**MySafety - Business Requirements Document (BRD) Scope - Final (Compliance Focused, with Integrations and DB Structure)**

* Version 1.3
* 15/May/2025
* Shyam Velumani

**1. Introduction**

**1.1 Purpose of this Document**

This document provides a detailed scope of the MySafety software application, breaking down the requirements to a micro level suitable for a development team. It outlines the specific functional and non-functional requirements for the initial phase of development, serving as a guide for design, implementation, and testing. This version includes requirements for a Super Admin panel to manage the SaaS aspects of the application, defines the initial technology stack, places a strong emphasis on data points and requirements critical for achieving HIPAA, GDPR, and SOC 2 compliance, includes a dedicated section on the Safety Score Algorithm definition, details the database structure by microservice, and incorporates the use of Vimeo for video services and a detailed model for image storage using AWS S3.

**1.2 Scope of the MySafety Application**

MySafety will be delivered as a SaaS application with mobile applications for Safety Officers, Supervisors, Subcontractors, and Employees, along with a web-based administration dashboard for Safety Officers and a Super Admin panel for platform management. The system will integrate with existing construction management software, such as Procore, via API for data synchronization and with a payment gateway (Stripe) for customer billing. All video content for the platform will be hosted and managed via Vimeo. Image content (photos and documents) will be stored and managed using AWS S3. The detailed scope in this document covers the specific behaviors, data points, and interactions required for the defined modules and features, including the Super Admin functionalities, the planned technology stack, critical considerations for data privacy, security, and compliance with HIPAA, GDPR, and SOC 2, the definition of the safety score algorithm, the recommended database structure, and the integration with Vimeo for video services and AWS S3 for image storage.

**1.3 Target Audience**

This document is primarily intended for the development team, quality assurance team, and technical project managers involved in building the MySafety application.

**1.4 Document Conventions**

* "Must" indicates a mandatory requirement.
* "Should" indicates a highly desirable requirement.
* "May" indicates an optional requirement.
* User stories are included to illustrate requirements from a user perspective.
* [COMPLIANCE CRITICAL] highlights data points or requirements with significant implications for HIPAA, GDPR, or SOC 2 compliance.

**2. Business Context**

**2.1 Background**

The construction industry faces significant challenges in maintaining high safety standards across multiple sites with diverse workforces, including subcontractors. Managing safety parallelly across these sites, ensuring compliance, tracking training, and responding to hazards and incidents efficiently are complex tasks often hindered by manual processes and fragmented information. MySafety is being developed as a SaaS solution to address these challenges by providing a centralized, digital platform for comprehensive safety management accessible to multiple construction companies on a subscription basis. Given the nature of safety management, the system will handle sensitive information, including personal data and potentially health-related information, necessitating strict adherence to data privacy and security regulations like HIPAA and GDPR, and aiming for SOC 2 certification to demonstrate robust controls. The platform will leverage Vimeo for secure and efficient video hosting and streaming across all modules requiring video content, and AWS S3 for secure and scalable storage of image and document files.

**2.2 Business Goals**

* Reduce workplace incidents and accidents across all managed sites for all customer organizations.
* Improve compliance with safety regulations and company policies among all personnel, including subcontractors' employees, for all customer organizations.
* Increase the efficiency and effectiveness of safety officers and site supervisors in monitoring and managing safety.
* Provide transparent and trackable safety performance data for individuals, teams, subcontractors, and sites within each customer organization.
* Enhance employee engagement with safety protocols and training through gamification and ease of access.
* Establish a scalable and manageable SaaS platform for delivering safety management services to multiple construction companies.
* Enable seamless customer onboarding, license management, and billing through a Super Admin panel and integrated payment gateway.
* Ensure the highest standards of data privacy and security to comply with HIPAA, GDPR, and meet the requirements for SOC 2 certification.
* Utilize Vimeo for reliable and secure video hosting and streaming.
* Utilize AWS S3 for secure and scalable image and document storage.

**2.3 Stakeholders**

* Super Admins (Platform Administrators)
* Safety Officers (Customer Administrators)
* Site Supervisors
* Subcontractors
* Construction Company Employees
* Clients (of the construction companies)
* IT Department (of customer companies and MySafety provider)
* Regulatory Bodies (e.g., OSHA, GDPR supervisory authorities, HIPAA enforcement agencies)
* Auditors (for SOC 2 certification)

**2.4 Operational Context**

MySafety will be used by multiple construction companies as a subscription service. Each company will manage its own sites, users, and safety data within their isolated instance or tenant of the application. The Super Admin panel will manage the platform itself, including customer accounts, licensing, billing, and shared resources. The software needs to support a distributed workforce operating on different sites and with varying levels of technical access and roles within each customer organization. The system must facilitate communication and action regarding safety matters within each customer's hierarchy. All data handling processes must be designed and implemented to comply with HIPAA (where Protected Health Information - PHI - is involved), GDPR (for personal data of EU citizens), and SOC 2 security, availability, processing integrity, confidentiality, and privacy principles. Video content, including training videos and videos attached to reports/incidents, will be managed through Vimeo. Image and document content, such as photos attached to hazard reports, inspections, and incidents, will be stored and managed in AWS S3.

**3. Functional Requirements**

**3.1 User Roles and Access**

* Super Admin (Web Panel):
  + Must have full administrative control over the MySafety platform, managing customer accounts, licenses, billing, and system-wide configurations.
  + Must be able to manage common pools of content (e.g., checklists, training videos hosted on Vimeo, documents stored on S3) accessible to all customers.
  + Must be able to configure subscription plans and access levels.
  + Must have access to system-wide monitoring and analytics (non-customer-specific operational data).
  + [COMPLIANCE CRITICAL] Must have granular, auditable access to customer data only for support and platform management purposes, with strict controls and logging. Access to sensitive data (PHI, personal data, sensitive images/documents) must be restricted and require justification.
  + Must be able to manage Vimeo API integration settings.
  + Must be able to manage AWS S3 configuration settings related to MySafety's storage.
* Safety Officer (Web Dashboard & Mobile App):
  + Full administrative control within their specific customer organization's account, managing sites, users, subcontractors, modules, rules, and reporting for that organization.
  + Ability to perform user-level actions via the mobile app (hazard reporting, inspections, viewing tickets/permits, including viewing videos hosted on Vimeo and images/documents stored on S3).
  + Ability to upload videos for organization-specific use (e.g., in notifications), which will be uploaded to Vimeo via the MySafety platform.
  + Ability to upload images and documents for organization-specific use (e.g., in notifications, reference materials), which will be uploaded to AWS S3 via the MySafety platform.
  + [COMPLIANCE CRITICAL] Access to sensitive data (e.g., detailed incident reports with injury information, training records, potentially wearable data) must be role-based and limited to authorized personnel within their organization. Access to videos and images/documents linked to sensitive data (e.g., incident videos/photos) must also be restricted.
* Supervisor (Web Login & Mobile App):
  + Access limited to assigned sites within their customer organization.
  + Ability to perform site-level safety tasks (hazard reporting, inspections, permit requests, viewing relevant tickets/permits, including viewing videos hosted on Vimeo and images/documents stored on S3).
  + Ability to upload videos for hazard reports and inspections, which will be uploaded to Vimeo via the MySafety platform.
  + Ability to upload photos and documents for hazard reports and inspections, which will be uploaded to AWS S3 via the MySafety platform.
  + [COMPLIANCE CRITICAL] Access to sensitive data must be restricted to information necessary for their role and assigned sites. Access to videos and images/documents linked to sensitive data must also be restricted.
* Subcontractor (Mobile App):
  + Access limited to their own teams and relevant site information within their customer organization.
  + Ability to manage their employees, respond to assigned hazard tickets, view relevant permits, and track team training progress (including viewing training videos hosted on Vimeo and documents stored on S3).
  + Ability to upload videos for hazard reports and inspections, which will be uploaded to Vimeo via the MySafety platform.
  + Ability to upload photos and documents for hazard reports and inspections, which will be uploaded to AWS S3 via the MySafety platform.
  + [COMPLIANCE CRITICAL] Access to employee data must be limited to their own employees and relevant safety performance metrics. Access to videos and images/documents linked to sensitive data must also be restricted.
* Employee (Mobile App & Kiosk Mode):
  + Access to personal training modules (LMS, including viewing training videos hosted on Vimeo and documents stored on S3), individual safety scores, coupons/incentives, and incident reporting within their customer organization.
  + Ability to upload videos for incident reports, which will be uploaded to Vimeo via the MySafety platform.
  + Ability to upload photos and documents for incident reports, which will be uploaded to AWS S3 via the MySafety platform.
  + [COMPLIANCE CRITICAL] Must have secure access to their own personal safety data and records. Should have the ability to request access to, rectification of, or erasure of their personal data as per GDPR requirements. Access to videos and images/documents linked to their reports must be secure.

**3.2 Module Requirements**

**3.2.1 Hazard Reporting Module**

* User Story (Supervisor): As a supervisor, I want to quickly report a hazard I observe on site using my mobile app, including photos and location, so that it can be addressed promptly.
* Create Hazard Report:
  + Data Fields: Hazard Title, Description (text), Location (Site, specific area/description, GPS coordinates - auto-capture if possible), Date/Time (auto-capture), Reported By (User, Role), Severity Level (Dropdown: Low, Medium, High, Critical - configurable by Safety Officer), Hazard Type (Dropdown: e.g., Fall Risk, Electrical, Equipment, Environmental - configurable by Safety Officer, potentially selectable from a Super Admin managed common pool), Recommended Action (text - optional).
  + Media: Must allow attaching multiple photos and videos. Photos and documents must be uploaded to AWS S3 via the MySafety platform. The system must store the S3 object key or URL. Videos must be uploaded to Vimeo via the MySafety platform. The system must store the Vimeo video ID or URL. [COMPLIANCE CRITICAL] Media containing identifiable individuals or sensitive information must be handled securely on S3 and Vimeo with appropriate privacy settings, and access controlled within MySafety.
  + Assignment: Must allow assigning as a ticket to one or more specific subcontractors or all subcontractors on the site. Additionally, the user must be able to assign the ticket to a specific team or individual person from a dropdown list populated with relevant teams and users for that site/subcontractor within their organization.
  + Notifications: Must trigger immediate notification to assigned subcontractors, teams, persons, and relevant Safety Officers/Supervisors within the same customer organization. [COMPLIANCE CRITICAL] Notifications should not contain excessive sensitive information.
* Hazard Ticket Management:
  + Ticket View: Assigned subcontractors, teams, and individuals must see a list of tickets assigned to them within their organization. Safety Officers/Supervisors must see tickets for their sites/oversight area within their organization.
  + Ticket Details: Must display all hazard report details, assignment information (including assigned team/person), and a history of actions/comments. Must embed or link to videos hosted on Vimeo and images/documents stored on S3. [COMPLIANCE CRITICAL] Access to ticket details and associated media must be restricted based on user role and assignment.
  + Actions: Assigned parties (subcontractors, teams, individuals) must be able to add comments, update status (e.g., In Progress, Resolved), and mark as Complete.
  + Re-open: Safety Officers must be able to re-open a completed ticket with comments if the resolution is unsatisfactory.
* Hazard Report Review (Web Dashboard): Safety Officers must have a dashboard view of all open, in-progress, and closed hazard reports for their organization, with filtering and sorting options.

**3.2.2 Onboarding Training (LMS) Module**

* User Story (Employee): As a new employee, I want to easily access and complete my required onboarding safety training on my phone, and see my progress.
* Course Management (Web Dashboard - Safety Officer): Safety Officers must be able to create, edit, and manage onboarding training courses specific to their organization.
  + Must be able to select content (videos hosted on Vimeo, documents stored on S3, etc.) from a Super Admin managed common pool or upload organization-specific content (videos uploaded to Vimeo via MySafety, documents uploaded to S3 via MySafety).
  + Support for multi-lingual content (text, videos, presentations).
  + Ability to structure courses into learning paths.
  + Integration of multi-choice questions for assessments.
  + Must allow setting passing scores for assessments.
  + Must allow assigning courses to specific roles, sites, or subcontractors within their organization.
  + Must support assigning languages to users/sites.
* Course Management (Web Panel - Super Admin): Super Admins must be able to manage a common pool of training content (e.g., generic safety videos) hosted on Vimeo that can be made available to customer organizations based on their subscription plan.
  + Ability to upload, categorize, and manage training resources (videos uploaded to Vimeo via MySafety) in multiple languages.
* Employee Training Access (Mobile App/Kiosk): Employees must be able to access and complete assigned onboarding training courses for their organization, including viewing videos hosted on Vimeo.
  + Gamified elements (points, progress tracking, badges).
  + Ability to take assessments and receive immediate feedback.
* Training Tracking and Reporting:
  + Must track completion date and status for each module and course per employee within their organization.
  + Must store assessment scores and pass/fail status.
  + Must generate certificates of completion (digital).
  + Safety Officers must provide reports on training completion rates for their organization (overall, by site, by subcontractor, by course).
  + Must send automated notifications to subcontractor supervisors/managers for employees with overdue or incomplete training within their organization.
  + Must maintain a historical record of all training completed by each employee within their organization.

