**Document 1- Business case document template**

1. **Why is this project initiated?**

**Security Improvements:** The current login module may not meet modern security standards, making it vulnerable to cyber threats.

**Regulatory Compliance:** Healthcare data is highly sensitive, requiring compliance with HIPAA, ACA, and other industry regulations.

**User Experience Enhancement:** Simplifying login while ensuring security to reduce authentication issues during annual healthcare enrollment peaks.

**Fraud Prevention:** Prevent unauthorized access to healthcare plans, employee benefits, and personal health records.

1. **What are the current problems?**

**Weak Password Policies:** Users may still can set weak passwords, increasing security risks.

**No Multi-Factor Authentication (MFA):** Single-factor authentication (password only) exposes accounts to phishing and brute-force attacks.

**Account Lockout & Recovery Issues**: Frequent lockouts due to password failures, causing delays during critical enrollment periods.

**Slow Login Performance**: High traffic during open enrollment results in delayed authentication and system crashes.

**Compliance Risks**: The current system may not fully align with HIPAA, SOC 2, or other security frameworks.

1. **With this project, how many problems could be solved?**

**Stronger Security:**

Implementing MFA (e.g., SMS/Authenticator app-based verification) reduces unauthorized access risks.

Using adaptive authentication to flag suspicious logins based on device, IP, and behavior.

Enforcing password complexity rules (e.g., minimum length, special characters, periodic changes).

**Better User Experience:**

Single sign-on (SSO) for seamless access across multiple systems.

Self-service password reset options to reduce IT support requests.

Optimized login performance to handle high traffic during enrollment.

**Regulatory Compliance & Risk Mitigation:**

Encryption and secure session management.

Audit logs and tracking login attempts for forensic investigations.

Meeting HIPAA/ACA data security requirements.

1. **What are the resources required?**

**Technical Teams:**

Developers – Enhance authentication mechanisms.

Cybersecurity Team – Implement MFA, threat detection, and compliance controls.

Cloud/Infrastructure Engineers – Ensure system scalability.

QA Testers – Test security, performance, and compliance.

**Non-Technical Teams:**

Compliance Experts – HIPAA, ACA, and data security assessments.

Change Management & Training Teams – Educate users on new login procedures.

Customer Support – Handle login-related queries and issues.

1. **How much organizational change is required to adopt this technology?**

Minimal for Users: MFA adoption will require user education, but an intuitive UX design can ease the transition.

Moderate for IT Teams: New configurations, monitoring tools, and policy updates will be needed.

Significant for Compliance & Security Teams: Policies will need updating, and HIPAA audits may be required.

1. **Time frame to recover ROI?**

Short-Term (6–12 months): Reduced helpdesk calls for password resets and account lockouts.

Mid-Term (12–24 months): Improved compliance, avoiding potential penalties for non-compliance.

Long-Term (2+ years): Increased user satisfaction and system efficiency during peak enrollment

1. **How to Identify Stakeholders?**

**Primary Stakeholders:**

 Employees & Customers – Impacted by login enhancements.

HR & Benefits Teams – Need smooth access during enrollment.

IT & Security Teams – Manage implementation and compliance.

Healthcare Partners & Insurers – May require integration with their systems.

**Secondary Stakeholders:**

Executives & Compliance Officers – Oversee security and legal risks.

Customer Support Teams – Handle login-related escalations.

Third-Party Vendors – If integrating external authentication services**.**

**Document 2 – BA approach strategy**

1. **Steps to Complete a Project**

1. Initiation: Understand project goals, objectives, and scope.
2. Planning: Define tasks, timelines, and deliverables.
3. Requirement Gathering: Conduct stakeholder interviews, workshops, and document business needs.
4. Analysis: Analyze requirements for feasibility and align them with business objectives.
5. Documentation: Prepare BRD, FRD, user stories, and other necessary documents.
6. Validation: Obtain stakeholder feedback and refine requirements.
7. Solution Assessment: Evaluate proposed solutions against requirements.
8. Implementation Support: Support development, testing, and deployment phases.
9. UAT Coordination: Assist stakeholders in User Acceptance Testing.
10. Closure: Facilitate sign-off on final deliverables and project acceptance.

