swiss medical weekly

Review article: Biomedical intelligence | Published 25 October 2024 | doi:https://doi.org/10.57187/s.3954
Cite this as: Swiss Med Wkly. 2024;154:3954

Chatbots in medicine: certification process and applied use case

Mayssam Nehme[a], Franck Schneider[b], Esther Amruthalingam[c], Elio Schnarrenberger[d], Raphaël Trëmeaud[e], Idris Guessous[ac]

[a] Division of Primary Care Medicine, Geneva University Hospitals
[b] Direction of Communication, Geneva University Hospitals
[d] Säfeli Sàrl
[e] Promotion Santé Suisse
[c] Faculty of Medicine, University of Geneva

Summary

Chatbots are computer programs designed to engage in natural language conversations in an easy and understandable way. Their use has been accelerated recently with the advent of large language models. However, their application in medicine and healthcare has been limited due to concerns over data privacy, the risk of providing medical diagnoses, and ensuring regulatory and legal compliance. Medicine and healthcare could benefit from chatbots if their scope is carefully defined and if they are used appropriately and monitored long-term.

The conflAnce chatbot, developed at the Geneva University Hospitals and the University of Geneva, is an informational tool aimed at providing simplified information to the general public about primary care and chronic diseases. In this paper, we describe the certification and regulatory aspects applicable to chatbots in healthcare, particularly in primary care medicine. We use the conflAnce chatbot as a case study to explore the definition and classification of a medical device and its application to chatbots, considering the applicable Swiss regulations and the European Union AI Act.

Chatbots can be classified anywhere from non-medical devices (informational tools that do not handle patient data or provide recommendations for treatment or diagnosis) to Class III medical devices (high-risk tools capable of predicting potentially fatal events and enabling a pre-emptive medical intervention). Key considerations in the definition and certification process include defining the chatbot's scope, ensuring compliance with regulations, maintaining security and safety, and continuously evaluating performance, risks, and utility. A lexicon of relevant terms related to artificial intelligence in healthcare, medical devices, and regulatory frameworks is also presented in this paper.

Chatbots hold potential for both patients and healthcare professionals, provided that their scope of practice is clearly defined and that they comply with regulatory requirements. This review aims to provide transparency by outlining the steps required for certification and regulatory compliance, making it valuable for healthcare professionals, scientists, developers, and patients.

Mayssam Nehme
Division of Primary Care Medicine
Geneva University Hospitals
Rue Gabrielle-Perret-Gentil 4
CH-1205 Genève
Mayssam.Nehme[at]hcuge.ch

Introduction

The use of chatbots has been accelerated in recent years, particularly since the public deployment of ChatGPT [1]. Chatbots hold significant potential across multiple fields, including in medicine and healthcare, as these domains depend heavily on service delivery and information exchange. In recent years, electronic patient messages have increased by 1.6 times, resulting in additional time spent using electronic health records and increased after-hours work for healthcare professionals [2, 3]. This surge raises the risk of physician burnout [3, 4]. Moreover, unanswered messages may lead to a decline in the physician-patient relationship. Chatbots could serve as a complementary resource, reinforcing this relationship by addressing some patient inquiries without attempting to diagnose or replace the physician's role. If chatbots can reduce even part of the messaging burden, they could potentially improve time management, liberating some of physicians' time, and allowing more meaningful interactions between physicians and patients. In turn, this could facilitate patient acquisition of verified knowledge and foster greater empowerment in healthcare. It is essential that physicians, caregivers, and patients understand the core principles underpinning these systems to make their operations more transparent, accessible, and easier to grasp.

Large language models (LLMs) encode vast amounts of text in a way that captures how words and phrases relate to each other, allowing them to predict which words are likely to follow. Driven by advanced algorithms, they have become more powerful than earlier tools and are scalable for use in specific fields. The rapid advancements in artificial intelligence (AI) have attracted significant attention. New technologies using LLMs hold considerable promise for the efficient use of chatbots in healthcare, including summarising clinical documentation or research papers, answering patient-specific questions, and assisting with appointments and workflow management in medical practices or hospitals.

Some studies have evaluated the role of chatbots in managing and supporting patients in primary care medicine. Chatbots can play a crucial role in chronic disease management, providing support [5] and assisting patients with spe-

cific tasks such as self-monitoring and self-management [6, 7]. The overall acceptance of chatbots in primary care and chronic conditions appears promising, particularly in areas such as cancer [8], hypertension [9], heart conditions [10, 11], pulmonary conditions [10], mental health [12], and adherence to therapy [13, 14]. User experience is one of the most frequently cited metrics in studies, which reflects user satisfaction with perceived usefulness, ease of use, and improved quality of life in managing their condition [15]. Studies have reported that patients with chronic diseases may feel more comfortable using chatbots compared to continuous in-hospital follow-ups [7]. For example, chatbots providing assistance and follow-up to adults receiving cancer treatment have been shown to reduce anxiety levels, limiting the need to contact healthcare professionals [16]. However, concerns about confidentiality and content quality arise with the use of these technologies [17].

