

Experiences Developing an AI Chatbot in the Pharmaceutical Industry

Samuel Abedu
samuel.abedu@mail.concordia.ca
Concordia University
Montreal, QC, Canada

Adam Yuen
adam.yuen@ucalgary.ca
University of Calgary
Calgary, AB, Canada

Ahmad Abdellatif
ahmad.abdellatif@ucalgary.ca
University of Calgary
Calgary, AB, Canada

Saviour Owolabi
saviour.owolabi@ucalgary.ca
University of Calgary
Calgary, AB, Canada

Cedric Lim Ah Tock
cedric.limahtock@mail.concordia.ca
Concordia University
Montreal, QC, Canada

Emad Shihab
emad.shihab@concordia.ca
Concordia University
Montreal, QC, Canada

Mayra Sofia Ruiz Rodriguez
mayrasofia.ruizrodriguez@mail.concordia.ca
Concordia University
Montreal, QC, Canada

Ali Zaraket
ali.zaraket@sandoz.com
Sandoz
Montreal, QC, Canada

Nahal Nasseri
nahal.nasseri@sandoz.com
Sandoz
Montreal, QC, Canada

Abstract

Chatbots have become prevalent in industries such as health and pharmaceutical. They make access to streamlined information easier and faster. With recent advances in large language models (LLMs), chatbots powered by LLMs offer new opportunities to improve access to information, including information about drugs. However, developing chatbots in pharmaceutical practice remains challenging due to safety and regulatory compliance requirements and the unique nature of the data in this domain. In this paper, we share our experience deploying an LLM-based chatbot to answer drug-related questions. We highlight the challenges we encountered developing the chatbot for a global pharmaceutical company. Among these challenges are ensuring that our chatbot retrieves reliable, up-to-date information from trusted sources and that its responses are trustworthy. We also share the strategies we adopt to overcome these challenges and the lessons we learn from deploying the chatbot. We believe these insights can guide the BoatSE and the broader software engineering community when deploying chatbots for highly regulated domains like pharmaceuticals.

CCS Concepts

• Applied computing → Computers in other domains; • Software and its engineering → Software design engineering.

Keywords

Chatbot, Artificial Intelligence, Industry, Pharmaceutical, LLM

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

BoatSE '26, Rio De Janeiro, Brazil

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 978-1-4503-XXXX-X/2018/06

<https://doi.org/XXXXXXX.XXXXXXX>

ACM Reference Format:

Samuel Abedu, Saviour Owolabi, Mayra Sofia Ruiz Rodriguez, Adam Yuen, Cedric Lim Ah Tock, Ali Zaraket, Ahmad Abdellatif, Emad Shihab, and Nahal Nasseri. 2025. Experiences Developing an AI Chatbot in the Pharmaceutical Industry. In *Proceedings of the 7th International Workshop on Bots and Agents in Software Engineering (BoatSE '26)*. ACM, New York, NY, USA, 7 pages. <https://doi.org/XXXXXXX.XXXXXXX>

1 Introduction

Chatbots are increasingly becoming important tools for organizations, offering conversational interfaces that automate information retrieval and other routine interactions [1]. The recent advances in LLMs have equipped chatbots with cutting-edge capabilities, which have contributed to the rise in adoption of chatbots in various domains such as customer support [21], financial assistants [7, 23], programming assistants [22], and in e-commerce [17]. The pharmaceutical and medical domains have also seen growth in the interest of chatbots. For instance, Google's Med-PaLM 2 was trained to answer medical questions, and it demonstrated superior performance over other models on healthcare QA benchmarks [24]. Steybe et al. [25] also introduced GuideGPT, a context aware chatbot for answering clinical questions on osteonecrosis medications.

These capabilities prove attractive to a global pharmaceutical company that receives a high volume of inquiries about dosage, contraindications, or storage of their products from health professionals (e.g., doctors and pharmacists), patients and the general public. Responding to such inquiries traditionally demands significant human effort, as relevant information is often dispersed across multiple sources. In this context, a chatbot can help automate responses, improving efficiency, reducing response times, and enhancing customer satisfaction.

However, developing a chatbot in the pharmaceutical domain presents unique challenges. The pharmaceutical domain is highly regulated, and information disseminated by pharmaceutical companies (and, by extension, their chatbots) must comply with stringent regulatory standards. These regulations exist for good reason, as

117 inaccurate information about drugs can have serious consequences
 118 for patient health and safety.

119 As part of our ongoing collaboration with the global pharmaceutical
 120 company to transform drug-related inquiries with artificial
 121 intelligence (AI), we developed a drug information chatbot. The
 122 chatbot combines data from a pharmaceutical company's internal
 123 databases and reputable external sources, utilizing AI to analyze
 124 and synthesize this information to deliver accurate, relevant, and
 125 compliant responses in a reduced turnaround time. Our chatbot
 126 answers questions related to drug information, such as “*Can I take*
127 drug A while taking drug B?” or “*How should I store drug X?*”. To
 128 ensure the integrity of the information provided by our chatbot,
 129 we implement several safeguards, including strict external source
 130 selection and a confidence scoring mechanism that provides trans-
 131 parency to users.

