Hazard Analysis
CXR

Team 27, Neuralyzers
Ayman Akhras
Nathan Luong
Patrick Zhou
Kelly Deng
Reza Jodeiri

Date	Developer(s)	Change
Date1	Name(s)	Description of changes
Date2	Name(s)	Description of changes
...	...	...

Table 1: Revision History

Contents

1 Introduction

Following the principles outlined by **?**, a hazard in our AI-based chest X-ray analysis system is any condition or event that could negatively affect the system's operation, integrity, or safety. This includes software bugs, hardware failures, user mistakes, or external disruptions. A hazard becomes significant when it might interfere with the system's ability to provide accurate diagnostic support, protect patient confidentiality, or operate reliably in clinical settings.
This document presents a detailed hazard analysis of our AI-powered chest X-ray analysis application. Throughout this document, we identify potential hazards and suggest ways to eliminate or reduce them. By examining different types of hazards, assessing how likely they are to happen and how severe they might be, and proposing actions to address them, we aim to improve the safety and security requirements for our project.

2 Scope and Purpose

The purpose of this hazard analysis is to identify potential hazards in our AI-based chest X-ray analysis system and to propose ways to mitigate them. We focus on specific system components and boundaries to enhance the safety and reliability of the system. While we recognize that certain external factors, like differences in input image quality or user environments, are beyond our control, our system is designed to handle standard digital chest X-ray images provided by qualified healthcare professionals.
We assume that all system functions—especially those related to image processing, AI analysis, and reporting results—are working as intended. With this in mind, we concentrate on strengthening key components, such as the user interface, backend servers, machine learning models, and data storage systems, to prevent potential failures. Our goal is to ensure that the system provides an accurate, secure, and reliable experience that supports healthcare professionals in diagnosing and managing chest diseases.

3 System Boundaries

3.1 System Components

The system consists of the following main components:

- User Interface (Web Application)
- Backend Servers and APIs
- Machine Learning Model and Inference Engine
- Data Storage and Management Systems
- Security and Authentication Modules

These components are essential to our system's functionality. They handle user interactions, data processing, AI-based analysis, and secure data management.

3.2 Environment Components

The system interacts with the following external components:

- External Medical Imaging Systems (e.g., Picture Archiving and Communication Systems)
- Standard Digital Chest X-ray Images
- Network Infrastructure (Internet Connectivity)

These environment components influence how our system operates. While they are outside our system, they play a critical role in ensuring a smooth and effective user experience in clinical settings.

4 Critical Assumptions

To keep the hazard assessment focused and effective, we make the following critical assumptions:

1. We expect users to upload only legitimate and appropriate medical images. However, we recognize that irrelevant or corrupted data may sometimes be uploaded, and measures should be in place to detect and handle such inputs.
2. We assume that users are qualified healthcare professionals with the necessary training to interpret the system's outputs correctly. The system is primarily intended for professional use in clinical settings.
3. Our system is designed to handle unintentional user errors and common misuse scenarios, but it may not be fully protected against deliberate malicious activities aimed at exploiting vulnerabilities or deceiving the AI algorithms.
4. Our hazard analysis for external environment components, like network infrastructure and third-party systems, considers typical use cases and does not cover extreme conditions outside the intended operation of the system.

5 Failure Modes and Effects Analysis

The Failure Modes and Effects Analysis (FMEA) was selected as the hazard analysis tool to help identify, assess, and propose solutions to the risks and hazards associated with our AI-based chest X-ray analysis system.

5.1 Hazards Out of Scope

- Failures related to external AI libraries (e.g., TorchXRayVision)
- Issues due to external data sources (e.g., incorrect image formats or corrupted data files)
- Failures of the external hardware used by healthcare professionals

Our project is not responsible for the hazards listed above, as they are controlled by third-party systems or external users. While we will take steps to minimize the impact of these hazards, complete mitigation cannot be guaranteed.