However, there are also risks and challenges, along with concerns in the medical and scientific communities about how to best utilise and regulate this rapidly advancing technology [18]. LLM chatbots, for instance, can provide inaccurate information and can "hallucinate", providing seemingly coherent but incorrect answers. This poses a significant risk in healthcare, especially when chatbots are used for diagnosis or treatment [19]. One way to mitigate these risks is by restricting chatbots to a specific knowledge base through retrieval-augmented generation (RAG). RAG is an AI technique that combines the capabilities of LLMs with the specificity and accuracy of a verified knowledge base. The RAG technique consists of limiting the chatbot and allowing it to answer only within the predefined scope set by the developer. Other risk mitigation strategies include ongoing supervision and surveillance of chatbots. In September 2022, the U. S. Food and Drug Administration (FDA) issued guidance stating that chatbots and AI-assisted devices should require approval as medical devices unless their outputs are fully monitored by humans, who can *"independently review the basis for the recommendations presented by the software*" [20]. Another approach is to carefully define the chatbot's scope. For instance, a chatbot designed to provide general information is very different from one used for diagnosis or for administrative purposes like scheduling appointments. The scope changes not only the definition of the chatbot, but also its use, monitoring, and regulation. Indeed, several important questions arise, such as whether the chatbot includes identifiable information, making it as sensitive as electronic health records, whether it functions as a clinical decision-making tool, requiring consideration of medical responsibility, or whether it qualifies as a medical device, thus subject to the same certification process as other medical devices used in patient care. As a general approach, industry standards and best practices that companies and industry groups can adopt are essential, along with adaptive regulation and guidance from regulatory bodies.

The European Medicines Agency (EMA), through the Medical Device Regulation (MDR) [21] and Medical Devices Ordinance (MedDO) [22] in Switzerland, and the United States Food and Drug Administration (FDA) [23], are two of the main regulatory bodies for medical devices worldwide. Both agencies share similarities in their classification systems, although the MDR is considered more stringent in its equivalency and surveillance processes [24]. Additionally, the EMA uses notified bodies (as of March 2024, there were 41 notified bodies designated under the MDR) [25], whereas the FDA centralises this task under a single government authority. Both systems use the same risk classes (I, II, III) ranging from lowest to highest risk, with the EU MDR further subdividing Class II into IIa and IIb. The certification process varies depending on the risk class. Therefore, when developing chatbots, it is important to determine whether they are classified as medical devices and, if so, which risk class they fall under.

Based on our previous experience developing chatbots for post-COVID care [26] (www.rafael-postcovid.ch) and for general contact and administrative information (https://www.hug.ch/en/contact) at the Geneva University Hospitals, our team developed an informational chatbot for primary care, addressing the challenges of certification and validation. The chatbot, confIAnce, was developed by the Division of Primary Care Medicine, the communication department, and several stakeholders at the Geneva University Hospitals and the University of Geneva. It aims to provide simplified information to the general public on primary care and chronic diseases. The chatbot is designed for informational purposes only, using a knowledge base owned and updated by the Division of Primary Care Medicine, which reflects the most common pathologies and chronic conditions encountered in general practice [27]. This knowledge base was initially created for healthcare professionals and was adapted into layperson terms to serve the general population. The chatbot uses retrieval-augmented generation (RAG), limiting its scope to the verified database.

This paper aims to demystify the development and certification process for healthcare chatbots, defining their boundaries and capabilities within the framework of the MDR. Using the confIAnce chatbot as a case study, this paper provides insights into the necessary steps and best practices. Herein, we review the definition of a medical device under the MDR, the classification of chatbots according to risk levels, the certification process, including quality management systems for both medical and non-medical chatbots, data protection considerations, and new considerations under the EU AI act.

Definition of a medical device

According to the MDR (Article 2 and Annex VIII) [21], a medical device is "*any instrument, apparatus, appliance, software, implant, reagent, material, or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more specific medical purposes"*. These purposes include *"diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease; diagnosis, monitoring, treatment, alleviation of, or compensation for an injury or disability; investigation, replacement, or modification of the anatomy or of a physiological or pathological process or state; providing information by means of in vitro examination of specimens derived from the human body*". Devices for controlling or supporting conception, as well as those specifically intended for cleaning, disinfecting, or sterilising other medical devices, are also included. Additionally, "*software*

intended to provide information which is used to take decisions with diagnosis or therapeutic purposes, or to monitor physiological processes are also considered a medical device".

For a chatbot to qualify as a medical device, its application must be explicitly medical, such as aiding in the diagnosis, prevention, treatment, or management of diseases and medical conditions. Scope is a determining factor: a chatbot designed solely to give general health and wellness advice may not fall under the MDR classification, whereas one designed to diagnose or monitor specific medical conditions, or offer personalised medical advice, would. Moreover, understanding the limitations of chatbots is essential. While they can process and analyse large data sets and interact with patients, their ability to provide accurate medical advice or diagnoses depends on the sophistication of their underlying algorithms and the quality of the data they use. These limitations must be clearly defined to ensure safe and effective use, avoiding over-reliance on these digital tools for critical medical decisions.

Application: The confIAnce chatbot, designed for primary care medicine and chronic diseases, does not diagnose or recommend treatment. Based on MDR regulations and the definition of a medical device, confIAnce was classified as a non-medical device. Several considerations were taken to ensure safety and scope of use: the chatbot's scope was restricted to a specific knowledge base, additional control layers were added to fall back to no response when outside the scope of practice, and users were explicitly informed that the chatbot is for informational purposes only. Safeguards were implemented to maintain a non-personalised approach, reminding users that they are interacting with a machine, and providing general information on chronic diseases without interpreting patient data.

Classification of chatbots as medical devices

If a chatbot is defined as a medical device based on its application, it must then be classified under the MDR into one of the risk classes (figure 1).

