Review

Development and Regulation of Connected Combined Products: Reflections From the Medtech & Pharma Platform Association

Thomas C. Kühler, PhD[1]; Marc Schoenmakers, BS[2]; Oliver Shergold, PhD[3]; Stephan Affolter, BS[4]; Winona Rei Bolislis, MA[1]; Ruth Foster, BSc[5]; Paul Gardner, BEng[6]; Svenja Hruschka, PhD[7]; Thierry Jomini[8]; Sathish Kaveripakam, MA[9]; Karl Mayerhofer, PhD[10]; Tomaso Scherini, PDEng[11]; Marta Swierczynska, PhD[12]; Gretchen Vandal, MS[13]; and Shayesteh Fürst-Ladani, MS[14]

[1]Global Regulatory Science and Policy, Sanofi R&D, Chilly-Mazarin, France; [2]Product Quality, Regulatory, and Compliance, Philips Engineering Solutions, Eindhoven, the Netherlands; [3]Connected Health Product Development, Novartis Pharma AG, Basel, Switzerland; [4]Strategic QM&RA, Ypsomed AG, Burgdorf, Switzerland; [5]Device and Digital Health, MSD France, Courbevoie Cedex, France; [6]Congenius AG, Dietikon, Switzerland; [7]Boehringer Ingelheim microParts GmbH, Dortmund, Germany; [8]Anteris Helvetia AG, Kuessnacht, Switzerland; [9]Connected Health Product Development, Global Drug Development, Novartis Pharma AG, Basel, Switzerland; [10]Regulatory Affairs, Ypsomed AG, Burgdorf, Switzerland; [11]Business Development, Philips Engineering Solutions, Eindhoven, the Netherlands; [12]Regulatory Affairs, SFL Regulatory Affairs & Scientific Communication, Basel, Switzerland; [13]Global Regulatory Affairs, Digital Health and Software Medical Devices, Sanofi, Cambridge, Massachusetts; and [14]SFL Regulatory Affairs & Scientific Communication, Basel, Switzerland

ABSTRACT

Purpose: Patients taking a medicinal product in a homecare setting typically use a medical device to facilitate the injection process. Reductions in wireless connectivity costs, combined with the rapid adoption of smartphones with connectivity to cloud-based services, are enabling these drug delivery devices to now be connected to a digital ecosystem as connected combined products (CCPs). The purposes of this article are to identify the challenges in developing and releasing these products when they straddle different regulatory frameworks and standards and to highlight gaps in the European Union regulations.

Methods: Industry subject matter experts from pharmaceutical, medical device, and consultancy companies, who are members of the Medtech & Pharma Platform Association, formed 4 working groups to address current best practice for developing and releasing CCPs and the different relevant regulatory frameworks. The 4 areas studied were clinical and regulatory, usability and human factors engineering, development and life cycle management, and cybersecurity.

Findings: Development teams require new skills to create innovative products that have a good safety profile and are simple to use, such as design thinking to understand user needs and systems engineering to manage complexity and ensure interoperability. Risk management process should integrate cybersecurity, data privacy, and data integrity, whereas design control processes should enable asynchronous development

Accepted for publication March 14, 2022
https://doi.org/10.1016/j.clinthera.2022.03.009
0149-2918/$ - see front matter

© 2022 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

cycles for hardware and software components. Regulatory frameworks exist for individual components within the CCP. However, for a complex product, regulatory guidance is needed when combining components with different risk and safety profiles and to ensure that the responsibilities and liabilities of companies contributing components are clear. The efficient management of software changes and product updates, as well as dealing with end-of-life hardware and backward compatibility to older software versions, needs agile approaches when it comes to regulatory updates.

Implications: The regulatory uncertainties and development processes outlined in this article need to be addressed. We call for joint discussions among the various stakeholders in the fields of medicinal products, medical devices, and *in vitro* diagnostics, as well as standalone software, data protection, and cybersecurity experts, together with regulators and lawmakers in the European Union to meet in focused discussion groups with the aim of devising pragmatic solutions and regulations for the benefit of the sector and hence the patients it serves. (*Clin Ther.* 2022;44:768–782.) © 2022 The Authors. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Keywords: Combination products, connected combined products, digital health, medical devices, medicinal products, software.

INTRODUCTION

Patients administering a medicinal product in a homecare setting typically use a medical device, such as an autoinjector or pen injector pump, to facilitate the injection process. These drug delivery devices can be mechanical or electromechanical, disposable or reusable, and supplied with the drug or separately, by the same legal manufacturer or separate legal manufacturers.

Reductions in wireless connectivity costs, combined with the rapid adoption of smartphones with connectivity to cloud-based services, are enabling these drug delivery devices to now be connected to a digital ecosystem. The components of this ecosystem may include a smartphone application for the patient to plan, control, and record their injections or cloud storage systems to collate their data in a medical health record, which their health care professional can access to track their medical status. Additional cloud-based services could include algorithms to analyze the data and provide recommendations on their disease progression and possible medical interventions, as well as educational material for the patient to understand their condition and manage it or to train themselves in how to administer an injection.

Examples of connected reusable electromechanical autoinjectors include Bayer's Betaconnect™ and Amgen's AutoTouch®, whereas Insulet's Omnipod Dash® features a disposable patch pump with connectivity to a smartphone application.[1–3]

There is no standard regulatory classification for a drug and delivery device combination with or without connectivity. For example, in the United States, the device may be classified as a standalone medical device or as part of a combination product when it is integrated with the drug, copacked with the drug, or referenced by the drug.[4] In the European Union, a device combined with a medicinal product may be classified as a medical device or as a medicinal product, depending on the principal intended action. In the latter case, the type of combination may be integrated, copacked, or obtained separately.[5] Therefore, for the purposes of this article, we refer to connected combined products (CCPs) as the use of a medicinal product with ≥2 of the following products with wireless connectivity: a drug delivery device, an *in vitro* diagnostic (IVD), standalone software on a mobile platform, and/or a cloud application, with the aim of delivering a medicinal product to patients and monitoring certain data and parameters, such as medical adherence.

CCPs are more complex than combined products to develop, achieve regulatory approval, use, and maintain. CCPs consist of mechanical, electronic, and software components that are developed and qualified according to different processes and timescales yet must work seamlessly as an integrated system. The components that constitute the CCP may be regulated as a medicinal product, a medical device (including medical device software [MDSW]), an IVD, or commercial grade software and sensors. Each component can have a different intended purpose as well as safety profiles and risk levels. Patients are expected to operate these products in an effective manner with minimal or no instruction from a health care professional. Patients also expect these products to ensure their

data privacy and be robust to cybersecurity threats. Regular updates of software components are to be anticipated to fix bugs, upgrade software, work on new operating system releases, and implement new features. The purpose of this article is to identify the challenges in developing and releasing CCPs and highlight and discuss gaps in the European Union regulations. We aim to stimulate discussions on how to address regulatory and development gaps that we identify in our analysis.