132 In this paper, we share our experience developing an LLM-based
 133 chatbot for a global pharmaceutical company. We believe this will
 134 provide valuable insights to both researchers and practitioners in
 135 the SE community when developing chatbots for highly regulated
 136 domains.

137 **Paper Organization.** The remainder of this paper is organized
 138 as follows. Section 2 presents the background, and Section 3 re-
 139 views related work. Section 4 describes the high-level architecture
 140 of our chatbot, while Section 5 discusses the technical and domain-
 141 specific challenges encountered during development and the strate-
 142 gies adopted to address them. In section 6, we share the lessons
 143 learned, and Section 7 concludes the paper.

144 2 Background

145 The pharmaceutical industry is highly regulated across the world.
 146 [12]. In the Canadian context, the regulatory authority, Health
 147 Canada (hereafter referred to as the regulator), maintains strict
 148 rules governing the communication of information about drug
 149 products. These requirements extend, by implication, to any chatbot
 150 endorsed by a pharmaceutical company, as it serves as a channel
 151 of communication with users. [4].

152 One key requirement is that communication about drug products
 153 be consistent with information in the product monograph [4]. The
 154 product monograph is an authoritative, publicly available docu-
 155 ment that provides comprehensive and factual information about
 156 a specific drug product. It is a mandatory component of market
 157 authorization and follows a standardized structure consisting of
 158 three parts:

- 159 (1) *Health Professional Information*, covering indications, con-
 traindications, warnings and precautions, adverse reactions,
 drug interactions, dosage and administration instructions,
 pharmacological properties, and other clinical and safety
 data;
- 160 (2) *Scientific Information*, detailing clinical pharmacology, tox-
 cology studies, product composition, and stability; and
- 161 (3) *Patient Medication Information*, providing information on
 the product's uses, correct administration, potential side
 effects, and when to seek medical attention.

162 The product monographs are lengthy documents with the *Health*
 163 and *Professional Information* and *Scientific Information* sections writ-
 164 ten in technical language intended for healthcare professionals and

165 may include tables, figures, and specialized terminology to sum-
 166 marize clinical and pharmacological data. By contrast, the *Patient*
167 Medication Information section is written in plain language, target-
 168 ing a Grade 6–8 reading level to ensure accessibility for patients
 169 and caregivers.

170 In addition to these product monographs, the pharmaceutical
 171 company maintains non-public reference materials, such as Fre-
 172 quently Asked Questions (FAQs) and marketing documents, which
 173 contain supplementary information used by correspondents to pro-
 174 vide accurate and consistent responses to inquiries from healthcare
 175 professionals or patients. Together, these materials form the knowl-
 176 edge base for a drug product, and all communication regarding that
 177 product (whether by humans or chatbots) must remain consistent
 178 with the information they contain.

179 LLMs are the state of the art in conversational AI, including
 180 chatbot applications. However, despite their remarkable general
 181 knowledge and strong performance on benchmarks such as MMLU
 182 and MedQA [19, 24], they cannot independently satisfy these re-
 183 quirements. While they demonstrate a broad understanding of
 184 generic molecules and popular product offerings, they lack reliable
 185 awareness of specific product-level details, such as brand names,
 186 packaging forms, or dosage forms [14].

187 A separate, but equally important requirement of the regulator
 188 is that serious adverse events associated with the use of a drug
 189 are reported within a defined time frame, as part of its pharma-
 190 covigilance framework[13]. While not required, the regulator also
 191 encourages the reporting of all adverse events associated with the
 192 use of a drug product. Among other required data points, such
 193 reports must include the drug product suspected and the adverse
 194 reaction described. These requirements mean that beyond question-
 195 answering the chatbot must incorporate a system for detecting
 196 and taking appropriate action in cases where a user expresses an
 197 adverse event in the course of their interaction with the chatbot.
 198 Given the potentially large volume of user interactions, manually
 199 reviewing conversations for adverse event detection would be im-
 200 practical, thus motivating the development of automated systems
 201 for detecting adverse events and drug names.

212 3 Related Works

213 Within the pharmaceutical domain, AI systems have long been
 214 explored for medication management, dosage optimization, and
 215 adverse event detection [5]. More recent studies have evaluated gen-
 216 erative models specifically: Al-Dujaili et al. [2] assessed ChatGPT's
 217 accuracy in pharmacotherapy decision-making, finding moderate
 218 reliability across repeated sessions. Beavers et al. [3] compared
 219 chatbot responses to those from clinical pharmacists, concluding
 220 that while LLMs can produce clinically acceptable information, they
 221 fall short in completeness and safety. Han [11] and Li et al. [16]
 222 further identified risks of misinformation in specialized contexts
 223 such as prescription review. More positively, de Jesus et al. [8]
 224 demonstrated that retrieval-augmented generation (RAG) using
 225 official patient information leaflets can improve factual correctness
 226 and clarity in medication instructions.