**3.2.3 Compliance Training Module**

* User Story (Subcontractor Manager): I need to see which of my employees have completed their required compliance training so I can ensure my team is compliant.
* Functionality: Similar to Onboarding Training, but specifically for recurring compliance requirements (e.g., Fall Protection Refresher, First Aid Certification) within each customer organization, including access to videos hosted on Vimeo and documents stored on S3.
* Assignment: Must allow assigning training based on roles, sites, and regulatory requirements with expiry dates.
* Automated Reminders: Must send automated reminders to employees and their supervisors/subcontractor managers within their organization before certifications expire or refresher training is due.
* Reporting: Safety Officers must provide detailed reports on compliance training status for their organization, including upcoming expirations.

**3.2.4 Inspection Checklist Module**

* User Story (Safety Officer): I need to create a specific checklist for inspecting scaffolding and ensure supervisors on relevant sites use it.
* Checklist Management (Web Dashboard - Safety Officer): Safety Officers must be able to create, edit, and manage inspection checklists specific to their organization.
  + Must be able to select checklist templates from a Super Admin managed common pool or create organization-specific templates.
  + Must support different item response types (e.g., Yes/No/N/A, Pass/Fail, Rating scale 1-5, Text input, Photo attachment).
  + Must allow attaching reference documents or images (stored on S3) to individual checklist items.
  + Must allow assigning checklists to specific sites, equipment types, or inspection types (e.g., Daily Pre-Task, Weekly Site, Equipment) within their organization.
* Checklist Management (Web Panel - Super Admin): Super Admins must be able to manage a common pool of checklist templates that can be made available to customer organizations based on their subscription plan.
  + Ability to create, categorize, and manage standard checklist templates.
* Inspection Execution (Mobile App): Supervisors must be able to conduct inspections using assigned checklists on their mobile devices for their organization's sites.
  + Ability to record responses, add comments, and attach photos and videos for individual checklist items. Photos and documents must be uploaded to AWS S3 via the MySafety platform. The system must store the S3 object key or URL. Videos must be uploaded to Vimeo via the MySafety platform. The system must store the Vimeo video ID or URL. [COMPLIANCE CRITICAL] Media containing identifiable individuals or sensitive information must be handled securely on S3 and Vimeo with appropriate privacy settings, and access controlled within MySafety.
  + Must support offline data capture with automatic synchronization when connectivity is restored.
  + Must capture date, time, and inspector details (auto-capture).
  + Must capture location details (site, specific area - text/dropdown, GPS - auto-capture if possible).
* Inspection Reporting:
  + Must instantly compile completed inspection data into a report format within the customer organization's account.
  + Must store digital copies of completed inspection reports, including links/embeds for videos hosted on Vimeo and images/documents stored on S3.
  + Safety Officer Dashboard: Safety Officers must display a summary view of recent inspections for their organization with a color-coded status (Green = Fully Compliant, Yellow = Minor Issues, Red = Major Issues/Non-Compliant) based on checklist responses and predefined rules.
  + Must allow drilling down from the summary to view the full inspection report, including viewing associated media.
  + Should allow assigning corrective actions directly from failed checklist items.

**3.2.5 Permits Briefcase Module**

* User Story (Subcontractor): I need to request a hot work permit for my team to perform welding in a specific area tomorrow.
* Permit Request (Mobile App): Supervisors and Subcontractors must be able to initiate a permit request for their organization's sites, providing necessary details and attachments (including potential videos uploaded to Vimeo and documents/images uploaded to S3). [COMPLIANCE CRITICAL] Personal information included in permit requests must be handled securely.
* Permit Review and Approval (Web Dashboard): Safety Officers must be able to review permit requests for their organization, add comments, and approve or reject them, including viewing any attached videos hosted on Vimeo and images/documents stored on S3. [COMPLIANCE CRITICAL] Access to permit requests and associated media must be restricted to authorized approvers.
* Permit Briefcase (Mobile App): Users must be able to view their active and past permits relevant to their work within their organization, including viewing any attached videos hosted on Vimeo and images/documents stored on S3. [COMPLIANCE CRITICAL] Access to permit details and associated media must be restricted to relevant users.
* Permit Tracking and Notifications: The system must track permit status and send notifications within the organization upon approval or rejection.
* Permit Type Management (Web Dashboard - Safety Officer): Safety Officers must be able to configure permit types specific to their organization.

**3.2.6 Incident Reporting Module**

* User Story (Employee): I was involved in a minor incident and need to report it quickly from my phone.
* Detailed Incident Report Creation (Mobile App): Users must be able to create a detailed incident report for their organization, including:
  + Date, time, and location of the incident.
  + Type of Incident (Dropdown - configurable by Safety Officer).
  + Description of Incident (text), Sequence of Events (text).
  + Involved Parties (List: Employees - link to user profiles within organization, Subcontractors, Equipment). [COMPLIANCE CRITICAL] Linking to user profiles must respect privacy.
  + Injury Details (if applicable: Type of Injury, Body Part, Severity, First Aid/Medical Treatment). [COMPLIANCE CRITICAL] This is Protected Health Information (PHI) under HIPAA. Must be handled with the highest level of security and access control.
  + Property Damage Details (if applicable).
  + Witness Information (Name, Contact - optional fields). [COMPLIANCE CRITICAL] Witness contact information must be handled securely.
  + Contributing Factors (text/dropdown - optional, configurable by Safety Officer).
  + Initial Actions Taken (text).
  + Environmental Conditions (text/dropdown - optional).
  + Must allow attaching photos and videos. Photos and documents must be uploaded to AWS S3 via the MySafety platform. The system must store the S3 object key or URL. Videos must be uploaded to Vimeo via the MySafety platform. The system must store the Vimeo video ID or URL. [COMPLIANCE CRITICAL] Media containing identifiable individuals or sensitive information must be handled securely on S3 and Vimeo with appropriate privacy settings, and access controlled within MySafety.
* Incident Management (Web Dashboard): Safety Officers must be able to review, investigate, add findings, root cause analysis details, identify and assign Corrective Actions, and close incident reports for their organization, including viewing associated media hosted on Vimeo and S3. [COMPLIANCE CRITICAL] Access to incident reports, especially those containing PHI and associated media, must be strictly controlled and auditable.
* Incident Reporting and Analysis: Safety Officers must provide reports and analytics on incident trends within their organization. [COMPLIANCE CRITICAL] Reports containing PHI and/or links to media with sensitive content must be restricted to authorized personnel. Aggregated or anonymized data should be used for broader analysis where possible.

**3.2.7 Gamification and Scorecard Module**

* User Story (Employee): I want to see my safety score and how I rank against my teammates to motivate me to be safer.
* Safety Score Calculation:
  + Must calculate scores based on a configurable rules engine (details of the algorithm rules and weighting are defined separately but the system must implement them) for each customer organization.
  + Rules will involve awarding points for positive actions and deducting points for negative events based on configurations set by the Safety Officer (within limits defined by Super Admin plans). [COMPLIANCE CRITICAL] If safety scores are influenced by incident data containing PHI, the calculation and display of scores must be handled carefully to avoid unauthorized disclosure of PHI.
  + Must support different scoring periods (e.g., daily, weekly, monthly, project duration).
* Score Grouping and Display:
  + Must display scores for individuals, teams (configurable grouping), subcontractors, and sites within their organization.
  + Must allow Safety Officers and Supervisors to view scores for their relevant groups within their organization.
  + Employees must only see their individual score and potentially team/site scores within their organization.
  + [COMPLIANCE CRITICAL] Display of scores must be carefully designed. Avoid displaying specific reasons for score deductions if they are linked to sensitive events (e.g., an incident with injury). Focus on categories of activities contributing to the score (e.g., "Incident Involvement" points deduction) rather than specific incident details.
* Gamification Elements:
  + Must track points earned from safety activities within their organization.
  + Must award badges for achieving milestones or specific safety actions.
  + Must display leaderboards for individuals, teams, subcontractors, and sites (with configurable ranking criteria) within their organization. [COMPLIANCE CRITICAL] Leaderboards should display names/identifiers only with user consent and should not expose sensitive performance details.
* Incentives Management (Web Dashboard - Safety Officer): Safety Officers must be able to define and manage incentives linked to gamification achievements for their organization.
* Scorecard Visibility: Must ensure data privacy by limiting visibility of detailed scores and contributing factors based on user role and customer organization. [COMPLIANCE CRITICAL] Implement granular controls over which users can see which levels of detail regarding safety scores and the factors influencing them.

**3.2.8 Help, Tutorials, and Documentation Module (Safety Officer Web Dashboard)**

* User Story (Safety Officer): As a Safety Officer, I need easy access to tutorials and documentation within the dashboard so I can quickly learn how to use different features and find answers to my questions.
* Access to Help Resources:
  + Must provide a dedicated section or prominent link within the Safety Officer web dashboard for accessing help, tutorials, and documentation.
  + Must include a searchable knowledge base or FAQ section covering common tasks and questions.
  + Must provide access to video tutorials (hosted on Vimeo) and document tutorials (stored on S3) demonstrating key functionalities (e.g., creating checklists, managing users, running reports).
  + Must link to comprehensive user documentation explaining all features and configurations.
  + Should include context-sensitive help options (e.g., tooltips, links to relevant documentation sections from specific pages).
  + Should provide access to contact information or a support ticket submission form for requesting assistance.
* Content Management (Super Admin): Super Admins must be able to manage the content of the help, tutorial, and documentation resources.
  + Must be able to upload, organize, and update documentation files (uploaded to S3 via MySafety), video tutorials (uploaded to Vimeo via MySafety), and FAQ content.
  + Must be able to categorize help content for easy navigation by Safety Officers.
  + Must support multi-lingual help content.

**3.3 Super Admin Functional Requirements (Web Panel)**

* Customer Account Management:
  + Must be able to create new customer accounts (spinning off licenses).
  + Must be able to view, edit, and manage existing customer accounts.
  + Must be able to activate, suspend, or terminate customer licenses.
  + Must be able to assign subscription plans to customer accounts.
  + Must be able to view customer usage metrics (e.g., number of active users, number of sites, data storage used).
  + [COMPLIANCE CRITICAL] Must manage customer accounts in a manner that respects data isolation and privacy.
* Subscription Plan Management:
  + Must be able to define and configure different subscription plans (e.g., Basic, Pro, Enterprise).
  + Must be able to define the features, user limits, site limits, storage limits, and access to common content pools associated with each plan. [COMPLIANCE CRITICAL] Plan features must align with compliance capabilities (e.g., higher plans may include advanced data retention or audit features).
  + Must be able to set pricing for each plan.
* Payment Gateway Integration (Stripe):
  + Must integrate with Stripe for processing customer payments (subscriptions, potentially one-time fees).
  + Must support direct customer signup and payment processing via a customer-facing portal or link managed by the Super Admin.
  + Must be able to view payment history and transaction details for each customer. [COMPLIANCE CRITICAL] Payment information must be handled according to PCI DSS standards (though not explicitly HIPAA/GDPR, it's a key compliance standard for payments).
  + Must be able to manage invoices and billing cycles.
  + Should support automated recurring billing.
* Common Content Pool Management:
  + Must be able to manage a central repository of reusable content (e.g., standard checklist templates, generic safety training videos hosted on Vimeo, regulatory documents stored on S3).
  + Must be able to categorize and tag content for easy searching and filtering by customer Safety Officers.
  + Must be able to control which content pools are available to specific subscription plans.
  + Must be able to update and version common content.
* System-Wide Configuration:
  + Must be able to configure global application settings (e.g., default language settings, notification system parameters).
  + Must be able to manage integrations with third-party services (e.g., Procore API credentials for the platform). [COMPLIANCE CRITICAL] Integration configurations must include security parameters and data mapping details relevant to compliance.
* System Monitoring and Analytics:
  + Must provide dashboards and reports on overall platform health, performance, and usage across all customers.
  + Must be able to monitor system errors and logs. [COMPLIANCE CRITICAL] System logs must be securely stored and include details relevant for audit trails (SOC 2). Access to logs containing sensitive data must be restricted.
  + Must provide analytics on feature adoption rates and user engagement across the platform (aggregated and anonymized where necessary for privacy). [COMPLIANCE CRITICAL] Aggregated data must be sufficiently anonymized to prevent re-identification.
* Customer Support Tools:
  + Should have tools to impersonate customer Safety Officers (with strict access control and logging) for troubleshooting and support purposes. [COMPLIANCE CRITICAL] Impersonation actions must be logged extensively and auditable. Access to sensitive customer data during support must be limited and justified.
  + Should have access to customer-specific logs and error reports. [COMPLIANCE CRITICAL] Access to logs containing sensitive data must be restricted and auditable.
* User Management (Platform Level):
  + Must be able to manage Super Admin user accounts and permissions. [COMPLIANCE CRITICAL] Super Admin permissions must be granular and follow the principle of least privilege.
  + Should be able to manage platform-level user roles beyond Super Admin if needed for internal staff.
* Vimeo API Integration Management:
  + User Story (Super Admin): As a Super Admin, I need to configure and manage the integration with the Vimeo API to ensure video content is uploaded and streamed correctly across the platform.
  + Must provide a dedicated section in the Super Admin panel for Vimeo API configuration.
  + Must allow Super Admins to input and update Vimeo API credentials (e.g., Access Token). [COMPLIANCE CRITICAL] API credentials must be stored securely and encrypted.
  + Must allow configuring default Vimeo settings for video uploads (e.g., privacy settings, folder structure).
  + Must provide a mechanism to test the Vimeo API connection.
  + Should display Vimeo account usage metrics (e.g., storage used, bandwidth) if available via the API.
  + Must log all changes made to Vimeo API integration settings. [COMPLIANCE CRITICAL]
* AWS S3 Configuration Management:
  + User Story (Super Admin): As a Super Admin, I need to configure and manage the AWS S3 settings used by MySafety for image and document storage to ensure data is stored securely and efficiently.
  + Must provide a dedicated section in the Super Admin panel for AWS S3 configuration.
  + Must allow Super Admins to input and update necessary AWS credentials (e.g., Access Key ID, Secret Access Key) or configure IAM roles for secure access. [COMPLIANCE CRITICAL] AWS credentials must be stored securely and encrypted. IAM roles are preferred for enhanced security.
  + Must allow configuring the target S3 bucket name(s).
  + Must allow configuring default S3 settings for file uploads (e.g., server-side encryption settings - SSE-S3 or KMS, access control policies).
  + Must provide a mechanism to test the AWS S3 connection and permissions.
  + Should display S3 storage usage metrics if available via AWS APIs.
  + Must log all changes made to AWS S3 configuration settings. [COMPLIANCE CRITICAL]