METHODS

The Medtech & Pharma Platform Association[6] is a nonprofit industry association that focuses on regulatory and policy developments for combined products. The Medtech & Pharma Platform Association established a working group on CCPs with industry subject matter experts from a number of pharmaceutical, medical device, and tech companies. The list of authors and their respective affiliations provides details on which companies were represented and the number of individuals in the working group.

The working group realized that there is a wide range of cases for how technology might be applied in the medical domain. The working group limited itself to the application of a CCP as mentioned in the introduction and defined as the use of a medicinal product with ≥2 of the following products with wireless connectivity: a drug delivery device, an IVD, standalone software on a mobile platform, and/or a cloud application, with the aim to deliver a medicinal product to patients and to monitor certain data and parameters, such as medical adherence.

Four workstreams were then formed to investigate the topics of clinical and regulatory, usability and human factors engineering,[7,8] development and life cycle management, and cybersecurity frameworks. Artificial intelligence and machine learning are rapidly evolving technologies with a highly disruptive potential and a dynamic regulatory environment that is considered only at high level in this article. It is a topic in its own right and is considered best addressed in more detail in a separate article.

Each workstream reflected on the current state of the art and its practice in relation to a CCP. Each workstream also identified areas for improvement to manage this class of products efficiently and practically. The workstream members gathered information from the European Medicines Agency (EMA), Notified Bodies and other national competent authorities, and the European Commission. When required, literature searches were conducted in PubMed®. All working groups contributed with best practice experience from their respective companies in their capacities as subject matter experts.

The working group decided to limit deliberations to the European Union regulatory framework by assessing European Union regulations for CCPs that are regulated by different regulatory frameworks, such as medicinal products, IVDs, medical devices, including MDSW, and so on. Notwithstanding this, in certain instances, findings may also apply to other regulatory jurisdictions.

RESULTS

Results are presented in the following 4 sections, which reflect the investigated topics: Clinical and Regulatory Frameworks, Usability and Human Factors Engineering, CCP Development Process and Lifecycle Management, and Cybersecurity. The Table 1 provides a summary of legislation and guidelines relevant to these 4 sections.

Clinical and Regulatory Frameworks

Different regulatory strategies may be applied when developing a CCP, depending on if and how the elements (separate hardware and/or software components) of the product are classified and will be marketed. The classification of the components is determined by several factors based on intended purpose and risk-safety profile. For example, a CCP could include 1 of the 2 following options.

First, a single integral drug-device combination product could be used with a standalone MDSW in a combined way for a medical purpose, for example, a disposable patch pump with a drug and a companion application. In this case, the drug and delivery device combination will be authorized by the EMA or a national competent authority. The delivery device component must comply with Article 117 of the Medical Devices Regulation (MDR),[9] and a Notified Bodies Opinion confirming its compliance with the relevant General Safety and Performance Requirements set out in MDR Annex I will need to be obtained.[10] The standalone software will be classified as MDSW and will require CE marking; depending on the product risk classification, the conformity assessment process before CE marking[11] may involve a NB.

Table I. Summary of key legislation and guidelines pertaining to the development of connected combined products in the EU.

Legislation	Standards	Guidance
• Regulation (EU) 2017/745 • Regulation (EU) 2017/746 • Regulation (EU) 2016/679 • Directive 2001/83/EC • Regulation (EC) 726/2004 • Regulation (EC) 1901/2006 • Regulation (EC) 141/2000 • Regulation (EC) 1394/2007	• ISO 14971:2019 • IEC 62366-1:2015 • IEC 62366-2:2016 • IEC/TR 62366-2:2016 • ISO 13485:2016 • IEC 62304:2006 • ISO 14971:2019	• EMA Guideline on quality documentation for medicinal products when used with a medical device • IMDRF Principles and Practices for Medical Device Cybersecurity • MDCG guidance 2019-16 Rev.1 • ISPE GAMP 5 Guide: Compliant GxP Computerized Systems • AAMI TIR57 AAMI TIR57 Principles for medical device security - Risk management

AAMI = Association for the Advancement of Medical Instrumentation; EC = European Community; EMA = European Medicines Agency; EU = European Union; GAMP = Good Automated Manufacturing Practice; GxP = good practice regulations and standards; IEC = International Electrotechnical Commission; IMDRF = International Medical Device Regulators Forum; ISO = International Organization for Standardization; ISPE = International Society for Pharmaceutical Engineering; MDCG = Medical Devices Coordination Group.

The second option is a medicinal product, a delivery device, and a standalone software package for connectivity and registration of therapy adherence that are registered or CE marked separately but used in a combined way for a medical purpose, for example, a reusable insulin pump with software for bolus calculation and therapy management. Each CCP component will need to fulfill the requirements of the applicable legislation. The medicinal product will be authorized by a competent authority, whereas each medical device component (eg, delivery device or MDSW) will need to undergo the applicable conformity assessment process and be CE marked.

For these examples, the MDR and the *In Vitro* Diagnostic Medical Devices Regulation (IVDR)[12] address the regulatory framework for single integral DDCs regulated as medicinal products (MDR Article 117) and companion diagnostics essential for the effective use of the corresponding medicinal product (IVDR Article 2[7]).

However, neither the MDR nor the IVDR addresses the regulatory framework for product connectivity, including safety and the roles and responsibilities of different stakeholders when it comes to individually registered or CE marked medicinal products, medical devices, e/m-Health applications, or nonregulated products, which are used in a combined way for a medical purpose.

In addition, both regulations contain a provision that when the device is used in combination with other devices or equipment, the whole combination should not impair the specified performance of either of the individual devices. The challenge for the CCP manufacturer is to provide a strong safety and efficacy profile for components that do not have a medical purpose and hence have not been developed to comply with the medical device legislation.

Usability and Human Factors Engineering

Usability

CCPs are more complex than traditional integral DDCs, and the introduction of software and connectivity creates many opportunities to engage the user with additional features and functions. This means that the early-stage discovery phase on user needs and feature values becomes increasingly important as does ensuring usability across all the components once the product is developed.