- Class I devices are low-risk, and their certification process typically involves self-certification. Self-certification is only applicable to Class I devices. This means the manufacturer applies the best standards and practices to the product without requiring external certification, though post-market surveillance and quality control are still necessary. Examples include a chatbot that reminds patients to take medications or schedules appointments without interpreting patient data or making clinical decisions.
- Class IIa devices are medium risk and require a conformity assessment, including a review of the quality management system and product testing by third-party laboratories. Examples include a chatbot integrated into a hypertension management program for patients with high blood pressure, providing lifestyle recommendations based on patient data, offering medication reminders, and sending alerts when readings fall outside safe ranges. The chatbot's role in guiding therapeutic decisions through the interpretation of patient data and supporting patient self-management qualifies it as a Class IIa medical device. Since hypertension is considered a low to medium-risk condition, the device remains classified as Class IIa.
- Class IIb devices present a higher medium risk and require rigorous third-party inspection and examination due to the increased risk of harm if the device fails or malfunctions. Examples include a chatbot integrated into a cardiac insufficiency program, designed to provide therapeutic recommendations based on patient data, with alerts to medical professionals if immediate intervention is needed. The chatbot's role in guiding therapeutic decisions through interpreting patient data in a high-risk condition, and the high-risk nature of cardiac management, qualifies this chatbot as a Class IIb medical device.
- Class III devices are high-risk and must undergo premarket approval, including detailed technical documentation and clinical data. These devices support therapeutic or diagnostic decisions that directly impact patient survival or could lead to death or irreversible health deterioration. Examples include a chatbot that analyses high-risk health indicators to predict acute events like sepsis or organ failure, potentially hours before they occur, allowing for pre-emptive medical interventions.

Chatbots may also be classified as in-vitro diagnostic medical devices (IVDs) if used for tests conducted on samples. Under the In-Vitro Diagnostic Medical Device Regulation (IVDR) [28], devices are classified into four categories (A, B, C, and D) based on risk, with Class A devices representing the lowest risk and Class D the highest. Similarly to medical devices, this classification imposes more stringent requirements as the risk increases.

Certification process

While the landscape of AI is rapidly evolving, some certification standards should be considered by developers and product owners in the development and dissemination of their tools. Once the initial development phase is completed and relevant standards are identified, the certification process begins with a clinical evaluation and the definition of the intended medical use, functionality, and market. These elements are integrated into the design, and a technical file or dossier is compiled. This technical file provides detailed documentation of the chatbot's development, demonstrating its compliance with required standards and regulations. The file is then submitted to a certified notified body designated by the European Union to assess the conformity of the product. The notified body grants certification once all requirements and standards are met, followed by required post-market surveillance under the MDR to ensure continued compliance. Finally, if the device is decommissioned, specific rules for ending its active use must also be followed. Each step of the certification process after the initial development phase is outlined below and in figure 2.

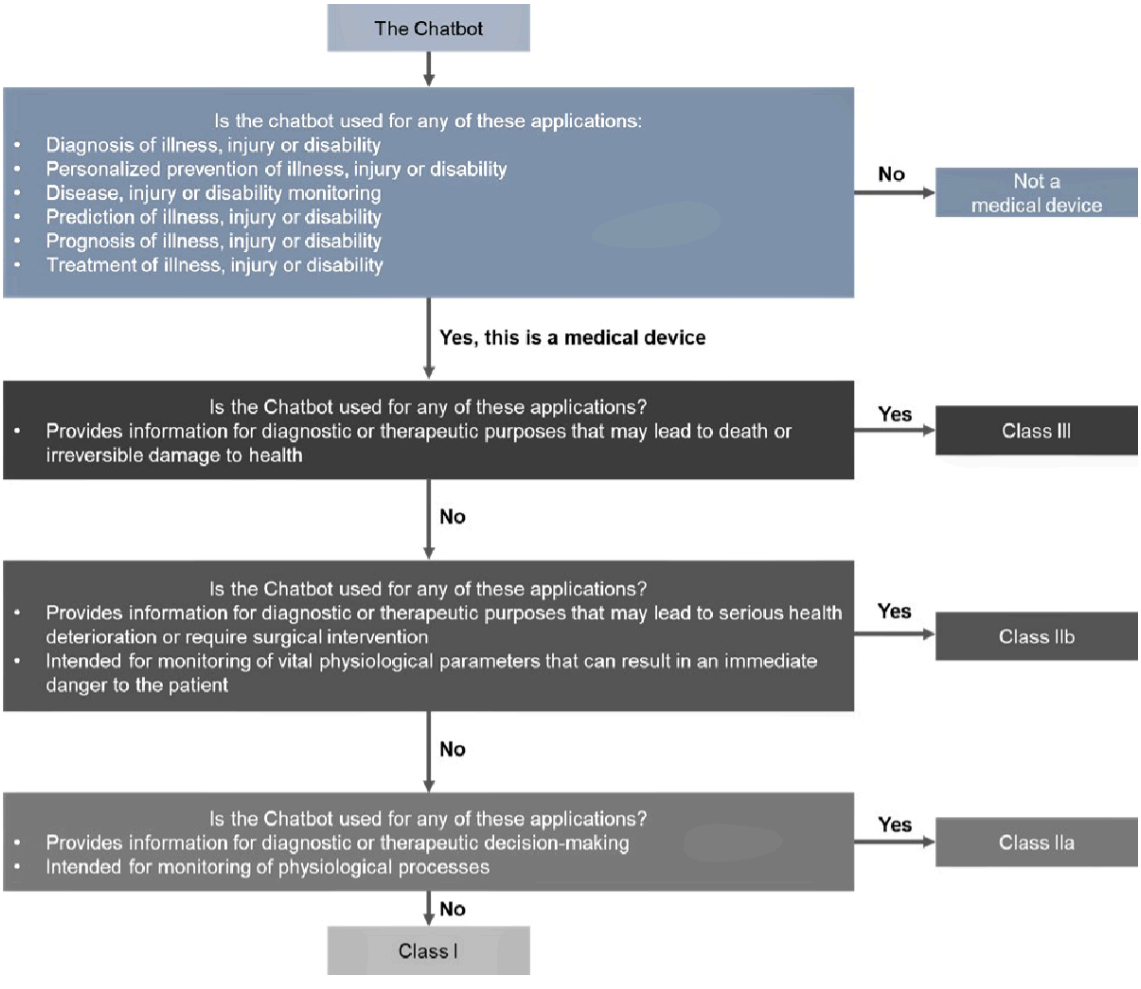
(1) Clinical evaluation should follow the specifications outlined in Article 61 and Annex XIV of the MDR [21]. Article 61 defines clinical evaluation, criteria for exemption, and demonstration of sufficient data access to justify claims of equivalence – an important factor if the manufacturer can show that the clinical data used is based on a device deemed equivalent. Clinical evaluation involves