**4. Safety Score Algorithm Definition**

**4.1 Introduction: Defining the Purpose and Importance of a Rules-Based Safety Score in the Construction Industry**

The construction industry, while vital to infrastructure and economic development, inherently involves numerous high-risk activities, leading to a concerningly high incidence of accidents, injuries, and even fatalities.[1, 2, 3, 4, 5] Despite the implementation of various safety training programs and regulatory measures, the sector continues to grapple with these challenges, indicating a need for more dynamic and effective approaches to bolster worker safety.[1] Traditional methods often fall short in providing a comprehensive and real-time assessment of safety performance, hindering the ability of organizations to proactively identify and mitigate potential hazards.

In response to this persistent need, the introduction of a rules-based safety score module presents a promising avenue for enhancing safety management within the construction industry. This module is envisioned as a system that objectively evaluates safety performance based on a predefined set of criteria and data inputs. By establishing a clear and consistent framework for assessing safety, this tool can serve as a valuable asset for construction organizations committed to fostering a safer working environment.

The primary objectives of implementing a safety score are multifaceted. Firstly, it aims to aid in the identification of specific hazards and unsafe practices prevalent on construction sites. By analyzing relevant data through a structured algorithm, the safety score can pinpoint areas where risks are elevated, allowing for targeted interventions. Secondly, the score is designed to promote safer behaviors among workers and other stakeholders by providing feedback on their safety-related actions and potentially incentivizing adherence to best practices. Furthermore, the safety score can serve as a benchmark for comparing safety performance across different projects, teams, or subcontractors within an organization, facilitating the identification of high-performing units and areas requiring improvement. Ultimately, the overarching goal is to contribute to a reduction in the number of incidents, injuries, and associated costs within the construction industry by fostering a culture of continuous safety improvement.

The implementation of a rules-based safety score aligns with the growing recognition of the benefits of a proactive approach to safety management.[6, 7, 8] Traditional safety measures often tend to be reactive, with actions being taken primarily after an incident has occurred. In contrast, a safety score system can encourage a shift towards prevention. By focusing on leading indicators and rewarding proactive safety measures, organizations can move beyond simply responding to past failures and instead work towards creating an environment where hazards are identified and mitigated before they can cause harm. This proactive stance is not only more effective in protecting workers but can also lead to significant long-term benefits for construction companies, including reduced costs associated with accidents and improved overall project efficiency.

**4.2 Core Principles of a Rule-Based Safety Score Algorithm: Explaining the Fundamental Components and Design Considerations**

The development of a robust and effective rules-based safety score algorithm for the construction industry necessitates careful consideration of several core principles. These principles will guide the design and implementation of the module, ensuring that it is practical, reliable, and contributes meaningfully to enhancing safety performance.

At the foundation of the algorithm lies a set of clearly defined rules.[9, 10] These rules must be specific, measurable, achievable, relevant, and time-bound (SMART) to ensure clarity and facilitate objective assessment. The rules should be meticulously derived from a combination of industry best practices, regulatory requirements mandated by bodies such as OSHA [6, 11, 12, 13, 14, 15, 16, 17, 18, 19], and the specific safety policies and procedures established by the construction organization itself. This comprehensive approach will ensure that the algorithm addresses a wide range of critical safety aspects relevant to the construction environment.

The efficacy of the rules will depend heavily on the quality and relevance of the data inputs.[9, 10, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38] The algorithm should be designed to operate on a diverse array of data, encompassing both lagging indicators that reflect past safety performance and leading indicators that provide insights into proactive safety measures. Furthermore, the potential integration of real-time data streams from wearable technology presents a significant opportunity to enhance the responsiveness and accuracy of the safety score. The selection of specific data inputs must be carefully aligned with the defined rules and the overarching objectives of the safety score module, ensuring that the algorithm analyzes information that is directly pertinent to assessing safety performance.

A well-defined scoring logic is essential for translating the data inputs into a meaningful numerical score.[39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54] This methodology should clearly outline how the rules are applied to the data and how the resulting score is calculated. A crucial aspect of the scoring logic involves the assignment of weights to different rules based on their relative importance in ensuring overall safety.[39, 41] For instance, rules pertaining to critical hazards or high-risk activities could be assigned a greater weight than those related to less severe risks. Additionally, the scoring logic should be carefully designed to incentivize desired safety behaviors and actively disincentivize unsafe practices, thereby promoting a culture of safety consciousness among users.

The utility of the safety score will be maximized through the establishment of clear guidelines for score interpretation.[39, 40, 41, 43, 52] These guidelines should define distinct risk levels or performance categories associated with different score ranges, enabling users to readily understand their safety performance standing. The interpretation should be actionable, providing users with specific insights into areas where they excel and areas that require attention and improvement.

Finally, transparency is a paramount principle that must underpin the entire safety score algorithm.[39, 40, 41, 43, 45, 47, 50, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72] The algorithm's underlying logic, the specific rules it employs, and the various data sources it utilizes should be communicated clearly and openly to all users.[62] This transparency is essential for fostering trust in the system and encouraging users to actively engage with it to improve their safety performance. When users understand how their score is calculated and the factors that influence it, they are more likely to embrace the system and take ownership of their safety behaviors.

**4.3 Identification of Key Construction Safety Indicators:**

A comprehensive rule-based safety score algorithm for the construction industry must consider a wide range of safety indicators to provide a holistic assessment of safety performance. These indicators can be broadly categorized into lagging indicators, which reflect past safety outcomes, and leading indicators, which are proactive measures that can predict and prevent future incidents.

Lagging indicators offer valuable insights into the historical safety performance of a construction site or organization.[8, 39, 41, 44, 45, 46, 52, 54, 63, 64, 69, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106] The Total Recordable Incident Rate (TRIR) is a fundamental lagging indicator that measures the number of recordable incidents, including injuries and illnesses requiring medical treatment beyond first aid, for every 100 full-time employees over a one-year period.[8, 39, 41, 45, 54, 63, 64, 69, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 87, 97, 101, 105, 106] A higher TRIR signifies a less safe work environment, and this metric is widely used for benchmarking safety performance against industry averages.[8, 73, 106, 107] The Days Away, Restricted, or Transferred (DART) Rate is another critical lagging indicator that tracks the number of incidents per 100 full-time employees that resulted in days away from work, restricted work activity, or job transfer due to a work-related injury or illness.[8, 39, 41, 54, 63, 64, 69, 73, 74, 75, 76, 77, 78, 79, 81, 82, 83, 87, 97, 101, 105, 106] The DART rate provides insight into the severity of incidents, as it focuses on cases that lead to lost or modified workdays.[8, 73, 77, 105, 106] The Experience Modification Rating (EMR) is a crucial metric used by insurance companies to assess a company's workers' compensation claims history.[8, 15, 39, 41, 52, 54, 69, 72, 73, 74, 76, 77, 78, 79, 80, 81, 82, 83, 87, 97, 101, 102, 103, 104, 105, 106, 108, 109, 110] It reflects a company's historical claims experience and is used to calculate insurance premiums. An EMR below 1.0 is generally considered indicative of better-than-average safety performance.[74, 103, 104] Other relevant lagging indicators include the overall frequency of safety incidents, the severity of these incidents (often measured in lost workdays), the number of fatalities, and the number and severity of OSHA violations and associated penalties.[18, 39, 41, 54, 69, 72, 73, 74, 77, 79, 80, 81, 83, 87, 97, 99, 105, 108, 111, 112, 113, 114, 115, 116, 117]

Leading indicators, on the other hand, are proactive measures that can provide insights into the effectiveness of safety programs and predict potential future incidents.[8, 39, 41, 63, 64, 69, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 87, 102, 105, 118, 119, 120, 121, 122, 123] Safety Training Completion and Attendance Rates are crucial leading indicators that reflect the engagement and competency of the workforce in safety practices.[8, 39, 41, 63, 64, 69, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 87, 102, 105, 118, 119, 120, 121] Higher completion rates and consistent attendance at safety sessions indicate a greater emphasis on safety knowledge and a more safety-conscious workforce. The Near-Miss Reporting Rate is another vital leading indicator that signifies a proactive safety culture where workers are encouraged to identify and report potential hazards before they result in actual incidents.[8, 39, 41, 63, 64, 69, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 86, 87, 102, 105, 119, 120, 121, 124, 125, 126, 127, 128, 129] A higher reporting rate suggests a greater awareness of potential hazards and a willingness among employees to communicate safety concerns. The frequency and scores of Safety Audits are also crucial leading indicators.[8, 39, 41, 63, 64, 69, 73, 74, 75, 76, 77, 79, 80, 81, 82, 83, 87, 102, 105, 119, 120, 121] Regular audits with high scores indicate a strong commitment to safety and compliance. Other important leading indicators include the frequency and quality of hazard identification and risk assessment activities, the effectiveness of safety communication strategies, and the frequency and quality of safety observations conducted on the job site.

**4.4 Defining the Rule Set and Scoring Logic:**

To construct a meaningful and effective safety score, a well-defined set of rules must be established, categorized by key safety domains relevant to the construction industry. These rules will form the basis of the algorithm and will dictate how the safety score is calculated based on the data inputs.

One critical safety domain is Training and Competency.[4, 6, 11, 12, 13, 15, 18, 43, 46, 73, 74, 76, 79, 86, 112, 117, 118, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150] Rules within this category should focus on the completion of mandatory safety training programs, the possession of necessary certifications for operating equipment or performing specialized tasks, and the demonstrated competency of workers to carry out their duties safely. For instance, the algorithm could award points for each safety training module completed by an employee within the required timeframe. Conversely, points could be deducted for expired certifications or for instances where workers are observed performing tasks for which they are not adequately trained or certified.

Another essential domain is Personal Protective Equipment (PPE).[1, 2, 3, 5, 6, 11, 12, 13, 14, 15, 26, 43, 46, 50, 51, 63, 73, 74, 76, 82, 83, 87, 105, 117, 130, 151, 132, 141, 143, 147, 150, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161] Rules in this category should address the proper use of required PPE, the regular inspection and maintenance of PPE, and the availability of appropriate PPE for specific tasks. For example, the algorithm could award points for documented regular inspections of PPE by designated personnel. Conversely, deductions could be applied when workers are observed not using the required PPE for a particular task or when PPE is found to be damaged or non-functional.