The process described in Figure 1 is a useful approach to use in the early development phases to

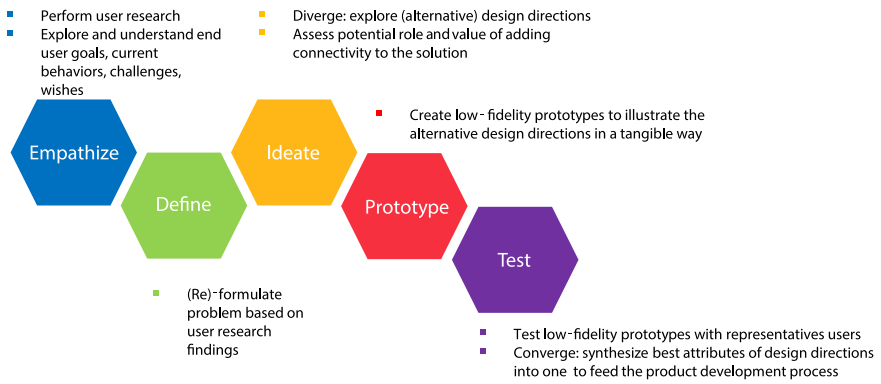

Figure 1. Key elements in the design thinking process according to the Hasso-Plattner Institute of Design. The proposed model aimed to provide practical reference to integrate design thinking best practices into the early development phases of a connected combined product.[8]

identify the user requirements and prepare the usability plan to be executed during product development. The process takes its inspiration from the Design Thinking Process proposed by the Hasso-Plattner Institute of Design at Stanford University.[13]

The first step is to empathize with the intended users, their environment, their tasks, and their current challenges and expectations related to their clinical workflow and tasks. Research performed with primary and secondary users will allow the project team to discover underlying user needs, goals, challenges, risks, and limitations. Building on the user research, the problem should be defined and possible design solutions ideated that can include connectivity and software. Throughout this process there should be a focus on the product value proposition for the patient, health care professional, and company, or several companies jointly, developing the CCP. Questions that can be asked include the following: Does connectivity introduce new risks, or increase them, related to data collection, corruption, or storage? What current user needs, or challenges, are connectivity addressing? What additional value will connectivity bring to the end user's clinical workflow? Is the added connectivity affecting the task flows of the primary user, or is it simply enabling data to be collected and processed by a secondary user or a third party? If connectivity has an effect on the tasks performed by the primary user, does it affect the primary function and risk profiles of the product? Is connectivity intended to improve the effectiveness of the product, for example, by supporting patients enhancing their therapy adherence? Do data collection, processing, and interpretation require patients to acquire new procedural knowledge or perform any new tasks?

Task analysis and risk assessment should be applied to understand and analyze the effect of connectivity on the task flow of the prospective users and inform design decisions. It is recommended even at this early stage to apply the principles of International Organization for Standardization (ISO) 14971 (Medical Devices – Application of Risk Management to Medical Devices)[14] as well as MDR Annex I, Chapter 1, Section 3, Use-related Risk Management.[9]

Once available, design concepts are prototyped and tested with representative users. Early-stage prototyping brings multiple benefits, from discovering potential design pitfalls and use-related failure modes to refining the user interface requirements as well as informing on the selection between competing designs.

Human Factors Engineering

Although the MDR does not provide any specific guidance on usability engineering practices to be followed when developing CCPs, the human factors engineering requirements for commercializing CCPs are similar to those for DDCs. Therefore, the provisions of MDR Annex I, Chapter 1: General Requirements, Chapter 2: Requirements Regarding Design and Manufacture, and Chapter 3: Requirements Regarding the Information Supplied With the Device[33] could be considered applicable to CCPs and should lead to the generation of input for the Marketing Authorization

Application. In addition, as described in Section 5.4, Usability Studies[15] of the EMA guideline on quality documentation for medicinal products when used with a medical device, the Marketing Authorization Application should include appropriate information on the usability of the drug-device combination product as defined for the intended patient population.

To address the expectations of the MDR while developing a CCP, it is recommended to refer to the content of the international standard for usability engineering International Electrotechnical Commission (IEC) 62366-1:2015 (Medical Devices – Part 1: Application of Usability Engineering to Medical Devices) and the technical report IEC 62366-2:2016 (Medical Devices – Part 2: Guidance on the Application of Usability Engineering to Medical Devices).[16,17] As mentioned in IEC 62336-1:2015, if the usability engineering process detailed in this standard has been complied with, then the usability of a medical device as it relates to the safety profile is presumed to be acceptable, unless there is objective evidence to the contrary. Data from summative human factors testing, as well as a summary of any residual risks and mitigation strategies, are expected to support this assessment.

Human factors methods for collecting user data described in IEC 62366-1:2015, such as contextual inquiries, ethnographic investigations, and, where applicable, digital data tracking methods, should be used to map out user flows and scenarios, understand user needs, and feed the risk analysis activities. Systems thinking should be applied to assess the effect of connectivity on the overall user journey, from unpacking and setting up the product to executing drug self-administration, as well as any active and passive steps related to data collection, transmission, and interpretation.

Because of the inherent complexity of CCPs, early and iterative human factors formative testing is highly recommended to progressively refine user interface requirements, identify use-related failure modes, and confirm and improve the effectiveness of any mitigation strategies designed into the product and its user interface. Formative tests can focus on specific hardware or software elements of the CCP to validate these specific design assumptions. However, it is critical that formative tests also progressively integrate CCP components to gain insights into whether the final product offers a coherent user experience. Connectivity offers the opportunity to improve the realism of the test and the quality of the data collected through real-time user behavior analysis and passive tracking.

Formative studies should focus on scenarios that are critical for the safety profile as well as outcomes that satisfy the product's primary function, including testing scenarios that involve connectivity. If the commercial relevance of the connectivity aspects of the product is high, for example, the connectivity related performance or benefits are mentioned as part of the product claim, testing the relevant connectivity scenarios as part of the formative testing is recommended.

Although there is no specific human factors guidance for the verification and validation of the connected functionality in the context of the MDR, as indicated in Annex I, Chapter 2, Section 14.1 of the Regulation,[33] the usability testing strategy should address the entire connected system.

Summative testing should also focus on effectively addressing critical scenarios, and connectivity should only be considered if part of this scope. Realistic testing of the connectivity-related scenarios with representative users and mature product samples is highly recommended as part of the product validation process.