227 Outside the pharmaceutical context, several case studies have
 228 reported successful deployment of retrieval-augmented chatbots
 229 for specialized industrial domains, including software engineering

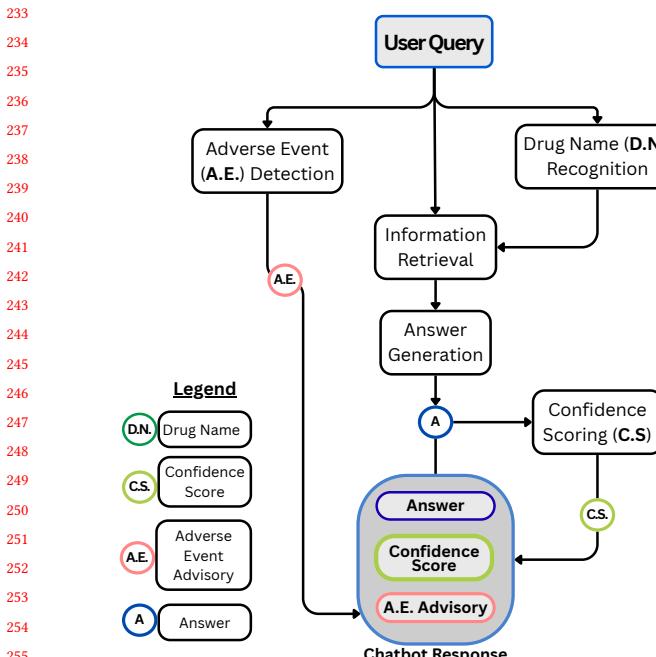


Figure 1: Flow of the Chatbot Interaction from User Question to Response Generation.

at Ericsson [6], aerospace [26], and tourism [15]. These efforts show how domain-grounded retrieval can mitigate hallucinations and improve contextual relevance, an insight increasingly applied to regulated settings such as pharmacovigilance, where Painter et al. [20] explored LLMs for drug-safety document retrieval.

These studies demonstrate the utility of LLMs for pharmaceutical-oriented tasks and highlight the promise of chatbots built around them in industrial contexts. In this paper we share our experience developing an LLM-based chatbot to address user inquiries about the drug products offered by a global pharmaceutical company.

4 Chatbot Design

We design the pharmaceutical chatbot to reduce the turnaround time for pharmaceutical questions, thereby improving the efficiency of health professionals by providing trusted, timely responses to their questions. Figure 1 shows the flow of the chatbot. The chatbot is designed using a retrieval-augmented generation (RAG) pipeline, augmented by specialized components such as custom entity recognizers trained on domain-specific data, a hybrid retrieval component that retrieves information from internal databases and the web, and a confidence scoring component to measure the trustworthiness of the response.

4.1 Corpus Creation for Internal Documents

Data Extraction. We ingest two data sources, i.e., the product monographs and the FAQ documents, as presented in section 2. When extracting information from the product monograph, we first extract all the top-level sections. If a section contains subsections,

we also extract the subsections and create a reference for each subsection to their top-level section. Then we extract the tables as separate entities and link them to their captions as metadata. The FAQ questions are also extracted and mapped to their corresponding answers.

Data Preprocessing and Indexing. When preprocessing the monographs, the extracted sections, subsections, and tables are processed as individual data chunks. We summarize each data chunk and use the summary for embedding creation. The embeddings of the summaries are mapped to the original chunks and are indexed in a vector store for embedding-based retrieval.

For data from the FAQ documents, each question forms a unique chunk, and a direct reference is created to its corresponding answer. These question-answer pairs are indexed in a vector store, allowing the chatbot to perform embedding-based retrieval.

4.2 Chatbot Walkthrough

The chatbot accepts the user's question in natural language and maintains conversational state across multiple turns. Each request is processed by handling the session state of the conversation. When a user submits a question, the chatbot attaches a unique session identifier and retrieves any existing conversation context. This allows the chatbot to recall previous questions and responses, maintaining continuity across turns.

The chatbot applies custom-trained Named Entity Recognition (NER) models to extract drug names, variants, and adverse events from the user's question. If multiple formulations or dosage forms exist for the identified drug, the chatbot prompts the user to select the correct variant in its response.

Based on the recognized drug, the chatbot retrieves relevant information from multiple sources. First, it checks the FAQ documents of the identified drug, and uses a semantic similarity search to find a question among the FAQs that matches the user's question. If a match to a question in the FAQ is found (i.e. semantic similarity higher than the specified threshold), the corresponding answer forms the basis of the chatbot's response to the user's question.

If the user's question does not match a question in the FAQ document (i.e. semantic similarity lower than the specified threshold), the retrieval component expands the search to the product monograph of the drug and a web search. The retrieval component uses similarity search to find the most relevant paragraphs in the monograph to answer the question. When conducting the web search, the retrieval component restricts the search to trusted domains (e.g., official regulatory agencies).

The retrieved paragraphs and the web results, along with the user's question and session context, are passed to the LLM to generate a response. We construct a prompt that instructs the LLM to prioritize information from the monograph, to avoid speculation, and to produce a concise, well-structured answer. After the LLM generates an answer, we compute a confidence score based on factors such as the model's internal certainty (log probabilities), the similarity score between the answer and retrieved context, and the sources of the information retrieved from the web. The final response, with the references and the confidence score, is returned to the user as shown in Figure 2. The adverse events, if detected are recorded separately for patients safety reports.