Job Site Inspections form a critical component of safety management. Rules in this category should incentivize the regular and thorough completion of safety inspections, the prompt identification of hazards, and the implementation of timely corrective actions. For example, the algorithm could award points for the documented completion of daily safety checklists or for the timely closure of corrective actions identified during inspections. Conversely, deductions could be applied for overdue corrective actions or for consistently incomplete or inadequate inspection reports.

Incident Reporting and Investigation is another crucial domain. Rules here should encourage the prompt and accurate reporting of all incidents, including near misses, and the conduct of thorough investigations to identify root causes and prevent recurrence. For instance, points could be awarded for reporting near misses within a specified timeframe. Conversely, deductions might be applied for unreported incidents or for investigations that are deemed incomplete or fail to identify adequate corrective actions.

Safety Meetings and Communication are vital for fostering a strong safety culture. Rules in this domain should incentivize the holding of regular safety meetings, such as toolbox talks, and the effective dissemination of safety information through various channels. For example, points could be awarded for documented attendance at weekly safety meetings or for the regular distribution of safety alerts and updates.

Finally, Hazard Control and Prevention is a fundamental category. Rules within this domain should focus on the proactive identification of hazards, the implementation of effective hazard controls (including engineering controls where feasible), and the adherence to safe work procedures. For example, points could be awarded for documented implementation of engineering controls for identified hazards or for the use of pre-task planning tools like Job Hazard Analyses (JHAs).[118]

The scoring methodology should involve awarding positive points for adherence to safety rules and engagement in proactive safety behaviors. Conversely, points should be deducted for violations of safety rules, the occurrence of incidents, and a lack of compliance with safety protocols. To accurately reflect the criticality of different safety aspects, a weighted scoring system should be considered, where rules related to critical hazards or high-risk activities carry a higher point value or penalty.

**4.5 Incorporating Advanced Safety Data:**

To enhance the sophistication and effectiveness of the safety score, the algorithm should be designed to incorporate advanced safety data beyond traditional lagging and leading indicators. This includes leveraging data from wearable technology, quantifying positive safety behaviors and hazard reporting, and effectively addressing negative events and violations.

Wearable technology offers a unique opportunity to collect objective, real-time data directly from workers and their environment.[20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 162, 163] The algorithm can be designed to ingest various data points from these devices, such as physiological data like heart rate, body temperature, and indicators of fatigue [20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 162, 163], proximity alerts that can warn workers of approaching hazards or entry into restricted zones [26, 27, 34, 35, 36, 38, 164], motion detection data that can identify falls or unsafe movements [3, 21, 24, 26, 27, 29, 31, 33, 34, 35, 36, 37, 38, 163], and environmental data such as levels of toxic gases or exposure to extreme temperatures.[31, 33, 35, 36, 37, 38, 165] For example, the algorithm could award points for workers consistently maintaining safe physiological parameters as monitored by their wearables. Conversely, it could deduct points for instances where a worker enters a restricted area without proper authorization based on proximity sensor data or trigger alerts for supervisors if a fall is detected by a wearable device.

To foster a more proactive safety culture, the algorithm should also consider positive safety behaviors and the reporting of potential hazards. Positive behaviors, such as active participation in safety initiatives and consistent adherence to safe work practices, can be quantified and incorporated into the score.[82, 142, 154, 155, 166] This could involve tracking participation in safety meetings, completion of voluntary safety training, or adherence to ergonomic guidelines observed through technology like AI-powered video analysis.[164] Furthermore, the algorithm should incentivize the timely and detailed reporting of potential hazards.[86, 119, 124, 125, 126, 127, 128, 156, 158, 167] Bonus points could be awarded for reporting a hazard that leads to a preventative action, and a leaderboard could be implemented to recognize individuals or teams with high hazard reporting rates.

Finally, the algorithm must effectively address negative events and violations. This involves assigning penalties based on the severity of incidents and violations.[16, 17, 18, 19, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 50, 52, 54, 59, 63, 64, 69, 71, 72, 73, 74, 77, 80, 89, 90, 91, 92, 93, 94, 99, 100, 102, 105, 106, 107, 113, 114, 115, 116, 117, 129, 139, 143, 150, 158, 161, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188] A risk matrix approach [158] could be utilized to categorize incidents and violations based on their potential severity (e.g., minor, moderate, serious, severe, fatality). The algorithm should also consider the frequency of similar incidents or violations, applying escalating penalties for recurring unsafe behaviors. For instance, the algorithm could deduct a higher number of points for incidents resulting in injury or lost time compared to minor first-aid cases. Similarly, repeated violations of the same safety rule within a defined period could result in progressively larger point deductions.

**4.6 Weighting and Levels of the Safety Score:**

To ensure that the safety score accurately reflects the most critical aspects of safety performance, a system of weighting should be implemented, assigning different levels of importance to various rule categories based on their impact on overall safety.[39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54] For example, rules pertaining to fall protection [5, 7, 13, 14, 19, 42, 43, 73, 74, 105, 113, 114, 115, 116, 117, 145, 147, 150, 153, 157, 170, 189, 190, 191, 192] or electrical safety, which are known to be significant causes of serious injuries and fatalities in construction, could be assigned a higher weight compared to rules addressing less critical hazards. Similarly, leading indicators, which reflect proactive safety efforts and have a direct impact on preventing future incidents, could be weighted more heavily than lagging indicators that merely report past occurrences.[39, 41] The specific weights assigned to each rule category should be carefully determined based on a thorough risk assessment and should align with the organization's safety priorities.[193]

To facilitate understanding and interpretation of the safety score, clear score ranges and corresponding performance levels should be defined.[39, 40, 41, 43, 52] A 0-100 scale is often used for safety scores, as it is widely understood and provides a granular view of performance.[39, 40, 41, 43, 52] The following table provides a suggested framework for defining these score ranges and performance levels:

|  |  |  |
| --- | --- | --- |
| Safety Score Level | Score Range | Description |
| Excellent Safety Performance | 90-100 | Consistently exceeds safety standards, demonstrating a strong safety culture with proactive hazard identification and minimal incidents. |
| Good Safety Performance | 70-89 | Generally adheres to safety standards with room for minor improvements. Shows a commitment to safety but may have occasional minor incidents or areas needing strengthening. |
| Fair Safety Performance | 50-69 | Meets basic safety requirements but needs improvement in several areas. Indicates a moderate level of risk with potential for more frequent incidents if improvements are not made. |
| Poor Safety Performance | Below 50 | Does not consistently meet safety standards, indicating significant risks and a high likelihood of incidents. Requires immediate attention and implementation of corrective actions. |

This table provides a clear and easily understandable way to communicate the meaning of different score ranges to the users, facilitating comprehension and action.

**4.7 Implementation and Communication Strategy:**

The successful implementation of a rule-based safety score algorithm requires a well-thought-out strategy that addresses data collection and integration, ensures transparency and user understanding, considers the diverse roles within the construction environment, and accounts for variations across different sites and subcontractors.

Effective data collection and integration are paramount for the algorithm to function accurately and efficiently. This involves identifying all relevant data sources, which may include safety management software, incident reports, training records, wearable technology platforms, and inspection logs. Developing a system for automated data collection and seamless integration between these various sources is crucial for ensuring efficiency and minimizing manual data entry.

Ensuring transparency and user understanding is vital for the adoption and effectiveness of the safety score system. The algorithm's rules, scoring logic, and the data sources it utilizes must be communicated clearly and accessibly to all users.[39, 40, 41, 43, 45, 47, 50, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72] The use of intuitive dashboards for data visualization [27, 194, 195, 196, 197, 198, 199] can greatly enhance comprehension. Users should also be provided with easy access to a breakdown of their individual scores, detailing the specific rules they adhered to or violated.[41, 43] Furthermore, comprehensive resources and training programs should be offered to help users fully understand the safety score system and learn how they can take proactive steps to improve their scores.[4, 6, 11, 12, 13, 15, 18, 43, 46, 63, 64, 67, 73, 74, 76, 79, 86, 112, 117, 118, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150]

The safety score algorithm should also be designed to consider the different roles within the construction environment. For workers, the focus should be on individual safety behaviors, completion of required training, and the active reporting of hazards.[6, 31, 33, 35, 36, 38, 151, 132, 133, 164, 162] The score should be readily accessible to them and provide clear feedback on how their actions impact their safety standing. For supervisors, the algorithm should incorporate metrics related to the safety performance of their teams, the completion of site inspections, and their oversight of incident investigations. Leaderboards could be a valuable tool for fostering a healthy sense of competition among supervisory teams, encouraging them to strive for higher safety scores. When assessing subcontractors, the algorithm should consider their overall safety record, including metrics like EMR and TRIR, their compliance with project-specific safety requirements, and their incident rates.[15, 39, 79, 80, 108, 109, 110, 160, 161, 181, 182, 183, 200, 201, 202] The safety score of subcontractors could potentially influence their eligibility for future projects.[54, 80, 108, 202] Recognizing that different roles have varying responsibilities and levels of influence on safety is crucial for creating a relevant and effective safety score system.[81, 139, 161, 179, 203]

Finally, to ensure fairness and comparability, the safety score algorithm should incorporate mechanisms for normalization across different construction sites and subcontractors. Scoring should be adjusted based on factors such as project size, complexity, and the inherent risks associated with the specific type of construction work being performed.[73, 102, 144, 145, 178, 179, 180, 201, 204, 205] This could involve considering metrics like contract sum, project duration, and the specific tasks involved.[39, 52, 102, 123, 206] Additionally, subcontractor safety scores should be normalized by comparing them against industry benchmarks or against the scores of similar-sized subcontractors operating in comparable sectors.[8, 15, 39, 41, 52, 54, 63, 64, 69, 72, 73, 74, 76, 77, 79, 80, 87, 97, 101, 102, 103, 104, 105, 106, 108, 109, 110] Normalization is essential for creating a level playing field and ensuring that the safety score provides a meaningful and equitable assessment of performance across diverse construction environments and organizational structures.[39, 45, 52, 109]

**4.8 Conclusion and Recommendations:**

In conclusion, the implementation of a rule-based safety score algorithm holds significant potential for enhancing safety performance within the construction industry. This framework, built upon clearly defined rules, diverse data inputs, and a transparent scoring logic, offers a proactive approach to hazard identification, promotion of safer behaviors, and benchmarking of safety performance. By considering both lagging and leading indicators, incorporating advanced safety data from wearables and hazard reporting, and addressing negative events with appropriate severity weighting, the algorithm can provide a comprehensive assessment of safety standing.

The potential benefits of such a safety score are substantial, including improved safety performance metrics, a demonstrable reduction in the frequency and severity of incidents, enhanced compliance with safety regulations, and the cultivation of a stronger, more safety-conscious culture across the organization. Furthermore, a positive safety score can contribute to reduced insurance premiums, improved project outcomes, and an enhanced reputation within the industry.[8, 39, 41, 54, 69, 72, 73, 74, 76, 77, 80, 83, 87, 97, 104, 105, 106, 109, 157]

To ensure the successful development and implementation of this safety score algorithm, the following actionable recommendations are provided:

* Initiate the process with a pilot program involving a representative group of users and a diverse range of construction projects. This will allow for thorough testing and refinement of the algorithm before a full-scale rollout.
* Actively involve safety experts, construction site managers, and workers in the algorithm development process. Their practical insights and feedback are crucial for ensuring the system is relevant, user-friendly, and addresses the real-world challenges of construction safety.[112, 182, 189, 202, 205, 207]
* Establish robust data collection and integration mechanisms that ensure the accurate and efficient flow of safety-related data from various sources into the algorithm.[99, 208, 209, 166] Prioritize the quality and reliability of the data inputs to ensure the integrity of the safety score.
* Place a strong emphasis on transparency and user communication throughout the implementation process. Clearly articulate the algorithm's rules, scoring logic, and data sources, and provide ongoing support and training to help users understand the system and how to improve their scores.[41, 43, 45, 47, 50, 53, 54, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72]
* Commit to regularly reviewing and updating the algorithm based on its performance data, user feedback, and any changes in safety standards, regulations, or industry best practices.[11, 12, 16, 17, 18, 19, 39, 41, 44, 46, 50, 52, 54, 69, 72, 73, 74, 77, 80, 81, 90, 91, 92, 93, 94, 105, 106, 114, 115, 116, 139, 161, 166, 169, 179, 180, 181, 183, 184, 200, 210] This iterative approach will ensure the algorithm remains relevant and effective over time.
* Explore the potential of incorporating gamification elements into the safety score system. Features such as points, badges, and leaderboards can further engage users, incentivize safe behaviors, and foster a sense of friendly competition that drives continuous improvement in safety performance. Focus on rewarding positive actions and leading indicators to reinforce preventative safety practices.[129, 147, 160]

**5. Common Logic and Features**

**5.1 Gamification and Tracking**

* All defined safety activities across modules must be integrated with the gamification system to award points and contribute to scores within each customer organization.
* All user actions and system events related to safety (e.g., ticket status changes, permit approvals) must be trackable and logged for auditing and reporting purposes within the respective customer organization's data and for platform-level analytics (aggregated). [COMPLIANCE CRITICAL] Audit logs must be comprehensive, tamper-evident, and retained according to compliance requirements (HIPAA, GDPR, SOC 2).