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
Image Input System	Failure to upload chest X-ray images to the system.	Delays in diagnosis and analysis, affecting clinical workflow.	a. Incompatible file formats or corrupted images cause upload failures. b. Insufficient server storage space leads to failed uploads.	a. Validate image files during upload by checking formats and integrity, and provide immediate error messages to guide users in resolving issues. b. Monitor server storage capacity regularly, and employ scalable storage solutions like AWS S3 to ensure adequate space is available.	SR1	FM1
Image Input System	System fails to process or analyze uploaded images due to poor image quality.	Inaccurate AI analysis leading to misdiagnosis.	a. System lacks mechanisms to detect and handle poor-quality images. b. Insufficient preprocessing capabilities to enhance or correct image quality issues. c. Absence of feedback to users when images are unsuitable for analysis. d. Limitations in the AI model to handle variations in image quality.	a. Implement image quality assessment during upload, providing warnings or errors if images do not meet quality thresholds. b. Enhance preprocessing algorithms to improve image quality where possible, such as noise reduction. c. Provide users with guidelines on acceptable image quality and instructions for obtaining better images if necessary. d. Train the AI model on a diverse dataset that includes variations in image quality to improve robustness.	SR2	FM2

Table 2: FMEA for Image Input Component (FM1 and FM2)

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
User Interface	Interface is non-intuitive or difficult to navigate for healthcare professionals.	Decreased efficiency and user frustration	a. Inconsistent use of medical terminology and symbols leads to confusion. b. Lack of user training or insufficient documentation. c. Interface not optimized for different devices or screen resolutions.	a. Standardize terminology and symbols according to medical standards, and ensure consistency throughout the interface. b. Provide comprehensive training materials, including user manuals and tutorials, and offer ongoing support. c. Test the interface across various devices and screen sizes, optimizing responsive design to ensure accessibility.	SR3	FM3
User Interface	Displays incorrect or misleading analysis results.	Risk of misdiagnosis due to wrong information.	a. Bugs in UI logic lead to incorrect data display. b. Data mismatch between frontend and backend systems causes inconsistencies. c. Network issues result in incomplete data retrieval, leading to partial displays.	a. Fix UI logic errors by conducting code reviews focusing on data binding and state management, and implementing unit tests for UI components. b. Ensure data synchronization by using consistent data formats, implementing version checks, and validating data integrity between frontend and backend. c. Implement reliable data retrieval methods using robust APIs with error handling and providing user feedback during data loading.	SR4	FM4

Table 3: FMEA for User Interface Component (FM3 and FM4)

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
Data Preprocessing	Incorrect preprocessing of chest X-ray images before AI analysis.	AI model receives improperly formatted data, leading to reduced accuracy or errors.	a. Misalignment in image resizing results in images not scaled to required dimensions. b. Incorrect normalization or standardization of pixel values distorts image data.	a. Implement strict preprocessing protocols and validate image dimensions using automated checks in the data pipeline. b. Utilize standardized libraries (e.g., PyTorch transforms) for image normalization, ensuring consistent preprocessing steps.	SR5	FM5
Data Preprocessing	Data augmentation introduces artifacts that mislead the AI model.	AI model learns from distorted data, leading to poor generalization and increased errors.	a. Introduction of noise that do not represent real-world variations. b. Mislabeling augmented data due to incorrect augmentation metadata handling. c. Lack of validation on the quality and clinical relevance of augmented datasets.	a. Monitor the quality of augmented images by reviewing samples and ensuring they maintain anatomical correctness. b. Verify and maintain accurate labels and metadata post-augmentation by automating checks and utilizing data integrity tools. c. Incorporate validation steps to assess the impact of augmentation on model performance, adjusting techniques based on results.	SR6	FM6

Table 4: FMEA for Data Preprocessing Component (FM5 and FM6)

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
AI Module	AI model misclassifies chest X-ray images, providing incorrect diagnoses.	Potential misdiagnosis leading to inappropriate treatment plans and patient harm.	a. Training data includes poor-quality images or lacks diversity, leading to biased model performance. b. Software bugs in the CNN architecture implementation or data preprocessing pipeline.	a. Levrage a high-quality, diverse training dataset, ensuring representation across demographics and conditions. b. Conduct thorough code reviews, unit tests, and integration tests on the AI model and preprocessing code.	SR7	FM7
AI Module	Model fails to improve over time despite updates.	Inability to detect new or rare conditions, reducing clinical effectiveness.	a. Insufficient incorporation of new training data or lack of ongoing data collection. b. Failure to integrate feedback from radiologists and healthcare professionals.	a. Establish a continuous data collection pipeline. b. Create a feedback loop with clinicians to gather real-world performance data and insights.	SR8	FM8

