Sigmatrix InterEx v1.0 — Use Cases & Requirements Document

---

1. Purpose and Scope

This document defines the use cases, requirements, operational assumptions, and non-functional criteria for InterEx v1.0—the replacement solution for the CMS HIH GUI/API, supporting provider organizations, HIHs, and Sigmatrix as integrator. It covers all documentation exchange, user management, eMDR/letter workflows, security, audit, compliance, and operational needs for migration to PCG FHIR.

Audience: Project sponsors, business/technical analysts, developers, QA, vendors, and operational stakeholders.

---

2. Version and Change History

Version	Date	Summary of Changes
1.0	2025-06-10	Initial version with User Stories and Requirements separately.
1.1	2025-06-10	Combined user stories with corresponding functional requirements.
1.2	2025-06-11	Initial consolidated version with ChatGPT-recommended structure.

---

3. User Roles and Permissions

Role	Permissions/Actions
Customer Admin	Full management of provider groups, users, NPIs, all submissions/letters.
Provider Group Admin	Manage users/NPIs within group, submissions/letters for assigned group.
Basic User	Submit/view docs for assigned NPIs, view/acknowledge letters, update provider info.

---

4. Use Case Summary & Mapping

UC ID	Use Case Summary	Related Requirements/Stories
UC1.1	Create submission (all LOBs)	DS1, DS2, DS3

UC ID	Use Case Summary	Related Requirements/Stories
UC1.2	Upload/support split/auto-split docs	DS4, DS5
UC1.3	Track status of submissions	DS6, DS7
UC1.4	View/search submission history	DS8, DS9
UC1.5	Handle duplicates/errors	DS10, DS11
UC2.1	Create/edit/delete Provider Groups	UM1, UM2
UC2.2	CRUD users (Admin/Group Admin/Basic User)	UM3, UM4, UM5
UC2.3	Add/edit/delete NPIs; assign to groups/users	UM6, UM7
UC2.4	Register/deregister providers for eMDR	UM8, UM9
UC2.5	Update provider info	UM10
UC2.6	View/search providers, NPIs, users	UM11
UC2.7	Basic users manage only assigned NPIs/providers	UM12
UC3.1	Receive/display eMDRs/letters with filters	EM1, EM2, EM3
UC3.2	Download/view PDF attachments and metadata	EM4, EM5
UC3.3	Acknowledge receipt of eMDR/letters	EM6, EM7
UC3.4	Track/view letter history, search by date/NPI/claim	EM8
UC4.1	Enforce secure logins (SAML, OAuth2, OpenID; MFA required)	S1, S2, S3
UC4.2	Manage user sessions, password policies, lockout/reset	S4, S5
UC4.3	Enforce least-privilege, RBAC	S6
UC5.1	Log all key user/admin/submission/letter/security events	A1, A2
UC5.2	View/export audit logs	A3, A4
UC5.3	Basic admin dashboards/reports	R1, R2
UC5.4	System health/status dashboards	OP1
UC5.5	Error monitoring/notification	OP2

---

5. Operational & Process Assumptions

- **API Compatibility:** PCG FHIR will fully support a wrapper for all CMS HIH API endpoints; legacy API clients require minimal changes to their endpoints.
- **GUI Transition:** InterEx is the sole supported GUI/browser app for ex-HIH GUI users.
- **Support:** All user/operational support post-migration provided by Sigmatrix.
- **User Model:** Hierarchical roles/permissions as per legacy HIH (see table above).
- **File Handling:** 200MB max payload, 600MB max per submission; PDF only.
- **eMDR/Letters:** Retrieved from PCG FHIR endpoints; original structure/metadata preserved. User acknowledgment required.
- **Provider Management:** eMDR registration/deregistration flows match HIH, including "electronic only" option.

- **Security:** OAuth2 (client ID/secret) for API users, SAML/OpenID/OAuth2+MFA for GUI; XSRF/message signature on all relevant calls.
- **Audit/Reporting:** All CRUD/submission/download/auth events logged; admins get basic reporting.
- **Testing/Onboarding:** All users receive test credentials for PCG FHIR; onboarding support required; InterEx launches in test mode for migration.

---

6. Functional Requirements and User Stories

A. Documentation Submission

- **DS1:** System must support all lines of business (ADR, Appeals, PWK, IRF, etc.) with correct "purpose_of_submission."
- **DS2:** Must allow users to create submission objects with metadata (NPI, claim/case ID, recipient, title, comments).
- **DS3:** System must support PDF upload; both auto-split and manual split, enforce payload/submission limits.
- **DS4:** Show status (Draft, Submitted, Delivered, Error) and transaction IDs.
- **DS5:** Allow search, filter, and download of submission history.
- **DS6:** Provide actionable error handling (e.g., for invalid metadata, duplicate, format error).
- **DS7:** API/GUI must both support all submission operations.

B. User Management & Provider/NPI/eMDR

- **UM1:** Admins can CRUD provider groups, users, NPIs.
- **UM2:** Assign NPIs to groups/users; enforce validation (10-digit NPI, format rules).
- **UM3:** Provider CRUD (name/address); registration/deregistration for eMDR, incl. "electronic only."
- **UM4:** Users see/manage only assigned NPIs/providers.
- **UM5:** View registration status, enrollment, change history.
- **UM6:** All user management actions via GUI and API.

C. eMDR & Letters

- **EM1:** Poll/retrieve all pre-pay, post-pay, PADL, RRL letters for assigned NPIs/providers.
- **EM2:** Allow download/view of letter PDFs and metadata.
- **EM3:** Filter/search by date, NPI, claim, type.
- **EM4:** Require acknowledgment for each letter; handle duplicate ack errors with clear flags/messages.
- **EM5:** Support all HIH API letter types, acknowledgment calls.