**5.2 Rules Engine**

* A flexible rules engine must be developed to allow Safety Officers (via the Web Dashboard) to configure rules for safety score calculation, notifications, and potentially automated actions *within the scope permitted by their customer's subscription plan*.
* Super Admins must be able to define the available rule types and parameters accessible to different subscription plans.
* [COMPLIANCE CRITICAL] Rules that process or are triggered by sensitive data (especially PHI) must be designed and implemented with privacy and security in mind.

**5.3 Notifications**

* The system must support push notifications to mobile applications and potentially email notifications.
* Notifications must be triggered by key events within each customer organization.
* Notification content must be clear and direct the user to the relevant section of the app/dashboard. [COMPLIANCE CRITICAL] Notifications must not contain sensitive personal data or PHI.
* Users should have some level of control over notification preferences (e.g., opt-in/out of certain types).

**5.4 Data Synchronization (Procore API)**

* Must integrate with the Procore API.
* Data Sync (Initial Scope):
  + Import Site/Project information from Procore (Name, Location, Project Dates).
  + Import User/Employee information from Procore (Name, Contact Info, Company/Subcontractor). [COMPLIANCE CRITICAL] Data import must be secure and respect privacy. User consent for data transfer should be considered if required by GDPR.
  + Import Subcontractor information from Procore.
  + Synchronize Incident data (MySafety -> Procore, if Procore API supports incident creation/update). [COMPLIANCE CRITICAL] Synchronization of incident data, especially if containing PHI, must be done securely via encrypted channels and comply with HIPAA/GDPR requirements.
  + Synchronize Inspection data (MySafety -> Procore, if Procore API supports inspection creation/update).
  + Synchronize Training completion status (MySafety -> Procore, if Procore API supports training record updates). [COMPLIANCE CRITICAL] Secure transfer of personal data required for GDPR.
* Synchronization: Must support both initial bulk sync and ongoing delta sync (near real-time or scheduled intervals).
* Must handle potential data conflicts and errors during synchronization, with logging and alerting for Safety Officers (for their organization's sync) and Super Admins (for platform-level sync issues).
* The Procore integration must be configurable per customer organization by their Safety Officer (using API keys provided by the customer), or potentially managed centrally by the Super Admin depending on the integration architecture. [COMPLIANCE CRITICAL] API keys and credentials must be stored securely, encrypted at rest and in transit.

**5.5 Multi-lingual Support**

* The application interface (mobile and web for all roles) must support switching between multiple languages.
* Training content and common content pool resources must be manageable and deliverable in multiple languages.
* User language preference should be configurable at the user level.

**5.6 Offline Capability**

* The mobile applications must allow users to perform the following actions while offline:
  + Create Hazard Reports (with photo/video capture).
  + Perform Inspections (using downloaded checklists).
  + Initiate Incident Reports.
* Data captured offline must be stored locally and automatically synchronized with the server once connectivity is restored. [COMPLIANCE CRITICAL] Data stored locally on mobile devices must be encrypted. Synchronization must occur over secure, encrypted channels.
* Users must be clearly notified when working offline and when data is being synchronized.

**5.7 Multi-Tenancy**

* The application architecture must be designed to securely separate data and configurations for each customer organization (tenant). Users from one organization must not be able to access data or configurations belonging to another organization. [COMPLIANCE CRITICAL] This is fundamental for SaaS compliance with HIPAA, GDPR, and SOC 2. Strict logical separation of data is required.

**5.8 Data Privacy and Consent Management**

* [COMPLIANCE CRITICAL] The system must include mechanisms for obtaining and managing user consent for the collection and processing of their personal data, particularly for sensitive data like PHI or location data from wearables.
* [COMPLIANCE CRITICAL] Users must be informed about what data is being collected, how it is used, and who it is shared with (e.g., via a clear Privacy Policy).
* [COMPLIANCE CRITICAL] The system must support the right of individuals to access, rectify, and request erasure of their personal data (Right to be Forgotten) as required by GDPR.
* [COMPLIANCE CRITICAL] Data minimization principles should be applied – only collect data that is necessary for the stated purpose.
* [COMPLIANCE CRITICAL] Data should be anonymized or pseudonymized where possible, especially for reporting and analytics that do not require individual identification.

**5.9 Data Retention and Disposal**

* [COMPLIANCE CRITICAL] The system must support configurable data retention policies per customer organization, allowing data to be retained only for as long as necessary for legal, regulatory, or business purposes.
* [COMPLIANCE CRITICAL] Secure data disposal procedures must be implemented to permanently delete data when it is no longer required. This includes deleting associated files from S3 and videos from Vimeo according to the retention policies.

**6. Data Requirements**

**6.1 Data Entities**

* Customer: Attributes: Customer ID (unique), Company Name, Contact Information, Subscription Plan ID, License Status (Active, Suspended, Terminated), Start Date, End Date, Usage Metrics (linked).
* Subscription Plan: Attributes: Plan ID (unique), Name, Description, Features Included (list), User Limit, Site Limit, Storage Limit, Access to Common Content Pools (list), Pricing Details.
* Payment Transaction: Attributes: Transaction ID (unique), Customer ID, Amount, Date, Status, Payment Gateway Reference ID, Invoice ID. [COMPLIANCE CRITICAL] Payment data must be handled according to PCI DSS.
* Common Content Pool: Attributes: Pool ID (unique), Name, Description, Type (Checklist, Training Video, Document), Content Items (list).
* Common Content Item: Attributes: Item ID (unique), Pool ID, Name, Description, File/Content URL (Vimeo URL or ID for videos, S3 Object Key/URL for images/documents), Language Versions (list), Tags.
* Site: Attributes: Site ID (unique), Customer ID, Name, Location, Start Date, End Date, Status (Active, Closed), Associated Procore Project ID.
* User: Attributes: User ID (unique), Customer ID, Name, Employee ID, Contact Information (Email, Phone), Role (Safety Officer, Supervisor, Subcontractor User, Employee, Super Admin), Associated Subcontractor ID (if applicable), Assigned Sites (list), Language Preference, Procore User ID. [COMPLIANCE CRITICAL] Personal data, requires GDPR compliance.
* Subcontractor: Attributes: Subcontractor ID (unique), Customer ID, Company Name, Contact Information, Associated Procore Company ID.
* Training Course: Attributes: Course ID (unique), Customer ID, Name, Description, Language Versions (list of content per language), Modules (list), Assessment Questions, Passing Score, Assigned Roles/Sites/Subcontractors.
* Training Record: Attributes: Record ID (unique), User ID, Course ID, Module Completion Status, Assessment Score, Completion Date, Certification Expiry Date (if applicable). [COMPLIANCE CRITICAL] Personal data, requires GDPR compliance.
* Checklist Template: Attributes: Template ID (unique), Customer ID, Name, Description, Type (Equipment, Process), Categories (list), Items (list with response types, reference attachments), Source (Organization-Specific, Common Pool).
* Inspection: Attributes: Inspection ID (unique), Site ID, Checklist Template ID, Inspector User ID, Date/Time, Location (text, GPS), Responses (list of item responses with photos/comments), Status (Complete, In Progress), Color-coded Status (Green, Yellow, Red). [COMPLIANCE CRITICAL] May contain personal data or link to equipment/locations involved in incidents.
* Permit Type: Attributes: Type ID (unique), Customer ID, Name, Description, Associated Risks.
* Permit Request: Attributes: Request ID (unique), Permit Type ID, Site ID, Requestor User ID, Date/Time Requested, Start Date/Time, End Date/Time, Description of Work, Personnel Involved (list of User IDs), Hazard Assessment Details, Required PPE, Attachments (e.g., JHA, site plan, Vimeo URL/ID for videos, S3 Object Key/URL for images/documents), Status (Pending, Approved, Rejected, Expired), Approver User ID, Approval/Rejection Date/Time, Comments. [COMPLIANCE CRITICAL] Contains personal data and links to personnel.
* Incident: Attributes: Incident ID (unique), Site ID, Date/Time, Location, Type, Description, Sequence of Events (text), Involved Parties (List: Employees - link to user profiles, Subcontractors, Equipment), Injury Details (if applicable: Type of Injury, Body Part, Severity, First Aid/Medical Treatment), Property Damage Details (if applicable), Witness Information (Name, Contact - optional fields), Contributing Factors (text/dropdown - optional), Initial Actions Taken (text), Environmental Conditions (text/dropdown - optional), Attachments (Vimeo URL/ID for videos, S3 Object Key/URL for photos/documents), Investigation Findings, Root Cause Analysis, Corrective Actions (list), Status (Open, Investigating, Closed). [COMPLIANCE CRITICAL] Contains PHI (Injury Details) and personal data (Involved Parties, Witness Info). Requires strict HIPAA and GDPR compliance.
* Hazard Report: Attributes: Report ID (unique), Site ID, Date/Time Reported, Reported By User ID, Location, Description, Severity Level, Hazard Type, Recommended Action, Attachments (Vimeo URL/ID for videos, S3 Object Key/URL for photos/documents). [COMPLIANCE CRITICAL] May contain personal data (Reported By) and link to locations/equipment involved in potential incidents.
* Hazard Ticket: Attributes: Ticket ID (unique), Hazard Report ID, Assigned Subcontractor ID(s), Assigned Team ID(s) (if applicable), Assigned User ID(s) (if applicable), Status (Open, In Progress, Resolved, Complete, Re-opened), Comments/Actions History. [COMPLIANCE CRITICAL] Links to Hazard Report and assigned personnel.
* Safety Score Rule: Attributes: Rule ID (unique), Customer ID, Description, Triggering Event/Action (e.g., 'TrainingCompleted', 'HazardReported', 'IncidentOccurred', 'InspectionFailed'), Associated Module, Conditions (if applicable), Points Awarded/Deducted, Weighting Factor.
* Safety Score: Attributes: Score ID (unique), User ID/Subcontractor ID/Site ID/Team ID, Score Value, Scoring Period, Contributing Factors (breakdown of points earned/lost based on rules). [COMPLIANCE CRITICAL] Score is derived from potentially sensitive data. Display must be handled carefully to avoid exposing underlying sensitive information.
* Gamification Incentive: Attributes: Incentive ID (unique), Customer ID, Name, Description, Trigger (e.g., 'Reach 1000 points', 'Earn 'Fall Protection Expert' badge'), Type (e.g., 'Virtual Coupon', 'Recognition').
* Audit Log: Attributes: Log ID (unique), User ID, Date/Time, Action Type (e.g., 'Created Hazard Report', 'Updated Ticket Status', 'Viewed Permit'), Record ID affected, Details, Customer ID (for customer-specific actions). [COMPLIANCE CRITICAL] Critical for SOC 2 and compliance audits. Must be comprehensive, immutable, and securely stored.
* Team: Attributes: Team ID (unique), Customer ID, Name, Site ID, Subcontractor ID (if applicable), Members (list of User IDs). [COMPLIANCE CRITICAL] Contains personal data (Members).
* System Log: Attributes: Log ID (unique), Date/Time, Event Type (e.g., 'Customer Created', 'Payment Failed', 'API Sync Error'), Details, Associated Customer ID (if applicable). [COMPLIANCE CRITICAL] May contain system-level information relevant for SOC 2.

**6.2 Data Dictionary**

(To be detailed further during design phase, defining data types, constraints, relationships, data classification (e.g., Personal Data, PHI, Sensitive Personal Data), and handling requirements for each attribute listed above).

