CSC 375 – Introduction to Systems Analysis

<u>Requirements Document</u>

Project Title	Reporting Pipeline Modernization
Team Members (Names)	Brian Pham, Xiangyu Yang, Wenchu Kan, Yilun Shi, Nitin Ruhil, Justin Chanhom
Group #	18

I. Functional Requirements	M	S	C	W
1. Data Reporting				
1.1 The system must provide a secure authenticated web-based interface for healthcare administrators and financial analysts to submit patient and financial data directly to the centralized reporting system. The interface will replace email- and Excel-based submissions, allowing users to enter information through a structured form after logging in.	x			
1.2 The system could provide a submission tracking dashboard displaying the status, history, and confirmation of each data entry. Users and managers can view submission timestamps, responsible staff, and version changes for traceability.			x	
1.3 The system will not automatically send confirmation emails or notifications upon submission in the first version. This feature would notify users when their data submission is received and stored successfully.				x
2. Data Processing				
2.1 The system must automatically validate all input data prior to submission to ensure content completeness and correct formatting, while preventing the submission of invalid or missing information. Examples include incorrect patient IDs or negative amounts.	x			
2.2 The system should incorporate a duplicate detection mechanism that automatically checks for identical patient IDs and submission times when users submit data, thereby preventing duplicate entries.			x	
2.3 The system can maintain detailed modification logs, recording the user, time, and specific changes for each data update to facilitate future tracking and auditing.				x

3. Transaction Handling					
3.1	The system must automatically direct each submitted dataset to the correct internal processing module based on its type (for example, patient information goes to the patient records module and financial information goes to the finance module). After processing, the data must be stored in the web system's database and then flow into the Health Authority's central data warehouse for reporting and analysis. This ensures that all data is handled through the correct workflow, eliminating the need for manual sorting or intervention.	x			
3.2	The system should support real-time monitoring of data across submission, validation, processing, and storage components through a management dashboard, enabling users and operational support teams/administrators to address errors and delays promptly.		x		
3.3	The system can generate an automatic data log that records each data transfer task, including the time, source and destination modules, and processing results, to support subsequent data traceability, review, and analysis.			x	

II. Non-Functional Requirements	M	S	C	W
1. External requirements				
1.1 The system must host and process data on servers physically located within Canada to prevent external data transfer outside jurisdiction.	x			
1.3 The system would not provide multilingual interface support for external stakeholders in the first version.				x
2. Product requirements				
2.1 The system must show results, alert messages, or web pages within **3 seconds** after a user submits data, so users do not have to wait too long.	x			
2.2 The system should maintain an uptime of 98.98% from 8AM-5PM. Staff should be able to access and operate the system during their work hours.		x		
2.3 The system could be built modularly, accommodating enhancements and data integrations from new legacy reports in the future without a full re-build.			x	
3. Organizational requirements				
3.1 The project must operate within the stated budget, and utilize resources and technologies as was stated in documentation.	x			
3.2 Progress and changes made to the project, both development-wise and structure-wise should be appropriately documented in a standardized format and stored in an internal repository.		x		
3.3 The project must comply with the client organization's data and information policies. Data and internal documents must be stored securely and must only be accessible to staff and developers with sufficient clearance.	x			