CCP Development Process and Lifecycle Management

Development challenges for CCP products include managing the interfaces and ensuring interoperability among the different components and aligning development processes for hardware and software components. Medical device design controls according to ISO 13485 (Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes)[18] requires products to be designed by structured processes. The stage gates of design input, design output, design verification and validation, risk management, and design transfer can be separated according to a waterfall methodology[19] or partially or fully combined using the agile methodology.[20]

Mechanical and electronic hardware development processes differ from those of software development because of the steps required to physically manufacture the components and so will apply different development methods and timelines. Figure 2 is a visualization of the development process of a CCP. Once the overall project is clearly defined and initiated,

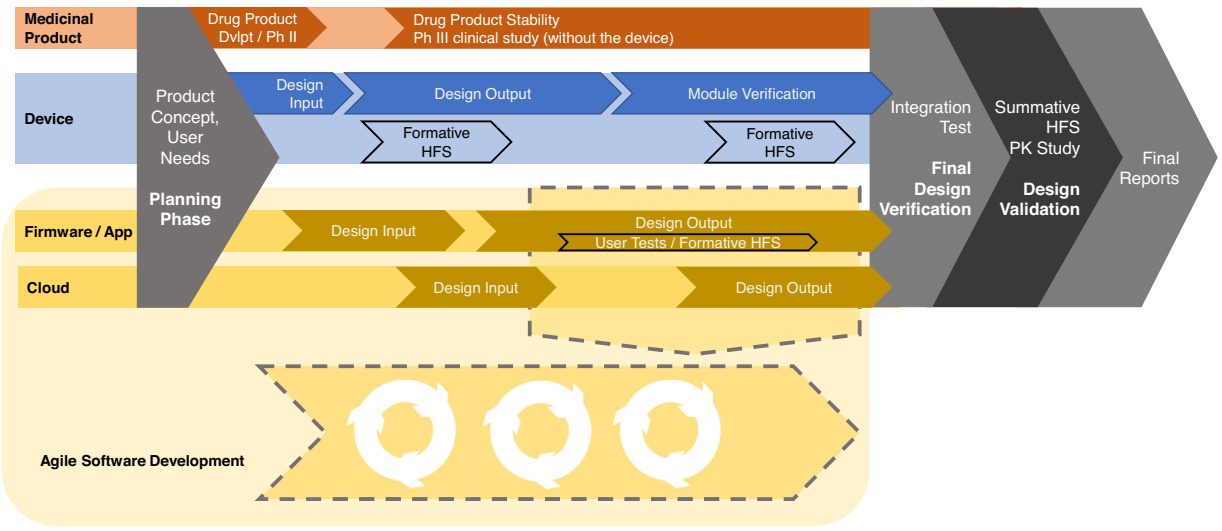

Figure 2. Schematic of the connected combined product (CCP) development process. Once the overall project is clearly defined and initiated, each component of the CCP (medicinal, device, and software) is developed in its own subprocess with careful attention on the interactions within the overall system. Each component may have different timelines and project phases that are not synchronized with the other components subprocesses. The software components are developed using the agile methodology. At the end of the subprocesses, an integration phase is performed to validate the design of the overall CCP as a system. A risk management process should accompany the overall development project taking all components into consideration. Dvlpt = development; HFS = human factor studies.

each component of the CCP (medicinal, device, and software) is developed in its own subprocess with careful attention on the interactions within the overall system. Each component has different timeline and project phases that are not synchronized with the other components' subprocesses. The software components are developed using the agile methodology. At the end of the subprocesses, an integration phase is performed to validate the design of the overall CCP as a system. A risk management process should accompany the overall development project, taking all components into consideration.

Careful definition of the product and component interface requirements facilitates the subsequent parallel building of hardware and software and allows for time and cost-efficient development. Lack of appropriate system requirements may result in a product or system that does not provide the expected interfaces or intended functionality, whereas overburdened requirements may result in overly complex products with extended development timelines and costs.

Systems Thinking

A system team should take responsibility for the definition of the overall system and the interfaces and integration of its components. This responsibility includes, in particular, risk management activities, which must address not only the individual CCP components but also the risk at the interfaces between the components and the interactions with the environment, including the user. Systems engineering[21] is a recommended method to handle the complexity of CCP development projects and ensures interoperability among the product components. In systems engineering, the product is decomposed into modules, each with a clear description of its requirements and interfaces to other modules within the overall product or system. This compartmentalized approach is suitable for more complicated electromechanical systems with connectivity, as well as additional components, such as mobile platforms and applications and cloud-based services. Because of this, systems engineering is already being applied to medical devices, such as pump systems, dialysis machines, and body scanners.

To prevent any system divergence, it is important to define requirements for the module interfaces, including interfaces to the medicinal product. The same holds true for any connectivity aspects to be implemented in each module. To ensure oversight over the interdependencies of the requirements and to ensure traceability of design inputs and outputs across all modules, a database tool for tracking design inputs, outputs, and verification data is highly recommended. Building and maintaining such a database are especially important in software development, where there are numerous input requirements to be traced.

Medicinal Product

Of all components in a CCP, the medicinal product has the longest development cycles and the least flexibility in terms of adaptation to other components in the system. Therefore, it must form the backbone of the CCP, around which all other components are developed. Existing connected solutions may be adapted to the medicinal product as applicable.

Hardware

Development of the hardware components of a CCP traditionally follows a waterfall methodology. Development cycles can be accelerated through rapid prototyping technologies, but the development of hardware components can still take several years.

Software

The agile methodology development principles are usually used when developing software. Experimental Physics and Industrial Control System or customer business requirements define the overall product or system requirements that are translated into software requirement specifications. In the first stage, a minimum viable product is developed that is usually based on a commercially established software architecture. This initial product is improved through a series of iterations. Each iteration involves the process of specifying, assessing risks, coding, testing, and documenting the improvement and can focus on ≥ 1 software items or units as well as checking interfaces to other hardware and software elements, such as the connectivity functionality.

A similar approach can be applied to the component design verification to support the overall product or system validation, which can be performed stepwise with the available units and repeated if an incremental improvement to the source code has taken place during the iteration. With this approach, functional software prototypes are available very early in the development and can be used for hardware testing and in formative user studies and even clinical trials. On the other hand, hardware prototypes or simulators can be created to facilitate early software development.

If the software is classified as a medical device, it can reference standard IEC 62304 (Medical Device Software – Software Life Cycle Processes) for medical device software life cycle processes.[22] In addition to the general expectations for software development, such software needs to meet Good Manufacturing Practice requirements, including readability and traceability.

Integration

Timing and synchronization are essential for the integration of the different modules into the final product or system as each module is developed at a different pace. This is especially important for (1) confirming product use cases and interface requirements, (2) meeting expected stage gates in traditional design controls, (3) preparing for integrated testing, (4) conductive summative studies, and (5) preparing for clinical trials or the actual launch of the CCP.