validating the clinical association and scientific validity of Medical Device Software (MDSW). Valid clinical association ensures that the device's outcome aligns with the intended clinical purpose, while scientific validity ensures that this association is grounded in well-established scientific principles and evidence. Clinical trials or investigations may be required to assess the device's safety and efficacy, subject to approval by ethics committees. Annex XIV provides additional guidelines on evaluation methods, including reviewing scientific literature, assessing safety and performance, defining the intended purpose, target groups, and clinical benefits, and determining methods to assess safety and benefit-risk ratios. It also includes an analysis of relevant clinical data to draw conclusions about safety and clinical performance. Clinical data may come from a device for which equivalence can be demonstrated (e.g., similar design, conditions of use, specifications, principles of operation, and critical performance requirements). The complete document can be found at (https://www.medical-device-regulation.eu/2019/08/14/annex-xiv/). Although these guidelines were written before the emergence of AI technologies, they still apply to the certification process of any medical device.

(2) Integrating the clinical evaluation and specifications into the design and development of the device is an essential step to ensure conformity and its potential use after certification while meeting all required standards. During development, it is important to adhere to existing norms, such as IEC 62304 for medical device software, and other software development requirements, especially given the current lack of specific standards for AI devices. Verification and validation should be completed prior to deployment, along with appropriate user training to ensure the correct and safe use of the device.

(3) Technical files must be submitted to a certified notified body. A list of notified bodies can be found at: https://health.ec.europa.eu/medical-devices-topics-interest/notified-bodies_en. Notified bodies are responsible for a comprehensive evaluation process, which includes reviewing the technical documentation of medical devices, auditing manufacturers' quality management systems, and ensuring ongoing compliance with applicable standards. This assessment is especially critical for higher risk medical devices, where independent verification of safety and effectiveness is essential. In contrast, Class I devices, which pose the lowest risk, may be self-certified. Notified bodies also conduct audits and oversee post-market surveillance to ensure continued compliance after certification is issued.

Figure 1: Definition and classification of chatbots as medical devices. Further information on the definition and classification of medical devices, including software, can be found in MDR article 2, MDR Annex VIII [21], Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 (MDR) and Regulation (EU) 2017-746 (IVDR) [35], and the Medical Devices Legislation by the Federal Office of Public Health [22].



(4) Certification: Once a medical device successfully passes this evaluation, the notified body issues a certificate of conformity. This certificate is crucial, as it allows the manufacturer to affix the CE marking, indicating that the device meets EU standards and can be marketed. After receiving the certificate, the device must be registered with the appropriate authorities (i.e., Swissmedic) before being introduced to the market.

(5) PMS is a systematic and essential process, ensuring the continued safety and effectiveness of medical devices after release to market. PMS involves real-world performance monitoring and mandatory incident reporting. This includes monitoring the software's use in various clinical settings, gathering performance data, and collecting user feedback. This step is crucial for quickly identifying and addressing potential issues to ensure the software remains compliant with regulatory standards.

– Real-world data utilisation: Analysis of real-world data helps refine the software and provides crucial insights into its performance in diverse real-life scenarios, which can lead to improvements and adaptations in functionality.
– Mandatory reporting of incidents: Reporting timeframes are determined based on the incident's severity. Any serious incidents and corrective actions taken to ensure safety must be promptly reported to the relevant authorities.

The MDR, particularly in Article 83, mandates that manufacturers establish a comprehensive PMS system as part of their quality management system. Manufacturers are required to actively and systematically collect, record, and analyse data on their device's quality, performance, and safety throughout its life cycle. For class I devices, manufacturers must compile a PMS report summarising the results and conclusions from the data, along with any preventive or corrective actions taken. This report must be updated as needed and made available to competent authorities upon request. For class IIa, IIb, and III devices, manufacturers are required to prepare a Periodic Safety Update Report (PSUR). The PSUR provides comprehensive summaries of PMS data, findings from post-market clinical follow-ups, sales volume, and estimates of the user population. For class IIb and III devices, the PSURs are reviewed annually by the notified body and made available to the competent authorities.