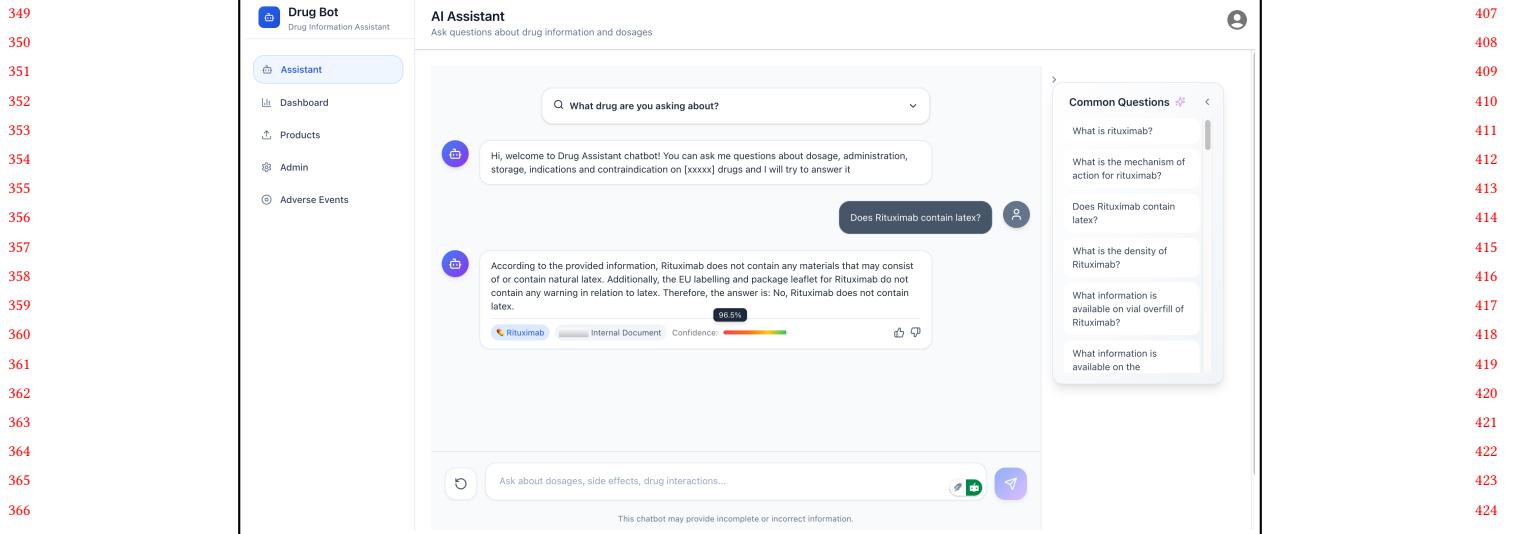


Figure 2: User Interface of the Pharmaceutical Chatbot. The UI shows the questions asked by the user, the response by the chatbot, the identified drug in the question, the source of the information used for the answer and the confidence score for the response.

5 Challenges and Mitigations

During the development of the chatbot for the pharmaceutical company, we had to address both technical and domain-specific challenges to meet regulatory and functional requirements. In this section, we discuss the challenges encountered and the strategies adopted to mitigate them.

5.1 Data Retrieval Challenges

Challenge I. Retrieving information accurately from product monographs.

Our experience in the early stages of developing the chatbot revealed that retrieving accurate information from the knowledge base for a drug posed a significant challenge. This challenge was particularly evident with the product monographs, which contain both unstructured text (often in long continuous paragraphs) and structured data in the form of tables. We found that the naive approach of using conventional dense retrieval with vector embeddings was inadequate, as simply partitioned chunks could omit important contextual information, reducing the effectiveness of the retrieval step. Moreover, direct embeddings of tables fail to capture their underlying structure and meaning, which limits their semantic representation. This limitation in the retrieval step affected the accuracy of the chatbot's responses.

Mitigation: To address this challenge and improve the performance of the retrieval step (and the subsequently generated answer), we implemented a summarization strategy that uses an LLM to summarize lengthy sections of the product monograph and generate descriptions of tabular data, prior to embedding. The resulting summaries and descriptions improve the effectiveness of the retrieval process, as the embeddings created from them capture more context.

Importantly, while we use embeddings of the summaries for the retrieval step, we maintain a map of each summary to its original text, which is used in the generation step (rather than the summary itself). This approach is similar to the strategy described by Liu [18] and Eibich et al. [9].

Challenge II. Retrieving reliable and current web information from reputable web source.

After implementing and integrating the web search component into the chatbot, we observed that the search process frequently returned information from unverified sources such as blogs. Given that the pharmaceutical domain is highly regulated, and responses from the chatbot must be accurate, trustworthy, and meet regulatory standards, we cannot rely on information from such sources. Doing so risks the chatbot producing answers based on outdated, speculative, or non-factual information, which can also violate regulatory requirements.

Mitigation: To address this, we implemented a **domain whitelisting and ranking system**. We consulted with our domain experts to make a list of reputable web domains from which we want the chatbot to retrieve information. We whitelisted these websites so that our web search component only retrieves and uses information from these pre-approved, reputable sources, such as Health Canada and official company publications. Also, in consultation with the domain experts, we implemented a ranking system to rank the pre-approved domains by reliability, ensuring that regulatory data took precedence over secondary literature or public repositories. For instance, information from Health Canada (which maintains a repository of verified information about drug products in Canada) is given higher priority and credence than information from PubMed, despite the latter's strong reputation. This filtering and weighting

465 mechanism reduced noise and improved the factual integrity of
 466 generated responses.