**2. Elicitation Techniques to Apply**

* Interviews: One-on-one discussions with stakeholders.
* Workshops: Collaborative sessions to gather detailed requirements.
* Surveys/Questionnaires: For broader stakeholder input.
* Document Analysis: Review existing documentation and reports.
* Observation: Shadow users to understand current processes.
* Prototyping: Create mock-ups for user feedback.
* Brainstorming: Generate innovative solutions collaboratively.

**3. Stakeholder Analysis and RACI/ILS**

* Identify Stakeholders: Map stakeholders based on influence and interest.
* Analyze Stakeholders: Determine their roles, expectations, and concerns.
* RACI Chart:
	+ Responsible (R): Who performs the task.
	+ Accountable (A): Who is ultimately accountable.
	+ Consulted (C): Who needs to be consulted.
	+ Informed (I): Who needs to be kept informed.
* ILS (Interest, Level of Influence, Support): Categorize stakeholders to tailor engagement strategies.

**4. Key Documents to Write**

* Business Requirements Document (BRD)
* Functional Requirements Document (FRD)
* Requirements Traceability Matrix (RTM)
* Use Case Specifications
* Gap Analysis Reports
* Test Plans and Scenarios
* Change Request Forms
* User Manuals and Training Guides

**5. Process to Follow for Document Sign-Off**

1. Drafting: Prepare initial document versions.
2. Internal Review: Collaborate with internal teams for feedback.
3. Stakeholder Review: Share with stakeholders for comments.
4. Incorporate Feedback: Update documents based on received feedback.
5. Formal Sign-Off: Circulate final documents for e-signature or written approval.

**6. Approvals from Clients**

* Formal Presentations: Showcase requirements and solutions.
* Approval Checklists: Align deliverables with agreed criteria.
* Official Sign-Off Forms: Use formal templates to capture client approvals.
* Meeting Minutes: Document discussions and decisions made during approval meetings.

**7. Communication Channels to Establish**

* Weekly Status Meetings: Regular updates with stakeholders.
* Project Management Tools: Jira, Confluence for collaboration.
* Email Updates: For formal communications.
* Instant Messaging: Slack, Teams for quick discussions.
* Dashboard Reporting: For real-time progress updates.

**8. Handling Change Requests**

1. Submission: Stakeholders submit change requests using a standard form.
2. Impact Analysis: Assess the impact on scope, timeline, and cost.
3. Stakeholder Review: Present analysis findings for decision-making.
4. Approval/Reject Decision: Formalize decisions through documented sign-offs.
5. Implementation: Incorporate approved changes and update relevant documentation.

**9. Updating Project Progress to Stakeholders**

* Progress Reports: Weekly or bi-weekly reports covering milestones, issues, and risks.
* Burndown Charts: Visual representation of work progress.
* Steering Committee Meetings: For strategic updates.
* Stakeholder Dashboards: Real-time access to key performance indicators (KPIs).

**10. Taking Sign-Off on UAT**

* UAT Planning: Define test cases and success criteria with stakeholders.
* UAT Execution: Support users in executing test cases and documenting results.
* Defect Resolution: Address issues identified during testing.
* UAT Completion Report: Summarize testing outcomes.
* Client Project Acceptance Form:
	+ Client reviews and signs the final acceptance form, indicating project deliverables meet business needs and are ready for deployment.