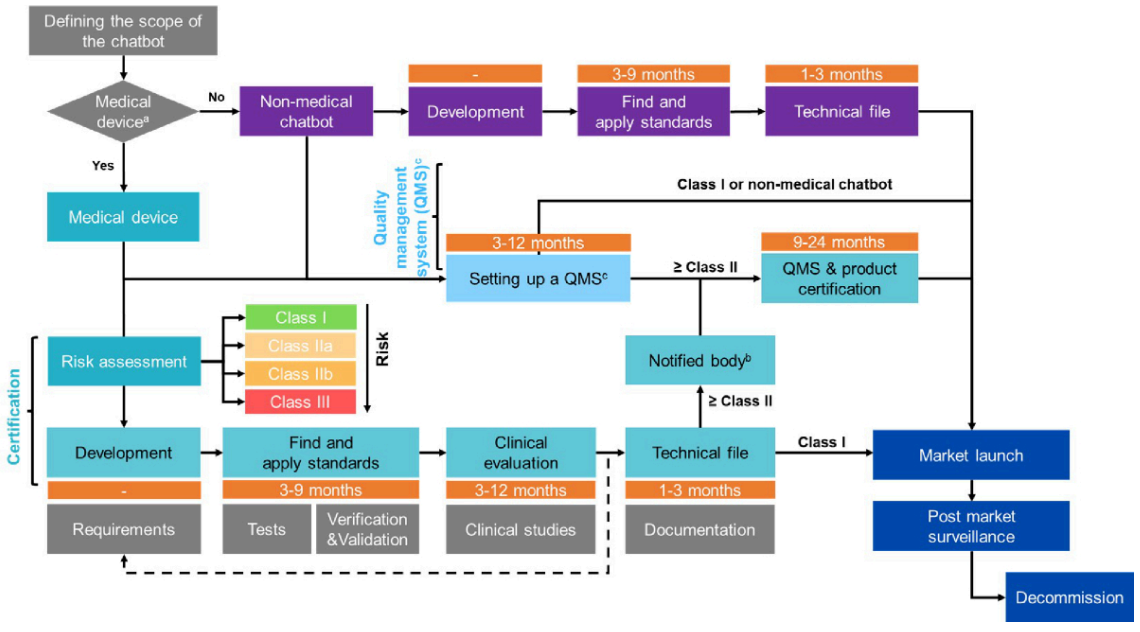
(6) The final phase in the device's lifecycle involves decommissioning. This process must ensure data integrity, compliance with regulatory standards, and proper communication with stakeholders.

Quality management system

A quality management system (QMS) is an essential framework that ensures a product consistently meets required quality and safety standards. Core elements of a QMS include the organisation's guiding principles, processes to ensure consistency and quality – especially for critical operations – and step-by-step procedures for carrying out specific tasks, providing clear guidance for employees.

If a chatbot is not classified as a medical device, quality management standards still apply. Relevant certifications may include ISO 4213 (assessment of machine learning classification performance), ISO 24027 (bias in AI systems and AI-aided decision making), ISO 24029 (robustness as-

Figure 2: Certification process, quality management system, and post-market surveillance for medical and non-medical chatbots. a: A medical device, as defined by the Medical Device Regulation (MDR), is an article, instrument, apparatus, or machine that is used in the prevention, diagnosis, or treatment of illness or disease, or for detecting, measuring, restoring, correcting, or modifying the structure or function of the body for a health-related purpose. b: A notified body is an organisation designated to assess the conformity of certain products before they are placed on the market. c: The quality management system (QMS) process can take longer for medical devices compared to non-medical devices. Setting up a QMS can take between 3 to 12 months, while QMS certification may take an additional 1 to 3 months. Based on the MDR, the conflAnce chatbot is considered a non-medical chatbot. However, steps such as implementing a QMS and adhering to necessary standards for product certification and data protection remain applicable.



sessment of neural networks), ISO 5469 (functional safety of AI systems), ISO 27563 (security and privacy in AI use cases), and ISO 8200 (controllability of automated AI systems). Additionally, processes should comply with standards such as ISO 5338 (AI system lifecycle processes), ISO 8183 (data lifecycle framework), and ISO 23053 (framework for AI systems using machine learning). The governing organisation should adhere to certifications like ISO 42001 (AI management system), ISO 23894 (AI guidance on risk management), ISO 5259-5 (data quality governance framework), and ISO DIS 5259-3 (data quality management requirements and guidelines).

For chatbots classified as medical devices, adherence to ISO 13485 is essential. This international standard outlines QMS requirements, including defining roles and responsibilities, ensuring quality control throughout design and development, planning validation and verification, risk management, and regulatory compliance. It also covers supply chain management, product realisation, and customer focus. ISO 13485 mandates regular monitoring and measurement of processes and devices. Additional relevant standards for medical software, which could apply to medical chatbots, include IEC 82304 (safety and security of health software), IEC 62304 (lifecycle requirements for medical software), ISO 14971 (risk management for medical devices), IEC 62366-1 (usability of a medical device related to safety), ISO 20417 (identification and labelling of medical devices), ISO 14155 (clinical investigation of medical devices), and ISO TR 20416 (PMS).

Implementing a QMS requires organisation-wide involvement, ensuring a unified approach to quality across all departments, employee training, and engagement, as well as leveraging external QMS expertise. Templates and tools can assist in implementation. QMS certification includes an initial audit by a third-party organisation, an assessment of any non-conformities, and the granting of certification. Ongoing surveillance audits are also conducted to maintain certification.