**6.3 Data Integration Requirements (Procore API, Vimeo API)**

* Must integrate with the Procore API.
* Data Sync (Initial Scope):
  + Import Site/Project information from Procore (Name, Location, Project Dates).
  + Import User/Employee information from Procore (Name, Contact Info, Company/Subcontractor). [COMPLIANCE CRITICAL] Data import must be secure and respect privacy. User consent for data transfer should be considered if required by GDPR.
  + Import Subcontractor information from Procore.
  + Synchronize Incident data (MySafety -> Procore, if Procore API supports incident creation/update). [COMPLIANCE CRITICAL] Synchronization of incident data, especially if containing PHI, must be done securely via encrypted channels and comply with HIPAA/GDPR requirements.
  + Synchronize Inspection data (MySafety -> Procore, if Procore API supports inspection creation/update).
  + Synchronize Training completion status (MySafety -> Procore, if Procore API supports training record updates). [COMPLIANCE CRITICAL] Secure transfer of personal data required for GDPR.
* Synchronization: Must support both initial bulk sync and ongoing delta sync (near real-time or scheduled intervals).
* Must handle potential data conflicts and errors during synchronization, with logging and alerting for Safety Officers (for their organization's sync) and Super Admins (for platform-level sync issues).
* The Procore integration must be configurable per customer organization by their Safety Officer (using API keys provided by the customer), or potentially managed centrally by the Super Admin depending on the integration architecture. [COMPLIANCE CRITICAL] API keys and credentials must be stored securely, encrypted at rest and in transit.
* Vimeo API Integration:
  + Must integrate with the Vimeo API for video uploads, management, and streaming.
  + Must use secure API authentication. [COMPLIANCE CRITICAL] API credentials must be stored securely.
  + Must handle video uploads from mobile and web applications to Vimeo.
  + Must retrieve video information (e.g., URL, metadata) from Vimeo.
  + Must embed or link to Vimeo videos within the MySafety application interfaces.
  + Must configure Vimeo privacy settings for uploaded videos to ensure data security and prevent unauthorized access. [COMPLIANCE CRITICAL] Video privacy settings must align with compliance requirements.
  + Must handle potential errors during Vimeo API interactions (e.g., upload failures, streaming issues).
* AWS S3 Integration:
  + Must integrate with AWS S3 for image and document uploads, storage, and retrieval.
  + Must use secure AWS authentication (IAM roles preferred over Access Keys). [COMPLIANCE CRITICAL] AWS credentials must be stored securely.
  + Must handle image and document uploads from mobile and web applications to S3.
  + Must store image and document files securely in S3 buckets. [COMPLIANCE CRITICAL]
  + Must retrieve image and document files from S3 for display within the MySafety application interfaces.
  + Must use secure methods for accessing files from S3, such as pre-signed URLs with limited validity, rather than making buckets publicly accessible. [COMPLIANCE CRITICAL]
  + Must handle potential errors during S3 interactions (e.g., upload failures, retrieval issues).

**6.4 Data Storage Requirements**

* Requirements for database technology, storage capacity, backup, and recovery, considering the multi-tenant architecture. [COMPLIANCE CRITICAL] Database must be configured for encryption at rest. Backups must be encrypted and stored securely.
* Video Storage: All video content will be stored on Vimeo. MySafety will store metadata about the videos (e.g., Vimeo video ID or URL, title, description) and link this metadata to relevant records (e.g., Hazard Reports, Incidents, Training Courses). [COMPLIANCE CRITICAL] Vimeo privacy settings must be configured to ensure videos are not publicly accessible and access is controlled via MySafety.
* Image and Document Storage (AWS S3 Model):
  + All image files (photos) and document files uploaded by users (Safety Officers, Supervisors, Subcontractors, Employees) for purposes such as Hazard Reports, Inspections, Incidents, Permits, and Common Content Pools will be stored in AWS S3.
  + Data Isolation: Data for each customer organization (tenant) must be logically separated within the S3 bucket(s). This will be achieved by using a consistent naming convention for object keys that includes the customer\_id as a prefix (e.g., customer\_id/module/record\_id/filename.jpg). This ensures that files belonging to one customer are stored in a distinct "folder" structure within the bucket, separate from other customers. [COMPLIANCE CRITICAL] This logical separation is essential for multi-tenancy compliance.
  + Security:
    - Encryption at Rest: All objects stored in S3 must be encrypted at rest. Server-Side Encryption with S3-Managed Keys (SSE-S3) or Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS) must be enabled for the S3 bucket(s). [COMPLIANCE CRITICAL]
    - Access Control: S3 bucket policies and IAM user/role policies must be configured to enforce the principle of least privilege. Backend services interacting with S3 should use IAM roles with specific permissions limited to necessary actions (putObject, getObject, deleteObject) within the designated customer prefixes. [COMPLIANCE CRITICAL]
    - Secure Access for Retrieval: Direct public access to the S3 bucket(s) must be disabled. When displaying images or documents in the MySafety application, the backend should generate pre-signed URLs with a limited time validity. These pre-signed URLs grant temporary access to a specific object without requiring the bucket to be public. [COMPLIANCE CRITICAL]
  + Linking in Database: The database will store metadata about the stored images and documents, including the S3 bucket name, the object key (which includes the customer\_id prefix), and potentially file name, size, and content type. This metadata will be linked to the relevant records in the application (e.g., hazard\_report\_media table will store the S3 key for photos attached to a hazard report).
* Requirements for storing other media files (excluding videos on Vimeo and images/documents on S3) securely and efficiently, ensuring separation per customer. [COMPLIANCE CRITICAL] Media storage must be encrypted at rest. Access controls must be strictly enforced.

**7. User Interface (UI) and User Experience (UX) Requirements**

**7.1 General UI Guidelines**

* Must adhere to a consistent design language and branding.
* Must prioritize mobile-first design for field users.
* Must be intuitive and easy to navigate for all user roles, minimizing the need for extensive training.
* Must use clear and legible fonts and color schemes with sufficient contrast.
* Must provide clear visual feedback for user actions.
* [COMPLIANCE CRITICAL] User interfaces must be designed to prevent accidental disclosure of sensitive information. Data fields containing PHI or sensitive personal data should be clearly identified and potentially require an extra step to view.

**7.2 Wireframes and Mockups (Reference)**

(To be provided separately to illustrate the intended layout and flow of the application interfaces for each user role and module, including the Super Admin panel. [COMPLIANCE CRITICAL] Wireframes and mockups should consider privacy-by-design principles, showing how sensitive data is handled and displayed.)

**7.3 Role-Specific UI Requirements**

* Mobile Apps (Supervisor, Subcontractor, Employee):
  + Focus on quick data entry, clear presentation of relevant information, and easy access to core functionalities within their organization's context.
  + Forms should be optimized for mobile input (e.g., large buttons, dropdowns).
  + Offline status must be clearly indicated.
  + Must include functionality for uploading videos, which will be sent to the backend for upload to Vimeo.
  + Must include functionality for capturing photos and selecting documents for upload, which will be sent to the backend for upload to AWS S3.
  + Must embed or link to videos hosted on Vimeo and display images/documents stored on S3 for viewing within the app.
  + [COMPLIANCE CRITICAL] Mobile apps must implement strong authentication and session management. Sensitive data displayed on the mobile app must be protected (e.g., requiring re-authentication to view PHI). Access to media linked to sensitive data must be controlled.
* Mobile App (Safety Officer):
  + Blend of quick action capabilities (like other mobile users) and access to key oversight information (e.g., dashboard summaries, notification lists) for their organization.
  + Must include functionality for uploading videos, which will be sent to the backend for upload to Vimeo.
  + Must include functionality for uploading images and documents, which will be sent to the backend for upload to AWS S3.
  + Must embed or link to videos hosted on Vimeo and display images/documents stored on S3 for viewing within the app.
  + [COMPLIANCE CRITICAL] Access to sensitive reports (e.g., incidents with injury details) and associated media must require appropriate authorization checks within the app.
* Web Dashboard (Safety Officer, Supervisor Login):
  + Designed for data analysis, configuration, and management within their organization.
  + Must provide robust filtering, sorting, and search capabilities for lists and reports.
  + Dashboards should present key metrics and attention areas visually.
  + Must include functionality for uploading videos, which will be sent to the backend for upload to Vimeo.
  + Must include functionality for uploading images and documents, which will be sent to the backend for upload to AWS S3.
  + Must embed or link to videos hosted on Vimeo and display images/documents stored on S3 for viewing within the dashboard.
  + [COMPLIANCE CRITICAL] Access to sensitive data and configuration options must be strictly controlled based on user role and permissions within the organization. Access to media linked to sensitive data must also be restricted.
* Super Admin Web Panel:
  + Designed for platform-level management, customer oversight, billing, and system configuration.
  + Must provide clear views of customer accounts, subscription details, and platform usage.
  + Intuitive interface for managing common content pools and subscription plans.
  + Secure access controls for Super Admin users.
  + Must include the new sections for Vimeo API Integration Management and AWS S3 Configuration Management.
  + [COMPLIANCE CRITICAL] Access to customer-specific data from the Super Admin panel must be restricted and logged. Sensitive data within customer accounts should be masked or require explicit action to view. Access to media linked to customer data must also be restricted and logged.
* Dropdowns: Must use standard dropdown UI elements for selecting teams or individuals when assigning hazard tickets. The dropdown should populate with relevant teams and users based on the site context and potentially subcontractor association within the user's organization. [COMPLIANCE CRITICAL] User lists in dropdowns should only display necessary identifying information (e.g., Name) and not sensitive details.

**7.4 Multi-lingual Support (UI)**

* All user-facing text elements in the application interface (mobile and web, including Super Admin panel) must be localizable and support switching between configured languages.

**8. Reporting Requirements (Detailed)**

**8.1 Standard Reports (Safety Officer - per Organization)**

* Hazard Report Summary: Count of reports by severity, type, site, subcontractor, assigned team/person, and status over a period. Average time to resolution. Includes links or embeds to associated media (videos and images/documents).
* Incident Summary: Count of incidents by type, severity, site, and contributing factors over a period. Injury types and severity analysis. Includes links or embeds to associated media (videos and images/documents). [COMPLIANCE CRITICAL] Reports containing PHI and/or links to media with sensitive content must be restricted. Options for generating reports with anonymized injury data should be available.
* Inspection Compliance: Percentage of completed inspections, average score/compliance rate per checklist type, site, and inspector. List of recurring failed items. Includes links or embeds to associated media (videos and images/documents).
* Training Completion: Percentage of employees who completed required training (overall, by course, by site, by subcontractor). List of overdue training. [COMPLIANCE CRITICAL] Reports containing individual training records are personal data and require appropriate access controls.
* Permit Activity: Number of permit requests by type, site, and status. Average time to approval. Includes links or embeds to associated media (videos and images/documents).
* Subcontractor Safety Performance: Summary of hazard reports, incidents, inspections, and training completion rates linked to specific subcontractors within the organization. Subcontractor safety score trends. Includes links or embeds to associated media where applicable. [COMPLIANCE CRITICAL] Ensure aggregated data in these reports does not inadvertently reveal sensitive individual information.
* Site Safety Performance: Summary of all safety activities and metrics for a specific site within the organization. Site safety score trends. Includes links or embeds to associated media where applicable.

**8.2 Ad-hoc Reporting (Safety Officer - per Organization)**

* Safety Officers must be able to build custom reports by selecting data fields from different modules, applying multiple filters, and grouping data, including filtering and grouping by assigned team or person for hazard reports within their organization. Must include options to include links or embeds to associated media. [COMPLIANCE CRITICAL] Access to sensitive data fields for ad-hoc reporting must be restricted based on user permissions. The system should prevent combining data fields in a way that could inadvertently expose sensitive information. Access to media linked to sensitive data must also be restricted.

**8.3 Report Export Formats (Safety Officer - per Organization)**

* PDF, PPT, DOC (for formatted reports with media, including embedded or linked videos and images/documents).
* CSV, Excel (for raw data export, including Vimeo video IDs or URLs and S3 Object Keys/URLs). [COMPLIANCE CRITICAL] Exported reports and data files containing sensitive information or links to sensitive media must be handled securely (e.g., password protection, encryption). Users must be warned about the risks of handling sensitive data outside the secure application environment.

**8.4 Data Visualization in Reports (Safety Officer - per Organization)**

* Must include options to generate charts (bar, line, pie) and graphs to visualize trends and comparisons within reports (e.g., incident trends over time, compliance rates by site). [COMPLIANCE CRITICAL] Visualizations must be designed to prevent the display of sensitive individual data. Aggregated or anonymized data should be used for charts where individual data is sensitive.

**8.5 Platform Reports (Super Admin)**

* Customer Overview Report: List of all customers, their subscription plan, license status, and key usage metrics.
* Revenue Report: Summary of subscription revenue over time (daily, monthly, annually), broken down by plan. [COMPLIANCE CRITICAL] Financial data must be handled securely (PCI DSS considerations).
* Platform Usage Report: Aggregated metrics on the use of different modules (e.g., total hazard reports created, total inspections completed, total training completions) across all customers or filtered by plan/date. Includes aggregated data on video uploads/views (Vimeo) and image/document storage usage (S3) if available via respective APIs. [COMPLIANCE CRITICAL] Aggregated data must be sufficiently anonymized to prevent re-identification of individuals or small groups.
* System Performance Report: Metrics on application uptime, response times, and error rates.
* Integration Status Report: Status of Procore, Payment Gateway, Vimeo, and AWS S3 integrations across the platform.