Once each module is ready for verification, the design should be frozen and reviewed. According to ISO 13485, after design freeze and design output, any further changes to the design must be under a documented change control procedure, and all relevant design documents must be updated accordingly. The module data and report are considered valid once they reach the design verification stage of the CCP as long as there are no further changes to the module design.

Product Lifecycle Management

Regular maintenance of the CCP components after product launch is essential. Maintenance is especially frequent for software and includes fixing bugs or errors, adding new features, and resolving cybersecurity threats. Because these connected devices are distributed globally, providing solutions in such situations may require significant resource and time.

The software maintenance process (lifecycle management) needs to be set up in advance and should include procedures for change management, documentation, and traceability. IEC 62304 provides a useful framework to this end. IEC 62304 calls for a systematic

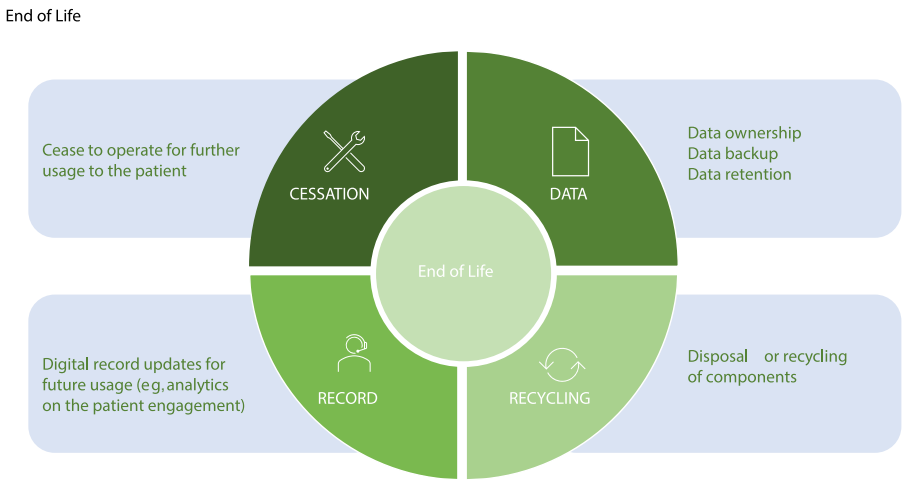

Figure 3. End of life of a connected combined product. The schematic shows the activities related to the end-of-life and the afterlife of a connected combined product, including the 4 areas that must be addressed thoroughly to ensure a smooth handling of such a product.

analysis of problems and changes that occurred in connection with the software application, including appropriate communication with users and responsible authorities. In addition, the standard describes how changes must be implemented and released in an orderly manner. The standard requires that the manufacturer reports, investigates, and informs involved parties of risks that arise in connection with the use of medical device software. The manufacturer should also keep all records and conduct a trend analysis of functionality and safety issues from postmarket surveillance monitoring. The process concludes with audit documentation.

End of Life

For CCPs, it is necessary to have effective procedures that ensure proper decommissioning, documentation, and data archiving for software. The procedures must consider different needs for hardware, software, and data disposal. The combination of a medicinal product with hardware and software components creates unique challenges at the end-of-life and afterlife periods of the CCP (Figure 3). It is important to consider options for the disposal and recycling during design and development of the CCP and how these fits within the circular economy. Hardware disposal is usually regulated at a country-specific level and can include contradicting or challenging requirements for biohazard material combined with electronic components and batteries within a single inseparable unit.

Decommissioning activities related to the software include the stopping of maintenance, support, and distribution in a managed way and are important to minimize the effect on public health. The activities may include deactivation and removal of the software and its supporting data; configuration management of the documentation, source code, or the delivered software; and communicating a plan to the user for effectively stopping maintenance and support of the software. The decommissioning of software data is particularly challenging because, although use of the product and/or access may stop, the MDR dictates that the data must be appropriately archived and not destroyed.

Manufacturers of CCPs must ensure the confidentiality, integrity, and availability of all electronic health information. Furthermore, they must protect against any reasonably anticipated threats or hazards to the security or integrity of such information and any reasonably anticipated unauthorized uses or disclosures of such information. Manufacturers are also obligated to ensure compliance by their workforce with these requirements.

Cybersecurity

Cybersecurity and maintaining data integrity are integral parts of any CCP development and need to

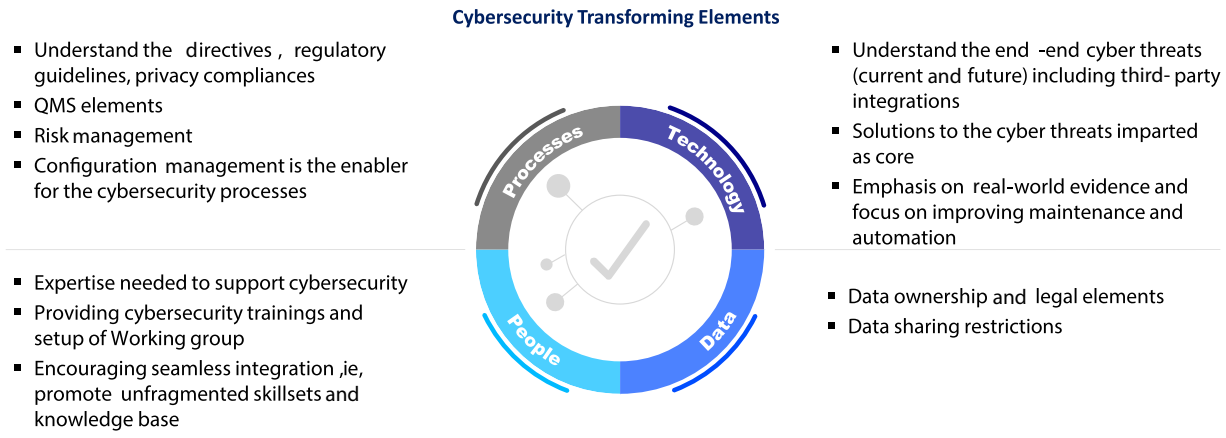

Figure 4. Cybersecurity transforming elements that need to be considered for a successful cybersecurity-compliant product taking underlying elements, such as directives, risk, quality, and configuration management, into account. QMS = quality management system.

be continuously managed throughout the product's lifecycle. In the European Union, cybersecurity of medical devices is considered part of the General Safety and Performance Requirements of the MDR.[23] In addition, the General Data Protection Regulation introduces certain data requirements and provides European Union residents fundamental rights over their data and the protection of these data.[24]

Next to the European Union legislation, the following guidelines on medical device cybersecurity should be considered when developing a CCP: International Medical Device Regulators Forum Principles and Practices for Medical Device Cybersecurity guidance[25]; Association for the Advancement of Medical Instrumentation technical information report on principles for medical device security in the context of the safety risk management process required by ISO 14971[26]; and Medical Devices Coordination Group guidance 2019-16 on cybersecurity for medical devices.[27]

Based on the use cases and intended purpose of the software, security features such as monitoring functionality or watchdogs need to be considered during the development process and from an operational point of view. Figure 4 illustrates the various transforming elements needed in successfully addressing cybersecurity requirements.