Data protection

Chatbots considered non-medical devices remain subject to regulations and standards including data protection, cybersecurity, and quality management. Data privacy and security, while not in the scope of this paper, must always comply with national or regional rules, such as the General Data Protection Regulation (GDPR) in Europe [29]. Key GDPR principles include consent, transparency, data minimisation, the right to access and erase information, data portability, data protection officers, security measures, and breach notification within 72 hours of becoming aware of the breach [29]. Non-medical chatbots must also implement strong cybersecurity measures to prevent data breaches, unauthorised access, or other risks. Regular audits and stress tests should be conducted to ensure compliance with security standards. ISO/IEC 27001 certification [30] is applicable in this context, confirming that the chatbot has adequate cybersecurity safeguards. Regular updates should be applied to comply with the latest security standards to protect users, along with a clear incident response plan in case of a breach.

Application: The confIAnce chatbot was designed to be completely anonymous for security and privacy purposes, and it does not collect any personally identifiable information. To enhance both accessibility and anonymity, we chose to avoid sign-ins and downloadable applications. The chatbot is hosted on the Geneva University Hospitals' website, accessible to all without the need for sign-in or specific software. The confIAnce chatbot has been reviewed by internal security officers and complies with GDPR and the Swiss Federal Act on Data Protection, addressing data transparency, security, quality, individual rights, and potential penalties for non-compliance. Additionally, ISO/IEC 27001 certification is applicable, ensuring that potential information security risks are identified and managed.

Additional provisions under the EU AI act

The EU AI Act [31] builds on existing regulations such as the MDR and IVDR, classifying AI systems into three categories: (1) prohibited, (2) high-risk, and (3) low to minimal risk. Prohibited systems are those that cannot be marketed due to the potential for physical, psychological, or other forms of harm. High-risk systems, which include products requiring third-party conformity assessment (Classes IIa to III under the MDR), must undergo the full certification process. Low to minimal-risk systems are not required to undergo the same level of scrutiny but are encouraged to establish behavioural codes of conduct to promote adherence to legal requirements applicable to high-risk systems. High-risk AI systems must follow the certification process, including registration in the EU database. These systems also require specific features, such as appropriate human-machine interface tools, human oversight proportionate to the level of risk, and transparency in providing information when necessary.

Application: Under the MDR, the confIAnce chatbot was classified as an informational non-medical chatbot. This evaluation was based on the fact that confIAnce provides users with information about chronic diseases and is limited to a verified knowledge base. As the chatbot is not designed to offer diagnosis or treatment options, it operates as an easily accessible knowledge repository without delivering personalised information. Safeguards include disclaimers, reminders of the chatbot's primary use, anonymisation of all data, and fallback mechanisms for prompts outside its scope. These considerations align with the current EU AI Act. Additionally, confIAnce undergoes continuous monitoring with automated tests and a chatbot master who regularly evaluates the prompts and answers for accuracy and harmlessness. Part of the ongoing quality improvement process involves reviewing recurring user prompts not yet included in the knowledge base.

Conclusion

Chatbots are rapidly evolving and, when used within their defined scope, hold significant potential in healthcare. Specific safeguards, adapted regulations, and transparency are essential to mitigate the risks and concerns regarding potential harm or misuse. The certification process applicable to medical devices provides a foundational understanding and starting point; however, further provisions applying directly to AI systems are still needed. In the meantime, clearly defining the scope of practice, implementing risk-

Table 1:
Lexicon in the development of chatbots and certification process.