Table 5: FMEA for AI Module Component (FM7 and FM8)

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
Backend Services	Experiences slow response times or timeouts during image upload and analysis requests.	Users face delays, reducing efficiency in clinical workflow .	a. High server load due to multiple concurrent image processing requests overwhelms resources. b. Inefficient code or algorithms cause bottlenecks, such as unoptimized database queries or synchronous processing. c. Insufficient server resources (CPU, memory) lead to lower performance.	a. Implement load balancing mechanisms to distribute requests, and optimize server configurations for concurrency. b. Optimize backend code by profiling performance, improving algorithms, implementing asynchronous processing where appropriate, and optimizing database queries. c. Scale server resources dynamically using AWS Auto Scaling groups, and monitor resource utilization to adjust as needed.	SR9	FM9
Backend Services	Experiences server downtime or crashes.	System is unavailable, affecting patient care.	a. The server cannot handle peak loads due to lack of scalability. b. Unplanned maintenance or deployment errors result in service interruptions.	a. Adjust capacity based on demand, ensuring sufficient server instances are running during peak times. b. Schedule maintenance during off-peak hours with advance notifications to users, and test updates in staging environments before production.	SR10	FM10

Table 6: FMEA for Backend Services Component (FM9 and FM10)

Component	Failure Mode	Effect	Cause	Recommended Action	SR	Ref
Data Storage	Experiences data loss or corruption of chest X-ray images and patient records.	Loss of critical medical data, disrupting patient care and violating data retention policies.	a. Software bugs cause data corruption during processing or storage operations. b. Accidental deletion of data by users or administrators due to inadequate safeguards. c. Inadequate backup procedures or failure to test data recovery processes.	a. Implement data validation checks during processing and use database transactions to maintain data integrity. b. Enforce strict permissions, employ deletion safeguards like multi-factor authentication for deletions, and provide training to prevent accidental deletions. c. Establish regular automated backups, and periodically test data recovery procedures to ensure they function correctly.	SR11	FM11
Security Modules	Suffers security issues leading to unauthorized access to personal information.	Exposure of patient data, violating HIPAA and PIPEDA regulations, leading to legal consequences and loss of trust.	a. Weak authentication mechanisms allow unauthorized access. b. Insufficient data encryption at rest and in transit exposes sensitive information. c. Inadequate access controls and monitoring fail to detect or prevent unauthorized activities.	a. Strengthen authentication using multi-factor authentication and enforce strong password policies. b. Encrypt data at rest using AWS KMS and enforce SSL/TLS protocols for data in transit to secure communications. c. Implement role-based access control (RBAC), monitor activities using AWS CloudTrail, and set up alerts for suspicious activities.	SR12	FM12

Table 7: FMEA for Data Storage Component (FM11 and FM12)

6 Safety and Security Requirements

Using the results of the FMEA, we can derive the following safety and security requirements for our system to mitigate the identified hazards.

6.1 Security and Privacy Requirements

SR3: The system shall anonymize all chest X-ray images and associated patient data before processing or storage, ensuring that no personally identifiable information (PII) is retained.

Rationale: Anonymization protects patient privacy and complies with healthcare privacy regulations, preventing unauthorized access to sensitive information.

Fit Criterion: Security audits confirm that all stored and processed data is anonymized; attempts to retrieve PII from the system yield no results.

Traceability: FM15, FM19

SR4: The system shall define a data retention policy that specifies how long patient data is stored and ensures secure deletion procedures after the retention period expires.

Rationale: Limiting data retention minimizes the risk of data breaches and complies with legal requirements for data protection.