Security threats, including those related to third-party and/or customer installations, need to be considered early in the development process. Some of the security activities, such as holistic architecture review, penetration testing, threat modeling, static application security testing, dynamic application security testing, and relevant risk management, help to uncover the potential vulnerabilities within the CCP and influence the confidentiality, integrity, availability of critical and/or sensitive data. Cybersecurity for a medical device needs to address the constant evolution of emerging technologies, processes, and skills. Addressing these factors can be achieved by adopting a proposed strategic framework (Figure 5) that considers the different elements of a CCP, such as the technology, people, process, and data.

In terms of technology, several approaches can be used to assess the various cybersecurity aspects. For example, the Microsoft Threat Modeling Method[28] defines 6 threats in certain cybersecurity properties and possible mitigation measures that can be adopted to address them. In addition, the Development, Security, and Operations[29] process can also be used to define and consider security aspects during the software development cycle rather than at the end of the lifecycle.

DISCUSSION

CCPs offer tremendous opportunities to improve the standard of patient care and improve the efficiency and effectiveness of health care professional workflows throughout the patient journey.[30,31] However, CCPs are complex products or systems that consist of

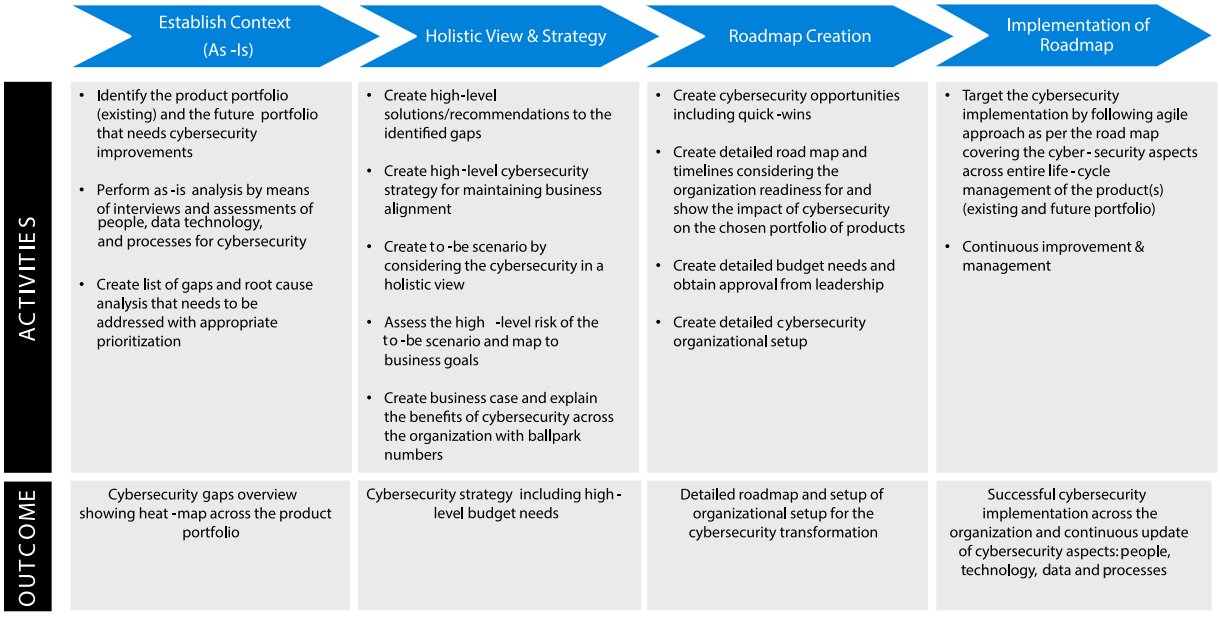

Figure 5. Proposed strategic framework in addressing cybersecurity aspects. The schematic showing a 4-step phased approach comprising elements that are considered key cornerstones for successfully implementing cybersecurity across an organization and its products.

hardware and software components that are, as we have illustrated, developed under a range of separate regulatory frameworks that have not always been developed in a concerted fashion. This complexity renders a number of regulatory and development challenges that need to be properly mastered and addressed when developing a CCP to ensure that the final product is user-friendly (intuitive), has a good safety profile, and minimizes risk.

Competent authorities in the European Union are aware of the risks and challenges related to medical devices connected to cloud applications directly via the internet or by other means of communication, such as Bluetooth or Near Field Communication technologies, but there is no program implemented to assess these vulnerabilities or to validate complex systems of components, such as in CCPs. The US Food and Drug Administration is beta-testing a program (Pre-Cert) for certification of Software as a Medical Device, which is covering part of the risks associated with a CCP. The CCP, being a combination of software and hardware elements or parts using existing platforms for connecting (nonmedical intended) or specific developed means of connectivity, should follow a complete certification program to guarantee efficacy of the complete (CCP) system.

Regulatory Challenges

Within the European Union, there are regulations, (harmonized) standards, guidelines, and common specifications on how to develop the individual hardware and software components that make up a CCP according to its intended purpose, risk profile, and classification. However, legislation is not always clear on how to define, develop, test, and manage risks when combining these individual components into a CCP. Guidance is especially needed when these components have different risk and safety profiles or when they fall under different regulatory frameworks, such as medicinal products, IVDs, medical devices including MDSW, validated software systems, or commercial software and hardware. Otherwise, the risk is that all components within the ecosystem must adopt the highest risk and safety profile of any individual component, increasing development and maintenance costs and timelines. In addition, regulatory departments used to dealing with pharmaceutical products may be called on to assess medical device components outside their normal area of expertise.

Components of the system may initially be developed for nonmedical use and marketed or distributed by different companies. Guidance is required regarding the responsibilities and liabilities of each company when these components interact with each other. In particular, clarification is required to ensure good efficacy and safety profiles and to manage patient risk, as well as the issues related to data integrity, security, and privacy when transmitted between components and managing cybersecurity threats.

Lifecycle management of MDSW is faster than that for medicinal products and medical device hardware. Frequent updates are needed for security and safety relevant issues, and software applications undergo rapid development as new features are added. Software versions may be retired as new ones are released.

