addition to software, such as wearables, if the main function is a predominantly digital one. If the requirements regarding security, functionality, quality, data protection, data security, and interoperability are met, along with evidence of positive healthcare effect, a digital medical device (class I or IIa) can achieve admission to the DiGA directory and be used by anyone of the 73 million participants in the German statutory health insurance with the corresponding reimbursement rate.

ABOUT THE AUTHOR

John Giantsidis is the president of CyberActa, Inc, a boutique consultancy empowering medical device, digital health, and pharmaceutical companies in their cybersecurity, privacy, data integrity, risk, SaMD regulatory compliance, and commercialization endeavors. He is also a member of the Florida Bar's Committee on Technology and a Cyber Aux with the U.S. Marine Corps. He holds a Bachelor of Science degree from Clark University, a Juris Doctor from the University of New Hampshire, and a Master of Engineering in Cybersecurity Policy and Compliance from The George Washington University.

ABOUT US

MED DEVICE ONLINE

Med Device Online is committed to advancing human health by connecting people, organizations, and ideas in the medical device industry. Readers come to us for the information they need to make critical decisions during the early phases of medical device and diagnostics development.

We provide in-depth editorial content focused on business solutions, industry best practices, and thought leadership across a wide range of topics, including product management, R&D, regulatory, manufacturing/operations, quality, reimbursement, sourcing/supply chain, corporate management, and many others.

MedDeviceOnline.com

info@MedDeviceOnline.com

724.940.7555

2009 Mackenzie Way #280, Cranberry Twp, PA 16066