467 468 5.2 Response Generation Challenges

469 470 **Challenge III.** Ensuring responses from the chatbot are trust-
 471 worthy.

473 In designing our chatbot, an important consideration is that
 474 users must find the answers from our chatbot useful [10, 27]. For a
 475 critical domain like pharmaceuticals, the answers from our chatbot
 476 must be factual and trustworthy for users to find them useful. In
 477 this context, the utilization of LLMs presents a challenge as they
 478 are prone to *hallucination*, potentially generating uncertain and
 479 factually incorrect responses. In the pharmaceutical domain, such
 480 hallucinations can have adverse consequences for users and erode
 481 trust in the chatbot's reliability. As such, answers generated by the
 482 chatbot must be verifiable by users to build and maintain trust in
 483 the chatbot's responses.

484 **Mitigation:** To address this, we introduced a **confidence scor-
 485 ing strategy** that quantifies the trustworthiness of the chatbot's
 486 response. The chatbot computes a confidence score based on the
 487 source of information used to answer the question. For instance,
 488 if the question is answered using information in the FAQ docu-
 489 ment, the confidence score is calculated from the combination of
 490 the retrieval similarity scores between the user's question and the
 491 FAQ entries with token-level log probabilities from the LLM. If
 492 the question is answered using information from monographs and
 493 web content, it combines the question complexity, the semantic
 494 similarity score of the retrieved documents, source reliability from
 495 web retrievals, and the token-level log probabilities from the LLM
 496 to compute the confidence score. The confidence score is returned
 497 with each response, allowing users to interpret the chatbot's cer-
 498 tainty in the response. The user might consider a response with a
 499 95% confidence score as trustworthy, while a response with a 50%
 500 confidence score would be considered less trustworthy and there-
 501 fore the user will not rely on it for decision-making. By combining
 502 multiple parameters to quantify the confidence of a response, the
 503 confidence score ensures transparency and prevents our chatbot
 504 from overconfidently providing low-certainty responses. In addi-
 505 tion to confidence scores, the chatbot returns a list of consulted
 506 documents, including hyperlinks to them where available, for each
 507 response. This enables users to verify the chatbot's answer against
 508 the underlying source materials.

509 510 5.3 Challenges Related to User Interaction

511 512 **Challenge IV.** Robust recognition of drug names in questions.

513 Users may make mistakes when typing drug names, such as
 514 misspellings or incomplete names, which can hinder accurate re-
 515 trieval. This presents a challenge for our chatbot, as inaccurate
 516 or incomplete drug names can hamper the information retrieval
 517 process. At the same time, requiring users to input drug names
 518 precisely imposes a practical burden that may hinder the user ex-
 519 perience. In addition to the potential for mistyped drug names, some
 520 drug products have multiple names: a **generic name**, shared by all

521 products containing the same active molecule, and a **brand name**
 522 that uniquely identifies the specific offering of the pharmaceutical
 523 company. A user may use either of these names in a question, ne-
 524 cessitating a mechanism that consistently maps all known names
 525 to the same underlying product and knowledge base.

526 **Mitigation:** To address this challenge, we implemented a **type-
 527 ahead recommendation** feature in the chatbot interface that
 528 suggests drug names as the user types. This feature reduces the
 529 cognitive and typing burden on users, particularly for complex
 530 drug names, and helps minimize input errors that could otherwise
 531 hinder accurate retrieval. In addition, we trained our NER model
 532 for drug names to tolerate minor misspellings and integrated a spell
 533 correction mechanism that works at inference time to map mis-
 534 spelled drug names to their correct forms. Finally, to address cases
 535 where a drug has multiple names, we implemented a **normaliza-
 536 tion pipeline** that links brand and generic names of the company's
 537 products. During data ingestion and processing the user's ques-
 538 tion, all drug mentions are normalized to a single canonical form,
 539 ensuring that they resolve to the same underlying data collection
 540 and responses remain consistent regardless of which variant of the
 541 drug name appears in a question.

542 543 **Challenge V.** Handling multiple dosage forms and concentra-
 544 545 tion levels of the same drug.

546 547 Some drugs in the database of the pharmaceutical company have
 548 multiple dosage forms and/or concentration levels. The different
 549 dosage forms sometimes have different concentration levels. For
 550 example, drug A has both tablets (with a concentration level of 50
 551 mcg) and injections (concentration level of 100 mg/mL) as dosage
 552 forms. In some cases, users ask about the drug without specifying
 553 the variant. For example, "How should I store drug A?". This situa-
 554 tion leaves the chatbot uncertain about which variant to reference,
 555 increasing the risk of mixing up information in its responses.

556 557 **Mitigation:** To handle this ambiguity, we designed the chatbot
 558 with an **interactive clarification mechanism**. When a query
 559 about a product with multiple variants is presented, the chatbot
 560 responds with a clarification prompt that lists the available dosage
 561 forms or concentration levels. Once the user selects the relevant
 562 form, that choice is stored in the session context and persists until
 563 the user switches to another drug or formulation. This prevents
 564 misinterpretation and ensures that accurate information is provided
 565 to the user about the variant of interest.