Regulatory guidance on the effective and safety-related management of these types of implementations (updates or changes) is needed, such as what level of change must be submitted to regulators or local authorities and whether minor changes can be bundled and submitted retrospectively through a notification process on a regular interval, for example, once a year. Without these agile approaches, there could be a significant slowdown in product innovation and overloading of regulatory teams dealing with update requests. In addition, although regulatory guidance defines how to manage end-of-life hardware, additional guidance is required for connectivity, cybersecurity, and effective data management and backward compatibility (efficacy related).

Development Challenges

In the early project stages, time and care are needed to understand the full range of users and their respective needs and to identify the value that the technical solutions could bring. Design thinking and usability processes provide a framework for achieving this. Systems engineering can define the product, structure the individual components, and ensure robust interfaces between them. Only when the product requirements and architecture are fully understood, along with the intended purpose and regulatory strategy, should product development activities under design controls start.

Each component's development can have its own dedicated team, with defined work packages, development plan, input requirements, design output, risk assessment, and verification activities. Module development can progress independently of each other, except for where interface requirements need to be defined and tested.

Holistic thinking at the system level and collaborative teamwork are essential to managing the complexity of CCPs and ensuring robust interfaces between individual components and a coherent user experience. This procedure will include deeper integration between product development teams and information technology functions, which typically already have dedicated functions for dealing with data privacy, data integrity, and cybersecurity issues, as well as providing data infrastructure.

Usability and human factors engineering must not only focus on formative and summative testing of critical functions for regulatory submission but also consider how to test the overall product to ensure end-user satisfaction. Real-time monitoring of the product through application monitoring tools can provide insights into how to improve the user experience.

Systems engineers must consider how to integrate, verify, and validate all the components, both regulated and nonregulated. Functional software prototypes are available very early in the development and can be used for hardware testing in formative user studies or even in clinical trials. Component design verification can be performed stepwise with the available units and repeated if an incremental improvement to the source code has taken place during the iteration. Similarly, hardware prototypes or simulators can be created to facilitate early software development. They will have to consider the information technology cloud backbone, which typically follows the International Society for Pharmaceutical Engineering Good Automated Manufacturing Practice standard on good practice regulations and standards[32] as well as software services and applications hosted on the cloud that may be classified as good practice regulations and standards or medical device. In addition, they should also address requirements regarding cybersecurity, data integrity, and data privacy and ensure that system-wide threat modeling and penetration testing occurs.

Risk management should include risks associated with cybersecurity, data integrity, and data privacy and how this may affect the therapeutic effect or patient safety. Data integrity issues can include distortions of the data stream arising from electromagnetic disturbances, signal blockages, or software errors.

Hackers may gain control of the medical device and cause an overdose or underdose.

Integral risk management should also consider the technical complexity of introducing connectivity into the product. In particular, multiple connectivity options may be offered, such as Bluetooth, Wi-Fi, and Near Field Communication, each with its own security and data transfer protocols and transfer speeds.

Limitations of the Present Study

This article focuses on how medicinal CCPs are regulated in the European Union. Although some of the problem statements articulated may have a broader geographic reach and apply to other regulatory jurisdictions, we have not attempted to analyze those. In addition, artificial intelligence is a rapidly evolving area with a significant regulatory gap that we have not discussed in this article.

CONCLUSIONS

The ability to connect drug delivery devices to a wider digital ecosystem of diagnostic sensors and software applications brings new challenges for product development teams and regulators. Development teams need to learn new skills and methods to create innovative products that, although technically complex, are simple to use and have a good safety profile for patients and health care professionals. In particular they should (1) use design thinking to understand the user needs; (2) implement systems engineering to manage complexity and ensure interoperability among components; (3) integrate cybersecurity, data privacy, and data integrity into existing risk management processes; and (4) adapt design control processes to allow for asynchronous development cycles for hardware and software components and the continuous evolution of the product ecosystem as components are updated or added. Regulatory frameworks exist for individual components within the CCP. However, for a complex product, regulatory guidance is needed on the following: (1) combining components with different risk and safety profiles, particularly if they fall under different regulatory frameworks; (2) the responsibilities and liabilities of companies, who contribute components to a digital ecosystem, especially in the areas of patient tolerability and risk, as well as data integrity and cybersecurity; and (3) the efficient management of software changes and product updates, as well as dealing with end-of-life hardware and backward compatibility to older software versions.

This article focuses on medicinal CCPs regulated in the European Union, but some of the issues discussed could potentially also apply to other regulatory jurisdictions. To address the regulatory issues and development processes outlined in this article, we call for joint discussions among the various stakeholders in the field of medicinal products, medical devices, and IVDs, as well as standalone software, data protection, and cybersecurity experts, together with regulators and lawmakers in the European Union.

DECLARATION OF INTEREST

All authors hold positions in commercial companies, but they have not received any grant, honoraria, or other compensation to author this article. The study was conceived of, executed on, and written during the authors' day job. Authors may hold shares and/or stock options in their respective companies. The authors have indicated that they have no other conflicts of interest regarding the content of this article.

ACKNOWLEDGMENTS

We thank Samuel Gavillet at the Medtech & Pharma Platform Association for organizing the meetings and taking care of the logistics associated with bringing this article to fruition. All authors designed the study, analyzed the data, and wrote the entire manuscript. The views expressed in this research paper are the independent views of the authors and should not be understood or quoted as being made on behalf of or reflecting of the position of their company or any other affiliation. Author contributions are as follows: Thomas C. Kühler: conceptualization, supervision, writing - review & editing, funding acquisition; Marc Schoenmakers: conceptualization, writing - review & editing, supervision, project administration; Oliver Shergold: writing - original draft, writing - review & editing, supervision; Stephan Affolter: writing - original draft, writing - review & editing; Winona Rei Bolislis: writing - review & editing; Ruth Foster: writing - original draft; Paul Gardner: writing - original draft; Svenja Hruschka: writing - original draft; Thierry Jomini: writing - original draft; Sathish Kaveripakam: writing - original draft; Karl Mayerhofer: writing - original draft; Tomaso Scherini: writing - original draft; Marta Swierczynska: writing - review & editing; Gretchen Vandal: writing - original draft; Shayesteh

Fürst-Ladani: conceptualization, writing - original draft, writing - review & editing, supervision.