Fit Criterion: Policy documents outline data retention periods; system logs verify that data is securely deleted after expiration.

Traceability: FM14, FM15

SR5: The system shall implement a consent management system that allows patients to control the use and sharing of their data, in accordance with relevant privacy regulations.

Rationale: Obtaining and managing patient consent ensures ethical use of data and compliance with laws like HIPAA and GDPR.

Fit Criterion: Records show that patient consent is obtained and honored; audits confirm that data sharing aligns with patient preferences.

Traceability: FM15

SR6: The system shall create detailed audit trails that track all access to and modifications of patient data, enabling detection and investigation of unauthorized activities.

Rationale: Audit trails enhance security by providing accountability and facilitating incident response in case of security breaches.

Fit Criterion: Audit logs are comprehensive and tamper-proof; security reviews confirm that all access and changes are properly recorded.

Traceability: FM15, FM17

SR7: The system shall ensure compliance with all relevant healthcare privacy regulations, such as HIPAA, GDPR, and PIPEDA, by implementing necessary technical and administrative safeguards.

Rationale: Compliance with legal regulations is mandatory to protect patient rights and avoid legal penalties.

Fit Criterion: Compliance assessments confirm adherence to regulations; certification from authorized bodies is obtained where applicable.

Traceability: FM13, FM15

6.2 Health and Safety Requirements

HS3: The system shall ensure that all AI-generated diagnoses are reviewed and confirmed by qualified medical professionals before being used in patient care decisions.

Rationale: To prevent misdiagnoses and ensure patient safety by involving human oversight in the diagnostic process.

Fit Criterion: System workflow requires medical professional validation before finalizing reports; logs confirm this process.

Traceability: FM7, FM9

HS4: The system shall provide clear warnings and notifications if the input data quality is insufficient for reliable analysis, prompting users to provide better data.

Rationale: Processing poor-quality images can lead to inaccurate diagnoses, potentially harming patients; users should be aware of data limitations.

Fit Criterion: The system detects low-quality inputs and displays warnings; user acknowledgment is required before proceeding.

Traceability: FM7, FM8

HS5: The system shall maintain high availability and reliability, ensuring that critical functionalities are accessible with minimal downtime to support timely patient care.

Rationale: System outages or performance issues can delay diagnoses and treatments, negatively impacting patient health.

Fit Criterion: System uptime is maintained at 99.9% or higher; performance metrics meet specified thresholds.

Traceability: FM12, FM18

HS6: The system shall provide clear and actionable error messages to users in the event of failures or crashes, including guidance on how to proceed.

Rationale: Informative error messages help users take appropriate actions quickly, reducing potential delays in patient care.

Fit Criterion: User acceptance testing confirms that error messages are clear and helpful; documentation provides further guidance.

Traceability: FM9, FM10

HS7: The system shall include disclaimers indicating that AI analysis is a diagnostic aid and not a replacement for professional medical judgment.

Rationale: Users must understand the limitations of AI to prevent overreliance and potential errors in patient care.

Fit Criterion: Disclaimers are prominently displayed on analysis results; users acknowledge understanding upon first use.

Traceability: FM7, FM11

HS8: The system shall ensure that user interfaces are responsive and intuitive, minimizing the potential for user error and enhancing efficiency in clinical workflows.

Rationale: Poorly designed interfaces can lead to mistakes or delays, adversely affecting patient safety and care quality.

Fit Criterion: Usability testing confirms that interfaces meet specified usability standards; user feedback is positive.

Traceability: FM10, FM11

7 Roadmap

[Which safety requirements will be implemented as part of the capstone timeline? Which requirements will be implemented in the future? —SS]

Appendix — Reflection

[Not required for CAS 741 —SS]

1. What went well while writing this deliverable?
2. What pain points did you experience during this deliverable, and how did you resolve them?
3. Which of your listed risks had your team thought of before this deliverable, and which did you think of while doing this deliverable? For the latter ones (ones you thought of while doing the Hazard Analysis), how did they come about?
4. Other than the risk of physical harm (some projects may not have any appreciable risks of this form), list at least 2 other types of risk in software products. Why are they important to consider?