566 567 5.4 Challenges Related to Compliance

568 569 **Challenge VI.** Identifying adverse events in user questions.

570 571 As part of regulatory compliance for monitoring and patient
 572 safety, our pharmaceutical chatbot must detect when users describe
 573 possible adverse drug reactions, as such cases require escalation
 574 or proper guidance. In line with pharmacovigilance responsibili-
 575 ties—and recognizing that regulators require prompt reporting of
 576 *serious* and *serious and unexpected* adverse reactions—the chatbot
 577 must maintain the capability to identify potential adverse events in
 578 user interactions. Each drug has its adverse event catalogue in the
 579 product monograph; however, relying on the LLM alone to detect

adverse events in users' questions is not always accurate, especially because adverse event descriptions may be implicit or ambiguous and some reactions are uncommon and specific to a given product. For example, for a drug administered as a patch, patients might experience adverse reactions if the patch falls off frequently, and such incidents have to be reported.

Mitigation: To address this challenge, we curated an **adverse event corpus** derived from product monographs and reported adverse-event databases, and trained a specialized NER model to recognize adverse-event mentions in questions. When such events are detected, the chatbot invokes a safety workflow that advises the user on appropriate reporting procedures (through a formal channel) and prevents the generation of potentially unsafe recommendations. In addition, a record of the adverse event, including the drug discussed in the conversation, is securely stored and shared with the appropriate stakeholders for review and action.

6 Lessons Learned

Our experience building the chatbot for information inquiries in the pharmaceutical domain yielded valuable lessons. In this section, we share these lessons, as we believe they offer valuable insights to the BoatSE and broader software engineering communities.

Designing such chatbots requires an interdisciplinary collaboration. It is important to have knowledge and inputs from domain experts when building domain-specific chatbots. During the development, our domain experts observed that our chatbot missed details like the brand names of drugs and adverse events associated with some drugs. With guidance from our domain experts, we curated domain-specific training data, built custom entity recognizers, and ran continuous reviews with the domain experts. This ensured that the chatbot could accurately answer questions about specific drug brand names and accurately identify adverse events, which is required for regulatory compliance.

Also, within our trusted, whitelisted domains, our domain experts found that information retrieved when using a drug's generic name can include details from brands other than our partner pharmaceutical company. The experts explained the issue with this is the same drug from a different manufacturers can have different inactive ingredients and concentration levels. Thus, using this information to answer questions can lead to inconsistent and incorrect responses. As a lesson, we always ensure that priority is given to the most trusted web domains. In our chatbot, results, with information from our partner pharmaceutical company ranked highest, followed by regulatory agencies and then secondary literature.

Prompting in Regulated Domains Requires Explicit Guardrails. Define the role and scope of the LLM when developing LLM-based chatbots. When developing chatbots for specific domains, it is essential to guard the chatbot from responding to questions not related to the domain to prevent abuse of the chatbot. For instance, in our chatbot, we have a default response when users ask questions that are irrelevant, like "*what is the recipe for apple pie*". Also, we explicitly define additional guardrails in our prompt to safeguard the chatbot to ensure the responses are safe. For example, we instruct the model to use information from the approved sources only, giving priority to those from highly rated pages and not rely

on its internal knowledge, which could be at risk of being outdated or incorrect.

7 Conclusion

In this paper, we share our experience developing and deploying a retrieval-augmented (RAG) LLM-based chatbot for pharmaceutical question answering. Our chatbot integrates domain-specific entity recognition to identify names of drugs in users' questions, embedding-based retrieval to obtain information from internal documents like monographs and FAQs for answer generation, performs web searches on a curated whitelist of domains, and uses a confidence-scoring framework to enhance the trustworthiness of the chatbot's responses. We also implement a patient safety feature that detects and reports any adverse events in the user's question to align with regulatory compliance.

In the paper, we highlight some of the challenges we encountered while deploying the chatbot and share the strategies we adopted to mitigate these challenges. We highlight that domain expert guidance is key when building safety-critical systems, that summary-based retrieval can improve performance, and that ensuring information for answering users' questions is sourced from reputable domains is essential. Our mitigation strategies and the lessons we share can serve as a reference and guidance for software engineers building chatbots in highly regulated domains and for the BoatSE community.