Artificial intelligence (AI)	The theory and development of computer systems capable of performing tasks that normally require human intelligence.
Machine learning	A branch of AI and computer science focused on using data and algorithms to enable AI systems to imitate humans learning, gradually improving accuracy [32].
Deep learning	A subset of machine learning that uses large multilayered (artificial) deep neural networks that compute with continuous (real number) representations, mimicking hierarchically organised neurons in the human brain. It is particularly effective at learning from unstructured data such as images, text, and audio [33].
Neural network	A computational model inspired by the structure and function of biological neurons [33].
Large language models (LLM)	A neural network trained on vast amounts of text to mimic human language. This type of foundation model processes large volumes of unstructured text and learns relationships between words tokens (portions of words) [33].
Generative AI	A form of machine learning where AI platforms generate new outputs in response to prompts, based on the data they were trained on [33].
Retrieval-augmented generation (RAG)	A technique that optimises the output of an LLM by referencing an external, authoritative knowledge base before generating a response.
Fine tuning	The process of adapting a pre-trained model for specific tasks or use cases [34].
Knowledge base	A centralised repository for information that can be integrated with AI technologies.
Prompt	Instruction or question provided to an AI system using natural language, rather than computer code.
Prompt engineering or prompt design	The process of carefully constructing prompts or inputs for AI models to enhance their performance on specific tasks [33].
Prompt injection	The process of overriding original instructions in a prompt with a special user input. This occurs when untrusted input is incorporated into the prompt. In a direct prompt injection, hackers control the user input and feed the malicious prompt directly to the LLM.
Bias	A phenomenon where AI systems produce results that are systematically unfair or inaccurate due to erroneous assumptions or influences during machine learning. Bias in AI can have negative impacts on individuals and society, such as discrimination, misinformation, or loss of trust [33].
Hallucination	A phenomenon in which an AI system produces outputs that are not based on reality or the given context [33].
Supervised learning	A type of machine learning that uses labelled datasets to train algorithms to classify data or predict outcomes. The datasets are pre-labelled by humans [33].
Unsupervised learning	A type of machine learning where algorithms learn patterns from unlabelled data, without human guidance or feedback [33].
AI-Assisted device	A device that leverages AI and machine learning algorithms to enhance or revolutionise its functionality.
Medical device	An article, instrument, apparatus or machine used in the prevention, diagnosis, or treatment of illness or disease, or for detecting, measuring, restoring, correcting, or modifying the structure or function of the body for a health-related purpose [28].
Medical device regulation	Regulation (EU) 2017/745 on the clinical investigation and sale of medical devices for human use in the EU, repealing Directives 93/42/EEC (medical devices) and 90/385/EEC (implantable medical devices), in effect since May 26th, 2021 [28].
Food and Drug Administration	A U.S. federal agency responsible for protecting public health by ensuring the safety, efficacy, and truthful labelling of food, cosmetics, and nutritional supplements [23].
European AI act	A European Union regulation establishing a common regulatory framework for artificial intelligence, proposed on 21 April 2021 and passed on 13 March 2024 [31].
General data protection regulation (GDPR)	A European Union regulation governing data privacy and information security, particularly Article 8 of the Charter of Fundamental Rights of the European Union [29] .
Notified bodies	Organisations designated by EU countries to assess the conformity of certain products before they are placed on the market [25].
Class I; IIa; IIb; III	Risk classification for medical devices, ranging from low risk (Class I) to high risk (Class III) [28].
Certification	The process that certifies a device's compliance with applicable regulations and standards, guaranteeing the device's safety and performance [28].
Post-market surveillance (PMS)	A systematic process that ensures the continued safety and effectiveness of medical devices after they have been released onto the market [28] .
Quality management system (QMS)	A framework that ensures a product consistently meets required quality and safety standards (ISO/IEC).

reduction tools and processes, and using chatbots for informational purposes based on a verified knowledge base represents an effective way to complement the relationship between healthcare professionals and patients, without making medical decisions or replacing physicians. The next steps would involve assessing the added value of integrating informational chatbots into general practice and identifying any challenges or limitations when deployed on a larger scale. In real-world scenarios, chatbots could become valuable tools for physicians, helping to free up time and improve the quality of care.

Financial disclosure
Funding: Fondation Privée des HUG.

Potential competing interests
All authors have completed and submitted the International Committee of Medical Journal Editors form for disclosure of potential conflicts of interest. No potential conflict of interest related to the content of this manuscript was disclosed.

References

1. Open AI. Introducing ChatGPT. 2022. https://openai.com/blog/chatgpt
2. Holmgren AJ, Downing NL, Tang M, Sharp C, Longhurst C, Huckman RS. Assessing the impact of the COVID-19 pandemic on clinician ambulatory electronic health record use [Erratum in: J Am Med Inform Assoc. 2022 Jan 10; PMID: 34888680; PMCID: PMC8689796]. J Am Med Inform Assoc. 2022 Jan;29(3):453–60. http://dx.doi.org/10.1093/jamia/ocab268.
3. Tai-Seale M, Dillon EC, Yang Y, Nordgren R, Steinberg RL, Nauenberg T, et al. Physicians' Well-Being Linked To In-Basket Messages Generated By Algorithms In Electronic Health Records. Health Aff (Millwood). 2019 Jul;38(7):1073–8. http://dx.doi.org/10.1377/hlthaff.2018.05509.
4. Sinsky CA, Shanafelt TD, Ripp JA. The Electronic Health Record Inbox: recommendations for Relief. J Gen Intern Med. 2022 Nov;37(15):4002–3. http://dx.doi.org/10.1007/s11606-022-07766-0.
5. Haque MD, Rubya S. An Overview of Chatbot-Based Mobile Mental Health Apps: Insights From App Description and User Reviews. JMIR Mhealth Uhealth. 2023 May;11:e44838. http://dx.doi.org/10.2196/44838.
6. Hauser-Ulrich S, Künzli H, Meier-Peterhans D, Kowatsch T. A Smartphone-Based Health Care Chatbot to Promote Self-Management of Chronic Pain (SELMA): Pilot Randomized Controlled Trial. JMIR Mhealth Uhealth. 2020 Apr;8(4):e15806. http://dx.doi.org/10.2196/15806.
7. Bin Sawad A, Narayan B, Alnefaie A, Maqbool A, Mckie I, Smith J, et al. A Systematic Review on Healthcare Artificial Intelligent Conversa-