**Document 3 – Functional Specification**

|  |  |
| --- | --- |
| **Project Name** | Login Module Enhancement – uPoint Healthcare Enrollment |
| **Customer Name** | KeyBank |
| **Project Version** | 1.1 |
| **Project Sponsor** | Amit Gautam |
| **Project Manager** | Kelly Nelson |
| **Project initiation date** | 2/1/2020 |
|  |  |
|  |  |

**Functional Requirements specification**

|  |  |  |  |
| --- | --- | --- | --- |
| **Req Id** | **Req Name** | **Req description** | **Priority** |
| FR001 | Strong Password Policy | Enforce a strong password policy (8+ characters, uppercase, lowercase, numbers, special characters). | 10 |
| FR002 | Multi-Factor Authentication (MFA) | Implement MFA using OTP via email or mobile for enhanced security. | 10 |
| FR003 | Account Lockout on Multiple Failed Attempts | Lock account after 5 failed attempts for 15 minutes; notify users via email. | 10 |
| FR004 | Login-Related Security Notifications | Send security alerts for new device logins, password changes, or MFA modifications. | 10 |
| FR005 | Emergency Access for Admins | Provide admin emergency access with logging and auditing features. | 9 |
| FR006 | Login Session Timeout | Auto logout users after 30 minutes of inactivity, with a warning 5 minutes prior. | 9 |
| FR007 | CAPTCHA Verification for Suspicious Activity | Add CAPTCHA when repeated failed login attempts are detected. | 9 |
| FR008 | SSO Integration with Third-Party Vendors | Enable Single Sign-On (SSO) for seamless access to external vendor services. | 8 |
| FR009 | Self-Service Password Reset | Allow users to reset passwords | 8 |
| FR010 | Password Expiration and Rotation Policy | Force users to change passwords every 90 days with reminders 7 days before expiration. | 7 |
| FR011 | User Account Recovery Options  | Provide multiple account recovery options, including phone and security questions. | 6 |
| FR012 | Remember Me Functionality | Allow users to stay logged in on trusted devices, with expiration after 7 days. | 5 |
| FR013 | Language and Accessibility Support | Support multiple languages and accessibility features (e.g., screen readers, high-contrast modes). | 3 |
| FR014 | Last login history | Enable users to view recent login history, including location, device, and timestamp | 4 |
| FR015 | Login Audit Logs | Maintain logs of login attempts, MFA verifications, and password resets for compliance. | 8 |

**Document 4 – Requirement traceability matrix**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Req Id** | **Req Name** | **Req description** | **Design**  | **Code** | **Unit Testing** | **Component testing** | **System Testing** | **UAT** |
| FR001 | Strong Password Policy | Enforce a strong password policy (8+ characters, uppercase, lowercase, numbers, special characters). | Completed | Completed | Pending | Pending | Pending | Pending |
| FR002 | Multi-Factor Authentication (MFA) | Implement MFA using OTP via email or mobile for enhanced security. | Completed | Completed | Pending | Pending | Pending | Pending |
| FR003 | Account Lockout on Multiple Failed Attempts | Lock account after 5 failed attempts for 15 minutes; notify users via email. | Completed | Completed | Pending | Pending | Pending | Pending |
| FR004 | Login-Related Security Notifications | Send security alerts for new device logins, password changes, or MFA modifications. | Completed | Completed | Pending | Pending | Pending | Pending |
| FR005 | Emergency Access for Admins | Provide admin emergency access with logging and auditing features. | Completed | Completed | Pending | Pending | Pending | Pending |
| FR006 | Login Session Timeout | Auto logout users after 30 minutes of inactivity, with a warning 5 minutes prior. | Completed | Completed | Pending | Pending | Pending | Pending |
| FR007 | CAPTCHA Verification for Suspicious Activity | Add CAPTCHA when repeated failed login attempts are detected. | Completed | In progress | Pending | Pending | Pending | Pending |
| FR008 | SSO Integration with Third-Party Vendors | Enable Single Sign-On (SSO) for seamless access to external vendor services. | Completed | In progress | Pending | Pending | Pending | Pending |
| FR009 | Self-Service Password Reset | Allow users to reset passwords | Completed | In progress | Pending | Pending | Pending | Pending |
| FR010 | Password Expiration and Rotation Policy | Force users to change passwords every 90 days with reminders 7 days before expiration. | Completed | In progress | Pending | Pending | Pending | Pending |
| FR011 | User Account Recovery Options  | Provide multiple account recovery options, including phone and security questions. | Completed | In progress | Pending | Pending | Pending | Pending |
| FR012 | Remember Me Functionality | Allow users to stay logged in on trusted devices, with expiration after 7 days. | Completed | In progress | Pending | Pending | Pending | Pending |
| FR013 | Language and Accessibility Support | Support multiple languages and accessibility features (e.g., screen readers, high-contrast modes). | Completed | In progress | Pending | Pending | Pending | Pending |
| FR014 | Last login history | Enable users to view recent login history, including location, device, and timestamp | Completed | In progress | Pending | Pending | Pending | Pending |
| FR015 | Login Audit Logs | Maintain logs of login attempts, MFA verifications, and password resets for compliance. | Completed | In progress | Pending | Pending | Pending | Pending |