References

- [1] Eleni Adamopoulou and Lefteris Moussiades. 2020. Chatbots: History, Technology, and Applications. *Machine Learning with Applications* 2 (Dec. 2020), 100006. doi:10.1016/j.mlwa.2020.100006
- [2] Zahraa Al-Dujaili, Sarah Omari, Jey Pillai, and Achraf Al Faraj. 2023. Assessing the Accuracy and Consistency of ChatGPT in Clinical Pharmacy Management: A Preliminary Analysis with Clinical Pharmacy Experts Worldwide. *Research in Social and Administrative Pharmacy* 19, 12 (Dec. 2023), 1590–1594. doi:10.1016/j.sapharm.2023.08.012
- [3] Jennifer Beavers, Ryan F. Schell, Halden VanCleave, Ryan C. Dillon, Austin Simmons, Huiding Chen, Qingxia Chen, Shila Anders, Matthew B. Weinger, and Scott D. Nelson. 2023. Evaluation of Inpatient Medication Guidance from an Artificial Intelligence Chatbot. *American journal of health-system pharmacy: AJHP: official journal of the American Society of Health-System Pharmacists* 80, 24 (Dec. 2023), 1822–1829. doi:10.1093/ajhp/zxad193
- [4] Health Canada. 2016. Guidance Document: Product Monograph. <https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/applications-submissions/guidance-documents/product-monograph/guidance-document-product-monograph.html>.
- [5] Sri Harsha Chalasani, Jehath Syed, Madhan Ramesh, Vikram Patil, and T.M. Pramod Kumar. 2023. Artificial Intelligence in the Field of Pharmacy Practice: A Literature Review. *Exploratory Research in Clinical and Social Pharmacy* 12 (Oct. 2023), 100346. doi:10.1016/j.crsop.2023.100346
- [6] Daksh Chaudhary, Sri Lakshmi Vadlamani, Dimple Thomas, Shiva Nejati, and Mehrdad Sabetzadeh. 2024. Developing a Llama-Based Chatbot for CI/CD Question Answering: A Case Study at Ericsson. In *2024 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE Computer Society, 707–718. doi:10.1109/ICSM58944.2024.00075
- [7] Zhisheng Chen. 2025. Revolutionizing Finance with Conversational AI: A Focus on ChatGPT Implementation and Challenges. *Humanities and Social Sciences Communications* 12, 1 (March 2025), 388. doi:10.1057/s41599-025-04725-y
- [8] Davi Dos Reis de Jesus, Antônio Pereira de Souza Júnior, Elisa Tuler de Albergaria, Adriana Silvina Pagano, Isaías Jose Ramos de Oliveira, Cristiane Dos Santos Dias, Eura Martins Lage, Flávia Ribeiro de Oliveira, Juliana Almeida Oliveira, Igor de Carvalho Gomes, Leonardo Chaves Dutra da Rocha, and Zilma Silveira Nogueira Reis. 2025. Enhanced LLM-supported Instructions for Medication Use through Retrieval-Augmented Generation. *Computers in Biology and Medicine* 198, Pt A (Oct. 2025), 111135. doi:10.1016/j.combiomed.2025.111135
- [9] Matouš Eibich, Shivay Nagpal, and Alexander Fred-Ojala. 2024. ARAGOG: Advanced RAG Output Grading. doi:10.48550/arXiv.2404.01037 arXiv:2404.01037