**9. Non-Functional Requirements**

* Performance:
  + Mobile app responsiveness: Actions (e.g., opening a form, submitting data) should complete within 2-3 seconds under normal network conditions. Video uploads may take longer depending on file size and network. Video playback performance is dependent on Vimeo and network conditions. Image/document uploads may take longer depending on file size and network. Image/document retrieval and display should be performant.
  + Web dashboard load time: Dashboards and reports should load within 5-7 seconds with typical data volumes per organization. Embedding multiple videos and displaying numerous images may impact load times.
  + Super Admin panel responsiveness: Panel should load quickly and handle queries efficiently, even with a large number of customers and aggregated data. Vimeo and AWS S3 integration management sections should be responsive.
  + Synchronization speed: Offline data synchronization should complete quickly upon reconnection. Procore sync frequency should be configurable. Video and image/document uploads upon reconnection are dependent on file size and network.
  + Scalability: The system architecture must support handling data and concurrent users for potentially hundreds or thousands of customer organizations, each with multiple sites and thousands of users, while maintaining performance under compliance requirements (e.g., encryption overhead). Scalability of video hosting is handled by Vimeo. Scalability of image/document storage is handled by AWS S3.
* Security:
  + User Authentication: Must implement secure login mechanisms (username/password with hashing, multi-factor authentication (MFA) is mandatory for Super Admins and highly recommended for Safety Officers and Supervisors)) for all user roles.
  + Authorization: Must enforce strict role-based and tenant-based access control, ensuring users only access data and features they are permitted to within their organization, and Super Admins have appropriate platform-level access. [COMPLIANCE CRITICAL] Implement granular permissions, especially for accessing sensitive data (PHI) and associated media (videos, images, documents).
  + Data Encryption: [COMPLIANCE CRITICAL] Sensitive data (including PHI, personal data, and credentials) must be encrypted at rest and in transit (using TLS/SSL). This applies to databases, file storage (S3), backups, and communication channels (APIs, including Vimeo API and AWS S3 API). Vimeo privacy settings must be configured to ensure videos are not publicly accessible and access is controlled via MySafety. S3 objects must be encrypted at rest (SSE-S3 or SSE-KMS).
  + Audit Trails: [COMPLIANCE CRITICAL] Comprehensive, immutable audit logs must be maintained for all user activity, data access (especially sensitive data and media), configuration changes (including Vimeo and AWS S3 settings), and system events. Logs must be securely stored and retained according to compliance requirements (HIPAA, GDPR, SOC 2).
  + Multi-Tenancy Security: [COMPLIANCE CRITICAL] Must ensure complete and verifiable data isolation between customer organizations through robust architectural design and implementation. This includes ensuring videos uploaded by one tenant are not accessible to another via MySafety (relying on Vimeo's privacy features and MySafety's access control) and ensuring images/documents stored on S3 by one tenant are not accessible to another (relying on S3 access policies and MySafety's access control based on the customer\_id prefix).
  + Vulnerability Management: Must have a process for identifying, assessing, and remediating security vulnerabilities in the application and underlying infrastructure.
  + Security Testing: Regular security testing, including penetration testing and vulnerability scanning, must be conducted.
* Usability:
  + Intuitive navigation within mobile apps and web dashboard for all user roles.
  + The Super Admin panel must be intuitive for managing customers, plans, content, and integrations (Vimeo, AWS S3).
  + Clear and concise error messages, including for media upload/streaming/retrieval issues.
  + Accessibility considerations (e.g., font sizes, color contrast) should follow relevant guidelines (e.g., WCAG). Media player/viewer controls should be accessible.
* Reliability:
  + System uptime: Target 99.9% availability for the core platform and customer-facing applications. Reliance on Vimeo for video availability and AWS S3 for image/document availability.
  + Data Backup and Recovery: [COMPLIANCE CRITICAL] Regular automated backups of all customer data (excluding videos stored on Vimeo and images/documents stored on S3) must be performed. Backups must be encrypted and stored securely offsite. A well-defined and tested disaster recovery plan with a low Recovery Point Objective (RPO) and Recovery Time Objective (RTO) is required for SOC 2. Video backup and recovery are handled by Vimeo. Image/document backup and recovery are handled by AWS S3's built-in redundancy and versioning features, but a strategy for lifecycle policies and potential cross-region replication should be considered for enhanced durability and disaster recovery.
  + Error Handling: Graceful handling of errors with informative messages and logging for both customer-level and platform-level issues, including issues related to Vimeo and AWS S3 integrations.
* Scalability:
  + Database must be able to handle significant growth in data volume across all customers while maintaining performance under encryption and access control requirements.
  + Application architecture should support scaling of servers/resources based on user load and the number of active customer organizations. Scalability of video hosting and streaming is handled by Vimeo. Scalability of image/document storage is handled by AWS S3.
* Maintainability:
  + Codebase should be well-structured, documented, and follow coding standards.
  + System architecture should support modular development and easier updates, including updates to Vimeo and AWS S3 integrations.
  + Deployment process should be streamlined for pushing updates to the SaaS platform.
* Portability:
  + Mobile applications must be compatible with target iOS and Android versions.
  + Web dashboard and Super Admin panel must be accessible via standard web browsers.
* Data Privacy:
  + [COMPLIANCE CRITICAL] Compliance with HIPAA (if handling PHI), GDPR (for personal data of EU citizens), and other relevant data protection regulations is mandatory. This includes implementing technical and organizational measures to ensure data protection by design and by default. This extends to handling video content and metadata stored on Vimeo and image/document content and metadata stored on S3. A Business Associate Agreement (BAA) with Vimeo and AWS may be required if PHI is included in videos or images/documents.
  + [COMPLIANCE CRITICAL] Clear data retention policies must be implemented and enforced. This includes a strategy for managing video content on Vimeo and image/document content on S3 according to retention policies.
  + [COMPLIANCE CRITICAL] Procedures for handling data subject requests (access, rectification, erasure) must be in place. This includes procedures for managing associated video content on Vimeo and image/document content on S3.
  + [COMPLIANCE CRITICAL] A process for data breach notification (to affected customers, individuals, and regulators) must be defined and ready. This includes breaches involving video content on Vimeo or image/document content on S3.

**10. Out of Scope for Initial Release**

* Integration with IoT devices for real-time sensor data beyond basic GPS. (Note: If IoT data includes physiological or highly granular location data, it would also have significant compliance implications).
* Advanced predictive analytics features (e.g., forecasting incident likelihood based on complex data patterns). (Note: If predictive analytics uses sensitive data, compliance considerations apply).
* Complex AI-powered autonomous actions beyond rule-based notifications and scoring. (Note: AI processing of sensitive data requires careful compliance review).
* Integration with additional third-party systems beyond Procore and Vimeo in the initial phase. (Note: Any future third-party integrations must also meet compliance requirements, potentially requiring BAAs).
* Advanced features like scheduling, resource management, or financial tracking within the safety modules (these are assumed to be handled by systems like Procore).
* Complex customization options for customer-specific branding beyond logo uploads.
* Direct video or image editing capabilities within the MySafety platform (editing will be assumed to be done outside the platform before upload).

**11. Glossary**

* HIPAA: Health Insurance Portability and Accountability Act - US law protecting sensitive patient health information.
* GDPR: General Data Protection Regulation - EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area.
* SOC 2: Service Organization Control 2 - An auditing procedure that ensures service providers securely manage data to protect the interests of their clients and the privacy of their clients' customers.
* PHI: Protected Health Information - Any information about health status, provision of healthcare, or payment for healthcare that is created or received by a covered entity, and can be linked to an individual.
* PCI DSS: Payment Card Industry Data Security Standard - A set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.
* Multi-Tenancy: An architecture in which a single instance of a software application serves multiple customers (tenants).
* BAA: Business Associate Agreement - A contract between a HIPAA covered entity and a HIPAA business associate that is required by law.

**12. Technology Stack**

Based on the requirements for a SaaS application with web and mobile interfaces, data integration, deployment on AWS, critical compliance needs (HIPAA, GDPR, SOC 2), and the use of Vimeo for video services and S3 for images/documents, the following technology stack is proposed:

* Frontend (Web Dashboard & Super Admin Panel):
  + React.js: A popular JavaScript library for building user interfaces. Its component-based architecture is well-suited for building complex and interactive web applications like the Safety Officer dashboard and Super Admin panel.
  + State Management: Libraries like Redux or Zustand for managing application state efficiently, especially in a large application with multiple modules.
  + Styling: Tailwind CSS or a similar utility-first CSS framework for rapid and consistent styling, ensuring a responsive and modern look and feel.
  + Video Player: Integration with a Vimeo-compatible video player library for embedding and streaming videos.
  + Image/Document Viewer: Libraries or components for displaying various image formats and potentially embedding/linking documents.
* Frontend (Mobile Applications):
  + Flutter: A UI toolkit for building natively compiled applications for mobile, web, and desktop from a single codebase. This aligns with the requirement for both iOS and Android apps and can potentially support a kiosk mode interface.
  + Video Player: Integration with a Vimeo-compatible video player library for embedding and streaming videos.
  + Image/Document Handling: Mobile code to capture photos, select documents, and send them to the backend for upload to AWS S3.
  + Video Upload Handling: Mobile code to capture video and send it to the backend for upload to Vimeo.
  + Image/Document Viewer: Components for displaying images and potentially viewing documents.
* Backend:
  + Node.js (with Express.js or NestJS): A popular choice for building scalable and efficient backend APIs. Node.js is well-suited for handling concurrent requests and integrating with various services.
  + Language: JavaScript or TypeScript (recommended for better code maintainability and scalability).
  + Vimeo API Client: Implementation of a client to interact with the Vimeo API for video uploads, metadata management, and retrieval of video URLs. [COMPLIANCE CRITICAL] Secure handling of API credentials.
  + AWS SDK: Utilizing the AWS SDK for interacting with S3 for image and document uploads, retrieval (generating pre-signed URLs), and management. [COMPLIANCE CRITICAL] Secure handling of AWS credentials/IAM roles.
* Database:
  + PostgreSQL: A powerful, open-source relational database system known for its reliability, extensibility, and strong support for complex queries. It is well-suited for handling structured data like user information, reports, and checklists, and its support for JSON can be useful for flexible data storage. [COMPLIANCE CRITICAL] Must be configured for encryption at rest.
  + Database Management: Consider using an ORM (Object-Relational Mapper) like Sequelize or TypeORM for easier interaction with the PostgreSQL database from the backend code. The ORM should support secure data handling practices.
* Cloud Platform:
  + AWS (Amazon Web Services): The chosen cloud provider for hosting the application. [COMPLIANCE CRITICAL] AWS offers services that are HIPAA eligible and support GDPR and SOC 2 compliance, but they must be configured correctly.
  + Relevant AWS Services:
    - EC2 (Elastic Compute Cloud): For hosting the backend application servers. [COMPLIANCE CRITICAL] Security hardening and access control are essential.
    - RDS (Relational Database Service): For managed PostgreSQL database instances, simplifying database administration, scaling, and backups. [COMPLIANCE CRITICAL] Must use encrypted RDS instances. Access must be restricted.
    - S3 (Simple Storage Service): For storing media files (photos, documents) uploaded by users (excluding videos). [COMPLIANCE CRITICAL] Must use encrypted S3 buckets. Access policies must be strictly controlled, and direct public access disabled. Use pre-signed URLs for retrieval.
    - Lambda (Serverless Compute): Potentially for handling specific tasks like processing notifications or background jobs, including triggering Vimeo and S3 uploads. [COMPLIANCE CRITICAL] Lambda functions handling sensitive data must be designed securely.
    - API Gateway: For managing and securing API endpoints for the mobile and web applications. [COMPLIANCE CRITICAL] Must enforce authentication and authorization. Use WAF for additional protection.
    - VPC (Virtual Private Cloud): For creating a secure and isolated network environment. [COMPLIANCE CRITICAL] Network segmentation and security group rules are critical for isolating resources and data.
    - IAM (Identity and Access Management): For managing user access and permissions within AWS. [COMPLIANCE CRITICAL] Implement least privilege access for all AWS resources.
    - CloudWatch: For monitoring application performance and logs. [COMPLIANCE CRITICAL] Logs must be securely stored and monitored for suspicious activity.
    - SNS (Simple Notification Service) / SES (Simple Email Service): For managing notifications (push notifications, emails). [COMPLIANCE CRITICAL] Ensure sensitive data is not included in notifications.
    - Elastic Load Balancing (ELB): For distributing incoming traffic across multiple EC2 instances to ensure high availability and scalability.
    - KMS (Key Management Service): For managing encryption keys used for RDS, S3, etc. [COMPLIANCE CRITICAL] Essential for managing encryption keys securely.
    - CloudTrail: For logging API calls and account activity. [COMPLIANCE CRITICAL] Provides audit trails for actions taken within the AWS environment.
* Integration:
  + RESTful APIs: Designing and implementing RESTful APIs for communication between the frontend (web and mobile) and the backend, and for integration with Procore, Stripe, Vimeo, and AWS S3. [COMPLIANCE CRITICAL] APIs must be secured using appropriate authentication and authorization mechanisms (e.g., OAuth2, JWT). Data transmitted via APIs must be encrypted (HTTPS).
  + Procore API: Utilizing the Procore API for data synchronization. [COMPLIANCE CRITICAL] Secure integration is paramount. Ensure Procore's API and your usage comply with HIPAA/GDPR if sensitive data is exchanged.
  + Stripe API: Integrating with the Stripe API for payment processing and subscription management. [COMPLIANCE CRITICAL] Adherence to Stripe's integration guidelines and PCI DSS is required.
  + Vimeo API: Integrating with the Vimeo API for video services. [COMPLIANCE CRITICAL] Secure integration and handling of sensitive video content are paramount. A Business Associate Agreement (BAA) with Vimeo may be required if PHI is included in videos.
  + AWS S3 API: Interacting with the AWS S3 API for file operations. [COMPLIANCE CRITICAL] Secure interaction and handling of sensitive image/document content are paramount. A BAA with AWS may be required if PHI is included in images/documents.
* Other Relevant Technologies:
  + Caching: Redis or Memcached for caching frequently accessed data to improve performance. [COMPLIANCE CRITICAL] Sensitive data should not be stored in cache without appropriate encryption and security measures.
  + Queueing: RabbitMQ or SQS (Simple Queue Service) for handling asynchronous tasks like sending notifications or processing background jobs, including media upload processing. [COMPLIANCE CRITICAL] Sensitive data in queues must be protected.
  + Containerization: Docker for packaging applications and their dependencies, facilitating consistent deployment. [COMPLIANCE CRITICAL] Docker images must be scanned for vulnerabilities.
  + Orchestration: Kubernetes (EKS on AWS) for managing and scaling containerized applications in a production environment. [COMPLIANCE CRITICAL] Kubernetes cluster security configuration is critical.
  + Monitoring and Logging: Tools like Prometheus, Grafana, or the ELK stack (Elasticsearch, Logstash, Kibana) for advanced monitoring and centralized logging. [COMPLIANCE CRITICAL] Logging infrastructure must be secure, and logs containing sensitive data must be protected and retained.
  + Data Masking/Anonymization Libraries: Libraries or tools to facilitate the anonymization or pseudonymization of sensitive data for reporting and analytics purposes.