**Document 5 – BRD template**

1. **Document Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| 1 | 2/19/2025 | Initial draft | Anjali Mehta |
| 1.1 | 2/19/2025 | Updated based on feedback | Anjali Mehta |

1. **Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Signature | Date |
| Mary langley | Project Sponsor |   | 2/19/2025 |
| Kelly Nelson | Project Manager |   | 2/19/2025 |
| Anjali Mehta | Business Analyst |   | 2/19/2025 |

1. **RACI Chart for This Document**

Codes Used in RACI Chart

R: Responsible

A: Accountable

C: Consulted

 I: Informed

|  |  |  |  |
| --- | --- | --- | --- |
| **R/A/C/I** | **Name of the person** | **Designation** | **Company** |
| Responsible | Amit Gautam | Delivery head  | Wipro |
| Kelly Nelson | Project Manager | Wipro |
| Karthikeyan G | Developer | Wipro |
| Maheshwaran VK | Network admin | Wipro |
| Prashant dhantakode | DB admin | Wipro |
| Avneet Kaur | Tester | Wipro |
| Deepanshu Kochar | Tester | Wipro |
| Anjali Mehta | BA | Wipro |
| Accountable | Katherine jes | Client | Alight |
| Daniel hogle | Financial head | Alight |
| Consulted | John A | Stakeholders | End users |
| John B | Stakeholders | End users |
| John C | Stakeholders | End users |
| Informed | Keybank end users |   | End users |

1. **Introduction**

**4.1. Business Goals**

To enhance the login module of the healthcare enrollment system by adding robust security features such as strong password policies, multi-factor authentication (MFA), and session management to ensure data security and compliance with healthcare regulations.

**4.2. Business Objectives**

* Strengthen user authentication processes.
* Minimize unauthorized access risks.
* Ensure seamless user experience during login and recovery processes.
* Achieve compliance with HIPAA and ACA regulations.

**4.3. Business Rules**

* Passwords must contain at least 8 characters, including uppercase, lowercase, numbers, and special characters.
* MFA must be enabled for all users.
* Accounts will lock after 5 unsuccessful login attempts.

**4.4. Background**

The existing login module lacks critical security features such as MFA and advanced password policies, posing potential risks to sensitive healthcare data. Enhancements will address these gaps.

**4.5. Project Objective**

Implement secure login enhancements, including:

* Strong password policy enforcement.
* Multi-factor authentication.
* Login session timeout.
* SSO integration with third-party vendors.

**4.6. Project Scope**

**4.6.1. In Scope Functionality**

* Password policy updates.
* MFA implementation.
* Account lockout on failed attempts.
* Security notifications and audit logs.

**4.6.2. Out Scope Functionality**

* Changes to existing user interface outside the login module.
* Third-party vendor portal updates.
1. **Assumptions**
* Users have access to devices for OTP-based MFA.
* All stakeholders are available for regular feedback sessions.
* Current system architecture supports SSO and MFA integrations.
1. **Constraints**
* Must comply with HIPAA and ACA guidelines.
* Limited budget and resources for extensive UI redesign.
* Project timeline restricted to [Project Timeline].
	1. **Risks**

**Technological Risks**

* Potential integration issues with third-party MFA providers.