- 697 [cs].
 698 [10] Asbjørn Følstad and Petter Bae Brandtzaeg. 2020. Users' experiences with
 699 chatbots: findings from a questionnaire study. *Quality and User Experience*
 700 5, 1 (April 2020), 3. doi:10.1007/s41233-020-00033-2
 701 [11] Jung Yeol Han. 2025. Usefulness and Limitations of Chat GPT in Getting Infor-
 702 mation on Teratogenic Drugs Exposed in Pregnancy. *Obstetrics & Gynecology*
 703 *Science* 68, 1 (Jan 2025), 1–8. doi:10.5468/ogs.24231
 704 [12] Shweta Handoo, Vandana Arora, Deepak Khera, Prafulla Kumar Nandi, and
 705 Susanta Kumar Sahu. 2012. A Comprehensive Study on Regulatory Requirements
 706 for Development and Filing of Generic Drugs Globally. *International Journal of*
 707 *Pharmaceutical Investigation* 2, 3 (2012), 99–105. doi:10.4103/2230-973X.104392
 708 [13] Health Canada. 2018. Reporting Adverse Reactions to Marketed Health
 709 Products: Guidance Document for Industry. <https://www.canada.ca/en/health->
 710 canada/services/drugs-health-products/public-involvement-consultations/
 711 medeffect-canada/consultation-reporting-adverse-reactions-marketed-health-
 712 products-guidance-document-industry/document.html#s1 Guidance document,
 713 Government of Canada.
 714 [14] Nikhil Kandpal, Haikang Deng, Adam Roberts, Eric Wallace, and Colin Raffel.
 715 2023. Large Language Models Struggle to Learn Long-Tail Knowledge. In *Proceed-
 716 ings of the 40th International Conference on Machine Learning (ICML'23, Vol. 202).*
 717 JMLR.org, Honolulu, Hawaii, USA, 15696–15707.
 718 [15] Pattama Krataithong, Watchira Buranasing, Marut Buranarach, Theerawat Wut-
 719 thitasarn, Pattraporn Meeklai, and Patipat Tumsangthong. 2025. Tourism Chat-
 720 bot Framework: Enhancing Visitor Experience Through GraphRAG and AI Chat-
 721 bot. In *2025 IEEE International Conference on Cybernetics and Innovations (ICCI)*.
 722 1–6. doi:10.1109/ICCI64209.2025.10987390
 723 [16] Lulu Li, Pengqiang Du, Xiaojing Huang, Hongwei Zhao, Ming Ni, Meng Yan, and
 724 Aifeng Wang. 2025. Comparative Analysis of Generative Artificial Intelligence
 725 Systems in Solving Clinical Pharmacy Problems: Mixed Methods Study. *JMIR*
 726 *medical informatics* 13 (July 2025), e76128. doi:10.2196/76128
 727 [17] Xiangci Li, Zhiyi Chen, Jason Ingyu Choi, Nikhita Vedula, Besnik Fetahu, Oleg
 728 Rokhlenko, and Shervin Malmasi. 2025. Wizard of Shopping: Target-Oriented
 729 E-commerce Dialogue Generation with Decision Tree Branching. In *Proceed-
 730 ings of the 63rd Annual Meeting of the Association for Computational Linguistics
 731 (Volume 1: Long Papers)*, Wanxiang Che, Joyce Nabende, Ekaterina Shutova, and
 732 Mohammad Taher Pilehvar (Eds.). Association for Computational Linguistics,
 733 Vienna, Austria, 13095–13120. doi:10.18653/v1/2025.acl-long.641
 734 [18] Jerry Liu. 2023. A New Document Summary Index for LLM-powered QA Sys-
 735 tems. <https://www.llamaindex.ai/blog/a-new-document-summary-index-for-llm-powered-qa-systems-9a32ece2f9ec>
 736 [19] Harsha Nori, Nicholas King, Scott Mayer McKinney, Dean Carignan, and
 737 Eric Horvitz. 2023. Capabilities of GPT-4 on Medical Challenge Problems.
 738 arXiv:2303.13375 [cs] doi:10.48550/arXiv.2303.13375
 739 [20] Jeffery L. Painter, Olivia Mahaux, Marco Vanini, Vijay Kara, Christie Roshan,
 740 Marcin Karwowski, Venkateswara Rao Chalamalasetti, and Andrew Bate. 2023.
 741 Enhancing Drug Safety Documentation Search Capabilities with Large Language
 742 Models: A User-Centric Approach. In *2023 International Conference on Com-
 743 putational Science and Computational Intelligence (CSCI)*. 49–56. doi:10.1109/
 744 CSCI62032.2023.00015
 745 [21] Philipp Reinhard, Mahei Manhai Li, Christoph Peters, and J. M. Leimeister.
 746 2024. Generative AI in Customer Support Services: A Framework for Aug-
 747 menting the Routines of Frontline Service Employees. *social science research*
 748 network:4862940 doi:10.2139/ssrn.4862940
 749 [22] Steven I. Ross, Fernando Martinez, Stephanie Houde, Michael Muller, and Justin D.
 750 Weisz. 2023. The Programmer's Assistant: Conversational Interaction with a
 751 Large Language Model for Software Development. In *Proceedings of the 28th Inter-
 752 national Conference on Intelligent User Interfaces (IUI '23)*. Association for Com-
 753 puting Machinery, New York, NY, USA, 491–514. doi:10.1145/3581641.3584037
 754 [23] Kuldeep Singh, Simerjot Kaur, and Charese Smiley. 2024. FinQAPT: Empowering
 755 Financial Decisions with End-to-End LLM-driven Question Answering Pipeline.
 756 In *Proceedings of the 5th ACM International Conference on AI in Finance (ICAIF*
 757 '24). Association for Computing Machinery, New York, NY, USA, 266–273. doi:10.
 758 1145/3677052.3698682
 759 [24] Karan Singhal, Tao Tu, Juraj Gottweis, Rory Sayres, Ellery Wulczyn, Mohamed
 760 Amin, Le Hou, Kevin Clark, Stephen R. Pfohl, Heather Cole-Lewis, Darlene Neal,
 761 Qazi Mamunur Rashid, Mike Schaeckermann, Amy Wang, Dev Dash, Jonathan H.
 762 Chen, Nigam H. Shah, Sami Lachgar, Philip Andrew Mansfield, Sushant Prakash,
 763 Bradley Green, Ewa Dominowska, Blaise Agüera y Arcas, Nenad Tomašev, Yun
 764 Liu, Renee Wong, Christopher Semturs, S. Sara Mahdavi, Joelle K. Barra, Dale R.
 765 Webster, Greg S. Corrado, Yossi Matias, Shekoofeh Azizi, Alan Karthikesalingam,
 766 and Vivek Natarajan. 2025. Toward Expert-Level Medical Question Answering
 767 with Large Language Models. *Nature Medicine* 31, 3 (March 2025), 943–950.
 768 doi:10.1038/s41591-024-03423-7
 769 [25] David Steybe, Philipp Poxleitner, Suad Aljohani, Bente Brokstad Herlofson,
 770 Ourania Nicolatou-Galitis, Vinod Patel, Stefano Fedele, Tae-Geon Kwon, Vittorio
 771 Fusco, Sarina E. C. Pichardo, Katharina Theresa Obermeier, Sven Otto, Alexan-
 772 der Rau, and Maximilian Frederik Russe. 2025. Evaluation of a context-aware
 773 chatbot using retrieval-augmented generation for answering clinical questions
 774

755
 756
 757
 758
 759
 760
 761
 762
 763
 764
 765
 766
 767
 768
 769
 770
 771
 772
 773
 774
 775
 776
 777
 778
 779
 780
 781
 782
 783
 784
 785
 786
 787
 788
 789
 790
 791
 792
 793
 794
 795
 796
 797
 798
 799
 800
 801
 802
 803
 804
 805
 806
 807
 808
 809
 810
 811
 812