**13. Database Structure by Microservice (Shared Tenant Data)**

This section outlines the recommended database structure for the MySafety application based on a microservices architecture using PostgreSQL, where each database serves multiple tenants with data logically segregated by a tenant identifier.

Important Note on Compliance (HIPAA, GDPR, SOC 2): In this shared-database-per-service model, data isolation between tenants relies heavily on the application logic and database-level security features (like Row-Level Security if implemented). This is a significant change from the physical isolation provided by the Database per Tenant model. Implementing robust security controls at both the application and database layers is absolutely [COMPLIANCE CRITICAL] to prevent unauthorized cross-tenant data access and meet the requirements of HIPAA, GDPR, and SOC 2. Audit trails for data access become even more critical.

Each database listed below would be a separate PostgreSQL database instance. Within each instance, tables would include a customer\_id or tenant identifier column to distinguish data belonging to different customer organizations.

**13.1 Super Admin Database**

* Primary Service: Super Admin Service
* Purpose: Stores platform-level data, configurations, and metadata that are not specific to any single customer organization.
* Key Tables:
  + customers: Stores information about each customer organization (name, contact, subscription plan ID, license status, etc.).
  + subscription\_plans: Defines the different subscription tiers, features, and limits.
  + payment\_transactions: Records billing and payment history integrated with Stripe.
  + common\_content\_pools: Manages metadata for shared checklists, training content, etc.
  + common\_content\_items: Metadata for individual items within common pools, including Vimeo video IDs or URLs and S3 Object Keys/URLs for images/documents.
  + super\_admin\_users: User accounts and permissions for Super Admins.
  + system\_logs: Platform-level error and activity logs.
  + platform\_configurations: Global application settings, including Vimeo API credentials (securely stored) and AWS S3 configuration details (bucket names, potentially IAM role ARNs, securely stored).
* Compliance Note: This database is critical for platform security and compliance management. Access must be highly restricted and auditable. [COMPLIANCE CRITICAL]

**13.2 User/Identity Database**

* Primary Service: User/Identity Service
* Purpose: Manages user accounts, roles, permissions, and team assignments across all tenants. Data is segregated by customer\_id.
* Key Tables:
  + users: Stores individual user profiles (name, contact, role, employee ID, language preference, Procore User ID). Includes customer\_id. [COMPLIANCE CRITICAL]
  + roles: Defines the different user roles (Safety Officer, Supervisor, Employee, etc.).
  + permissions: Maps roles to specific application permissions.
  + teams: Defines teams within customer organizations. Includes customer\_id.
  + user\_teams: Joins users to teams. Includes customer\_id.
  + user\_sites: Assigns users to specific sites. Includes customer\_id.
* Compliance Note: Contains personal data. Requires strict access control based on customer\_id and user role. [COMPLIANCE CRITICAL]

**13.3 Site Management Database**

* Primary Service: Site Management Service
* Purpose: Manages construction site and subcontractor information for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + sites: Stores details about construction sites (name, location, dates, status, Procore Project ID). Includes customer\_id.
  + subcontractors: Stores information about subcontractor companies (name, contact, Procore Company ID). Includes customer\_id.
  + site\_subcontractors: Maps subcontractors to sites. Includes customer\_id.
* Compliance Note: Contains organizational and location data. Requires access control based on customer\_id.

**13.4 Hazard Reporting Database**

* Primary Service: Hazard Reporting Service
* Purpose: Stores hazard reports and related ticket information for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + hazard\_reports: Stores details of reported hazards (title, description, location, severity, type, reported by user ID). Includes customer\_id. [COMPLIANCE CRITICAL]
  + hazard\_tickets: Manages the lifecycle of tickets created from hazard reports (assignment to users/teams/subcontractors, status, comments). Includes customer\_id. [COMPLIANCE CRITICAL]
  + hazard\_report\_media: Metadata for photos and videos attached to hazard reports (Vimeo video ID or URL for videos, S3 Object Key/URL for photos/documents). Includes customer\_id.
* Compliance Note: May contain personal data (reported by, assigned to) and location data. Requires access control based on customer\_id and user role/assignment. Access to associated media must be controlled. [COMPLIANCE CRITICAL]

**13.5 LMS/Training Database**

* Primary Service: LMS/Training Service
* Purpose: Manages training course assignments and tracks training records for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + training\_courses: Defines training courses (name, description, modules, assessments). Includes customer\_id (for organization-specific courses) or links to Common Content Pool. Includes Vimeo video IDs or URLs for video content and S3 Object Keys/URLs for document content.
  + training\_records: Tracks individual user progress and completion for assigned courses (user ID, course ID, completion status, scores, expiry dates). Includes customer\_id. [COMPLIANCE CRITICAL]
  + course\_assignments: Maps courses to users, roles, sites, or subcontractors. Includes customer\_id.
* Compliance Note: Contains personal data (training records). Requires access control based on customer\_id and user (for personal records) or role (for oversight). Access to associated training media must be controlled. [COMPLIENCE CRITICAL]

**13.6 Inspection Database**

* Primary Service: Inspection Service
* Purpose: Stores inspection checklist templates and completed inspection reports for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + checklist\_templates: Defines inspection checklist templates (name, items, response types). Includes customer\_id (for organization-specific) or links to Common Content Pool.
  + inspections: Records completed inspections (site ID, checklist ID, inspector user ID, date/time, location, status). Includes customer\_id. [COMPLIANCE CRITICAL]
  + inspection\_responses: Stores responses to individual checklist items. Includes inspection\_id and implicitly customer\_id. [COMPLIANCE CRITICAL]
  + inspection\_media: Metadata for photos and videos attached to inspection responses (Vimeo video ID or URL for videos, S3 Object Key/URL for photos/documents). Includes inspection\_id and implicitly customer\_id.
* Compliance Note: May contain personal data (inspector) and location data. Requires access control based on customer\_id and user role/site assignment. Access to associated media must be controlled. [COMPLIANCE CRITICAL]

**13.7 Permits Database**

* Primary Service: Permits Service
* Purpose: Manages permit types and stores permit requests and records for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + permit\_types: Defines permit types (name, description). Includes customer\_id.
  + permit\_requests: Stores permit application details (type, site ID, requestor user ID, work details, dates, status, approver user ID, comments). Includes customer\_id. [COMPLIANCE CRITICAL]
  + permit\_attachments: Metadata for documents and videos attached to permit requests (Vimeo video ID or URL for videos, S3 Object Key/URL for images/documents). Includes permit\_request\_id and implicitly customer\_id.
* Compliance Note: Contains personal data (requestor, personnel involved, approver). Requires access control based on customer\_id and user role/site assignment. Access to associated media must be controlled. [COMPLIANCE CRITICAL]

**13.8 Incident Reporting Database**

* Primary Service: Incident Reporting Service
* Purpose: Stores detailed incident reports and related investigation data for all tenants. Data is segregated by customer\_id. This database handles PHI.
* Key Tables:
  + incidents: Stores core incident details (site ID, date/time, location, type, description, sequence of events, status). Includes customer\_id. [COMPLIANCE CRITICAL]
  + involved\_parties: Lists users, subcontractors, or equipment involved in an incident. Links to incident\_id. Includes customer\_id. [COMPLIANCE CRITICAL]
  + injury\_details: Stores detailed information about injuries sustained in an incident (type, body part, severity, treatment). Links to incident\_id and involved\_party\_id. Includes customer\_id. [COMPLIANCE CRITICAL] This table contains PHI.
  + witness\_information: Stores witness details (name, contact). Links to incident\_id. Includes customer\_id. [COMPLIANCE CRITICAL]
  + incident\_attachments: Metadata for photos and videos attached to incident reports (Vimeo video ID or URL for videos, S3 Object Key/URL for photos/documents). Links to incident\_id. Includes customer\_id. [COMPLIANCE CRITICAL]
  + investigation\_findings: Stores details from the incident investigation. Links to incident\_id. Includes customer\_id.
  + corrective\_actions: Stores corrective and preventive actions identified. Links to incident\_id. Includes customer\_id.
* Compliance Note: This database is the most critical for HIPAA compliance due to PHI. Requires the highest level of security, granular access control (including Row-Level Security if possible in PostgreSQL), and strict auditing based on customer\_id and specific data sensitivity. Access to associated media containing PHI must be strictly controlled. [COMPLIANCE CRITICAL]

**13.9 Gamification/Scorecard Database**

* Primary Service: Gamification/Scorecard Service
* Purpose: Stores gamification data, safety score rules, and calculated safety scores for all tenants. Data is segregated by customer\_id.
* Key Tables:
  + safety\_score\_rules: Defines the rules and weighting for calculating safety scores. Includes customer\_id.
  + safety\_scores: Stores calculated safety scores for users, teams, sites, subcontractors, etc., for different periods. Includes customer\_id. [COMPLIANCE CRITICAL]
  + score\_contributions: Details which events/actions contributed to a specific score (linking back to source data in other databases). Includes customer\_id. [COMPLIANCE CRITICAL]
  + gamification\_incentives: Defines incentives linked to achievements. Includes customer\_id.
  + user\_achievements: Tracks badges and achievements earned by users. Includes customer\_id.
* Compliance Note: Stores data derived from potentially sensitive sources (like incident reports). Display and access to contributing factors must be carefully controlled based on customer\_id and user role to avoid exposing underlying sensitive data. [COMPLIANCE CRITICAL]

**13.10 Reporting/Analytics Database**

* Primary Service: Reporting/Analytics Service
* Purpose: Stores data optimized for generating reports and analytics across all tenants. Data is segregated by customer\_id. This database may contain denormalized or aggregated data from other databases for read performance.
* Key Tables:
  + Tables optimized for reporting queries, potentially denormalized copies or materialized views of data from other databases (e.g., aggregated\_incident\_data, inspection\_summary\_data). Includes customer\_id in all relevant tables. Includes links or embeds to associated media where applicable. [COMPLIANCE CRITICAL]
* Compliance Note: Aggregates data from potentially sensitive sources. Requires strong logical segregation and access control based on customer\_id to ensure reports only show data for the correct tenant. Anonymization or pseudonymization should be applied where possible for aggregated reports. Access to media linked to sensitive data must be controlled. [COMPLIANCE CRITICAL]