**Skills Risks**

* Limited expertise in SSO configuration among current team members.

**Political Risks**

* Possible resistance from stakeholders preferring legacy systems.

**Business Risks**

* Delays in deployment could affect the annual enrollment timeline.

**Requirements Risks**

* Changing compliance requirements during project execution.

**Other Risks**

* User resistance to new security measures due to increased complexity.
1. **Business Process Overview**

**8.1. Legacy System (AS-IS)**

* Simple login without MFA.
* Basic password policy (minimum 6 characters).
* No session timeout or account lockout features.

**8.2. Proposed Recommendations (TO-BE)**

* Enforced strong password policies.
* MFA using OTP via email or SMS.
* Session timeout after 30 minutes of inactivity.
* Detailed audit logs for login-related activities.
1. **Business Requirements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Req ID** | **Requirement Name** | **Description** | **Priority** |
| BR001 | Strong Password Policy | Enforce passwords with at least 8 characters, including uppercase, lowercase, numbers, and special characters to enhance account security. | 10 |
| BR002 | Multi-Factor Authentication (MFA) | Implement MFA using OTP sent via email or mobile to provide additional security for user accounts. | 10 |
| BR003 | Account Lockout on Failed Attempts | Lock the account after 5 consecutive failed login attempts for 15 minutes; send email notifications to the user. | 9 |
| BR004 | Login Security Notifications | Send real-time security alerts for activities such as new device logins, password changes, or MFA updates. | 8 |
| BR005 | Emergency Admin Access | Provide emergency access to admin users, ensuring all actions are logged for auditing purposes. | 8 |
| BR006 | Login Session Timeout | Automatically log out users after 30 minutes of inactivity, providing a 5-minute warning before termination. | 9 |
| BR007 | CAPTCHA for Suspicious Activity | Integrate CAPTCHA for additional verification when suspicious activities, such as repeated failed logins, are detected. | 7 |
| BR008 | SSO Integration | Enable Single Sign-On (SSO) for streamlined access to third-party vendor platforms, ensuring secure token-based authentication. | 8 |
| BR009 | Self-Service Password Reset | Allow users to securely reset their passwords through email verification and security questions. | 9 |
| BR010 | Password Expiration & Rotation Policy | Enforce password changes every 90 days with automated reminders 7 days before expiration. | 7 |
| BR011 | User Account Recovery Options | Provide multiple recovery options including phone-based OTP and security questions to regain account access. | 8 |
| BR012 | Remember Me Functionality | Allow users to stay logged in on trusted devices with an automatic logout after 7 days for enhanced convenience. | 6 |
| BR013 | Accessibility & Language Support | Ensure the login page supports multiple languages and accessibility features like screen readers and high-contrast display modes. | 6 |
| BR014 | Last Login History | Display the user's recent login history, including location, device used, and timestamp, on the user dashboard. | 5 |
| BR015 | Login Audit Logs | Maintain detailed audit logs of all login attempts, MFA verifications, and password reset activities for compliance and forensic analysis. | 10 |

**10. Appendices**

**10.1. List of Acronyms**

* MFA: Multi-Factor Authentication
* OTP: One-Time Password
* SSO: Single Sign-On
* HIPAA: Health Insurance Portability and Accountability Act
* ACA: Affordable Care Act

**10.2. Glossary of Terms**

* Multi-Factor Authentication (MFA): A security process that requires multiple methods of authentication.
* SSO (Single Sign-On): A session and user authentication process that permits a user to access multiple applications with one set of login credentials.

**10.3. Related Documents**

* Healthcare Enrollment System - AS-IS Architecture Document
* Security Compliance Guidelines - HIPAA and ACA
* Risk Management Plan for Login Module Enhancements