REFERENCES

1. BETASERON (n.d.). *The BETACONNECT™ Autoinjector.* https://www.betaseron.com/betaconnectsystem/betaconnecttm-electronic-autoinjector. Accessed on 4 February 2022.
2. Enbrel Etanercept (n.d.). *The Enbrel Mini® single-dose prefilled cartridge with AutoTouch® reusable autoinjector.* https://www.enbrel.com/resources/enbrel-mini-cartridge-with-autotouch-autoinjector. Accessed 4 February 2022.
3. Omnipod (n.d.). *The Omnipod DASH® System*. https://www.omnipod.com/en-fi. Accessed on 4 February 2022.
4. US FDA. (2020). *Frequently Asked Questions About Combination Products*. https://www.fda.gov/combination-products/about-combination-products/frequently-asked-questionsabout-combination-products#CP. Accessed on 8 February 2022.
5. EMA. (2021). *Medical devices*. https://www.ema.europa.eu/en/human-regulatory/overview/medicaldevices#medicinal-products-used-in-combination-with-a-medical-device-section. Accessed on 8 February 2022.
6. Medtech & Pharma Platform Association (n.d.). *Objectives*. https://www.medtech-pharma.com/. Accessed on 1 February 2022.
7. Pelayo S, Marcilly R, Bellandi T. Human factors engineering for medical devices: European regulation and current issues. *International Journal for Quality in Health Care*. 2021;33(Supplement_1):31–36. https://academic.oup.com/intqhc/article/33/Supplement_1/31/5912963. Accessed on 7 February 2022.
8. US FDA. (2016). *Guidance document on Applying Human Factors and Usability Engineering to Medical Devices*. https://www.fda.gov/regulatory-information/search-fda-guidancedocuments/applying-human-factors-and-usability-engineering-medical-devices. Accessed on 4 February 2022.
9. Regulation (EU) 2017/745. *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 and 93/42/EEC*. http://data.europa.eu/eli/reg/2017/745/oj.
10. Medical Device Regulation (n.d.). *ANNEX I – General safety and performance requirements*. https://www.medical-device-regulation.eu/2019/07/23/annex-i-general-safety-and-performancerequirements/. Accessed 1 February 2022.
11. European Commission (n.d.). *CE marking*. https://ec.europa.eu/growth/single-market/ce-marking_en. Accessed 1 February 2022.
12. Regulation (EU) 2017/746. *On in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU*. http://data.europa.eu/eli/reg/2017/746/oj.
13. Stanford University (n.d.). *Get Started with Design Thinking*. https://empathizeit.com/design-thinking-models-stanford-d-school/. Accessed on 2 February 2022.
14. ISO. (2019). *ISO 14971:2019 Medical devices — Application of risk management to medical devices*. https://www.iso.org/standard/72704.html. Accessed on 2 February 2022.
15. EMA. (2021). *Guideline on quality documentation for medicinal products when used with a medical device.* https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-quality-documentationmedicinal-products-when-used-medical-device-first-version_en.pdf. Accessed on 2 February 2022.
16. ISO. (2015). *IEC 62366-1:2015 Medical devices — Part 1: Application of usability engineering to medical devices*. https://www.iso.org/standard/63179.html. Accessed on 2 February 2022.
17. ISO. (2016). *IEC/TR 62366-2:2016 Medical devices — Part 2: Guidance on the application of usability engineering to medical devices*. https://www.iso.org/fr/standard/69126.html. Accessed on 2 February 2022.
18. ISO. (2016). *ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes*. https://www.iso.org/standard/59752.html. Accessed on 2 February 2022.
19. Royce WWinston. Managing the development of large software systems. *Proceedings. IEEE Wescon*; 1970:1–9.
20. Agile Alliance (n.d.). *What is Agile?* https://www.agilealliance.org/agile101/. Accessed on 2 March 2022. Abrahamsson, P. and al. *Agile Software Development Methods: Review and Analysis*. VTT Publications 478. 2002. Dingsøyr, T. and al. *A decade of agile methodologies: Towards explaining agile software development*. Journal of Systems and Software. Vol. 86, issue 6. Pp. 1213-1221. 2012
21. International Council on Systems Engineering (n.d.). https://www.incose.org. Accessed on 2 February 2022.
22. ISO. (2006). *IEC 62304:2006 Medical device software — Software life cycle processes*. https://www.iso.org/standard/38421.html. Accessed on 2 February 2022.

23. Macomber, L. Schroeder, A. (n.d.). *General Safety and Performance Requirements (Annex I) in the New Medical Device Regulation*. BSI Group. https://www.bsigroup.com/LocalFiles/es-MX/dispositivosmedicos/General_Safety_and_Performance.pdf. Accessed on 2 February 2022.
24. Regulation (EU) 2016/679. *On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. http://data.europa.eu/eli/reg/2016/679/oj.
25. IMDRF. (2020). *Principles and Practices for Medical Device Cybersecurity*. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-200318-pp-mdc-n60.pdf. Accessed on 2 February 2022.
26. ISO. (2019). *ISO 14971:2019 Medical devices — Application of risk management to medical devices*. https://www.iso.org/standard/72704.html. Accessed on 2 February 2022.
27. MDCGMDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices. *European Commission*. 2020. https://ec.europa.eu/health/sites/default/files/md_sector/docs/md_cybersecurity_en.pdf. Accessed on 2 February 2022.
28. Shostack A. Security Briefs: Reinvigorate your Threat Modeling Process. *MSDN Magazine*. 2008. https://docs.microsoft.com/en-us/archive/msdn-magazine/2008/july/security-briefs-reinvigorate-yourthreat-modeling-process. Accessed on 2 February 2022.
29. DEVSECOPS (n.d.). *Manifesto*. https://www.devsecops.org/. Accessed on 2 February 2022.
30. Henderson S. New science: Biopharma's new growth engine. *Accenture*. 2019. https://www.accenture.com/us-en/insights/life-sciences/new-science. Accessed on 2 February 2022.
31. Accenture (n.d.). *NEW SCIENCE - Biopharma's New Growth Machine*. https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/Secure/pdf-no-index-2/Accenture-Life-Sciences-New-Science.pdf#zoom=50. Accessed on 4 February 2022.
32. ISPE. (2008). *GAMP 5 Guide: Compliant GxP Computerized Systems*. https://ispe.org/publications/guidance-documents/gamp-5. Accessed on 2 February 2022.
33. Regulation (EU) 2017/745. Annex I. *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 and 93/42/EEC*. http://data.europa.eu/eli/reg/2017/745/oj.

Address correspondence to: Shayesteh Fürst-Ladani, MS, SFL Regulatory Affairs & Scientific Communication, Medtech & Pharma Platform, Aeschenvorstadt 52, Basel 4051, Switzerland. E-mail: association@medtech-pharma.com.