tional Agents for Chronic Conditions. Sensors (Basel). 2022 Mar;22(7):2625. http://dx.doi.org/10.3390/s22072625.
8. Xu L, Sanders L, Li K, Chow JC. Chatbot for Health Care and Oncology Applications Using Artificial Intelligence and Machine Learning: systematic Review. JMIR Cancer. 2021 Nov;7(4):e27850. http://dx.doi.org/10.2196/27850.
9. Lee N et al. Developing a Chatbot–Clinician Model for Hypertension Management. NEJM Catal Innov Care Deliv 2022;3(11) DOI: http://dx.doi.org/10.1056/CAT.22.0228. VOL. 3 NO. 11.
10. Ter Stal S, Sloots J, Ramlal A, Op den Akker H, Lenferink A, Tabak M. An Embodied Conversational Agent in an eHealth Self-management Intervention for Chronic Obstructive Pulmonary Disease and Chronic Heart Failure: Exploratory Study in a Real-life Setting. JMIR Hum Factors. 2021 Nov;8(4):e24110. http://dx.doi.org/10.2196/24110.
11. Vaddadi G, et al. A Pilot Program Utilising a "Chatbot " to Support Patients in the First 30 Days Following an Admission to Hospital With Acute Decompensated Heart Failure. Heart Lung and Circulation. July 2023. VOLUME 32, SUPPLEMENT 3, S139.
12. Griffin AC, Xing Z, Khairat S, Wang Y, Bailey S, Arguello J, et al. Conversational Agents for Chronic Disease Self-Management: A Systematic Review. AMIA Annu Symp Proc. 2021 Jan;2020:504–13.
13. Blasco JM, Díaz-Díaz B, Igual-Camacho C, Pérez-Maletzki J, Hernández-Guilén D, Roig-Casasús S. Effectiveness of using a chatbot to promote adherence to home physiotherapy after total knee replacement, rationale and design of a randomized clinical trial. BMC Musculoskelet Disord. 2023 Jun;24(1):491. http://dx.doi.org/10.1186/s12891-023-06607-3.
14. Schachner T, Keller R, V Wangenheim F. Artificial Intelligence-Based Conversational Agents for Chronic Conditions: Systematic Literature Review. J Med Internet Res. 2020 Sep;22(9):e20701. http://dx.doi.org/10.2196/20701.
15. Kurniawan MH, Handiyani H, Nuraini T, Hariyati RT, Sutrisno S. A systematic review of artificial intelligence-powered (AI-powered) chatbot intervention for managing chronic illness. Ann Med. 2024 Dec;56(1):2302980. http://dx.doi.org/10.1080/07853890.2024.2302980.
16. Greer S, Ramo D, Chang YJ, Fu M, Moskowitz J, Haritatos J. Use of the Chatbot "Vivibot" to Deliver Positive Psychology Skills and Promote Well-Being Among Young People After Cancer Treatment: Randomized Controlled Feasibility Trial. JMIR Mhealth Uhealth. 2019 Oct;7(10):e15018. http://dx.doi.org/10.2196/15018.
17. Thirunavukarasu AJ, Ting DS, Elangovan K, Gutierrez L, Tan TF, Ting DS. Large language models in medicine. Nat Med. 2023 Aug;29(8):1930–40. http://dx.doi.org/10.1038/s41591-023-02448-8.
18. Meskó B, Topol EJ. The imperative for regulatory oversight of large language models (or generative AI) in healthcare. NPJ Digit Med. 2023 Jul;6(1):120. http://dx.doi.org/10.1038/s41746-023-00873-0.
19. Webster P. Medical AI chatbots: are they safe to talk to patients? Nat Med. 2023 Nov;29(11):2677–9. http://dx.doi.org/10.1038/s41591-023-02535-w.
20. United States Food and Drug Administration. Clinical Decision Support Software. Guidance for Industry and Food and Drug Administration Staff. September 2022. https://www.fda.gov/media/109618/download
21. Regulation (EU) 2017/745 of the European parliament and of the council https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745
22. Swiss Confederation - Federal Office of Public Health - Medical Devices Legislation https://www.bag.admin.ch/bag/en/home/medizin-und-forschung/heilmittel/revision-med-prod-verord-mepv.html#:~:text=The%20EU%20Medical%20Devices%20Regulation,with%20developments%20in%20European%20law
23. Food and Drug Administration Regulations https://www.fda.gov/regulatory-information/fda-rules-and-regulations
24. Fink M, Akra B. Comparison of the international regulations for medical devices-USA versus Europe. Injury. 2023 Oct;54 Suppl 5:110908. http://dx.doi.org/10.1016/j.injury.2023.110908.
25. European Commission. Notified Bodies https://health.ec.europa.eu/medical-devices-topics-interest/notified-bodies_en
26. Nehme M, Schneider F, Perrin A, Sum Yu W, Schmitt S, Violot G, et al. The Development of a Chatbot Technology to Disseminate Post-COVID-19 Information: Descriptive Implementation Study. J Med Internet Res. 2023 Jun;25:e43113. http://dx.doi.org/10.2196/43113.
27. Division of Primary Care Medicine, Geneva University Hospitals. Strategies for Primary Care. https://www.hug.ch/medecine-premier-recours/strategies-medecine-premier-recours
28. European Union. Regulation (EU) 2017/746 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.
29. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj
30. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems Requirements. https://www.iso.org/standard/27001
31. European Parliament. Artificial Intelligence. https://www.europarl.europa.eu/topics/en/topic/artificial-intelligence
32. International Business Machines Corporation. IBM. What is Machine Learning (ML)? https://www.ibm.com/topics/machine-learning#:~:text=Machine%20learning%20(ML)%20is%20a,learn%2C%20gradually%20improving%20its%20accuracy. [Last accessed July 19, 2024].
33. International Monetary Fund. AI Lexicon. December 2023. Finance and Development Magazine. https://www.imf.org/en/Publications/fandd/issues/2023/12/AI-Lexicon [last accessed July 19, 2024].
34. International Business Machines Corporation. IBM. What is fine tuning? https://www.ibm.com/topics/fine-tuning#:~:text=Fine%2Dtuning%20in%20machine%20learning,models%20used%20for%20generative%20AI. [Last accessed July 19, 2024].
35. Medical Device Coordination Group Document. MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR. October 2019.