D. Security, MFA, Authorization

- **S1:** All logins require MFA (per HIPAA).

- **S2:** GUI supports SAML 2.0, OpenID Connect, OAuth2; API uses OAuth2 client credentials.
- **S3:** Secure all endpoints (HTTPS, OAuth2 tokens, XSRF).
- **S4:** API requires message signature (base64, private key), timestamp.
- **S5:** Password policy: min 12 chars, complexity, 90-day expiration, account lockout (5 failed attempts), session timeout (15 min inactivity).
- **S6:** Only authorized users access data (enforce RBAC at all levels).

E. Audit Logs, Reporting, and Operations

- **A1:** Log: login, failed login, MFA, CRUD (users/NPIs/groups), submissions, downloads, eMDR/letter viewing and acknowledgment, errors.
- **A2:** Retention: min 6 years (HIPAA); tamper-evident logs, restricted admin access.
- **A3:** Enable authorized users to view/export logs; filter by date/user/event.
- **A4:** Basic admin dashboard: counts, submission/letter status, user activity.
- **R1:** System health dashboard (jobs, error rates, outages, queue status).
- **R2:** Alerts: failures, outages, critical errors, data integrity issues.

---

7. Data Validation & Business Rules

- NPI: 10-digit numeric.
- Claim ID: 8, 13–15, or 17–23 alphanumeric, not all zeros/dashes.
- Case ID: up to 32 chars; PERM: 11 alphanumeric.
- File type: PDF only.
- File size: max 200MB per upload, 600MB total per submission.

---

8. Error Handling, Retries, and Messaging

- Errors in both GUI and API return clear codes/messages.
- System auto-retries transient errors for submissions/letters; persistent errors require user action.
- All user-facing errors are actionable with support reference codes.

---

9. Session and Security Details

- Session timeout: 15 min inactivity (configurable).
- Password: min 12 chars, complexity, expires in 90 days.
- Account lockout after 5 failed attempts; unlock via admin or validated email/MFA.
- MFA backup/alternate device required for recovery.

10. Audit Logging Events & Retention

- Events: login/logout, failed login, password/MFA reset, CRUD users/roles/NPIs/groups, submission create/upload, eMDR/letter view/acknowledge, error/warning.
- Retention: 6 years (HIPAA), tamper-evident, restricted admin access.

---

11. API-only vs GUI-only Features

- Manual file split: GUI only; API must set split metadata correctly.
- Some advanced admin/ops dashboards may initially be GUI-only.

---

12. Sample Acceptance Criteria

- Given a PDF >200MB, system auto-splits, each part has a unique transaction ID/status.
- Invalid NPI/Claim ID formats result in clear validation error, user cannot proceed.
- Unauthorized NPI access is denied, event logged.

---

13. Glossary/Abbreviations

- **NPI:** National Provider Identifier
- **eMDR:** Electronic Medical Document Request
- **PADL:** Provider Additional Documentation Letter
- **RRL:** Results Review Letter
- **ADR:** Additional Documentation Request
- **MFA:** Multi-Factor Authentication
- **SAML:** Security Assertion Markup Language
- **OAuth2:** Open Authorization 2.0
- **RBAC:** Role-Based Access Control
- **GUI:** Graphical User Interface
- **API:** Application Programming Interface

---

14. Open Questions/Clarifications (For Stakeholders/Vendor)

Question	Impact if Unresolved	Status/Owner
Will PCG FHIR wrapper fully replicate CMS HIH API endpoints?	Critical for migration; API users break if not	
Deprecation timeline for HIH endpoints, parallel run period?	Impacts migration planning/communications	
Data migration/retention: Existing submission/user data?	Compliance, user access, continuity	
SLA for eMDR/letter delivery, retries, acknowledgment?	Provider deadlines, error handling	
Will all legacy letter types (PADL/RRL) be delivered via FHIR?	Affects eMDR implementation scope	
Customer onboarding/training/support expectations?	Affects onboarding/helpdesk planning	
SAML/OIDC IdP: Single or multiple?	Auth integration complexity	
Private key/cert rotation policy?	Security, compliance	
Audit/report export: Required in admin UI or API sufficient?	Admin feature set	
Test environment & onboarding: workflows supported, credential reset?	Crucial for UAT and migration	
Future: Support non-PDF types, SMART on FHIR, next-gen provider workflows?	Technical roadmap	

---

15. Non-Functional, Ops, Migration, and Accessibility

- **Accessibility:** All UI must be WCAG 2.1 AA, supporting keyboard, screen readers, and color contrast.
- **Ops:** Admin dashboard: system health, queues, error/outage rates; configurable alerts.
- **Reporting:** Admins can export CSV/PDF; filter by date, user, and event.
- **Migration:** If user, NPI, or submission data migration is required, the necessary migration tooling, validation, and rollback procedures must be specified.
- **Version Control:** All requirements, test cases, and config items must have a version history.

---

16. Summary Table by Functional Area

Area	Key Requirements/Use Cases
Documentation Submission	All LOBs, metadata, file split, PDF only, status/error tracking

Area	Key Requirements/Use Cases
User Management	Hierarchical RBAC, CRUD, NPI/provider/eMDR management, validation
eMDR/Letters	Pre-pay/post-pay/PADL/RRL, display/download, search/filter, ack
Security/Authorization	OAuth2, SAML, OpenID, MFA, RBAC, message signing, password/session
Audit/Reporting/Support	Logging, admin dashboard, export, ops health/error monitoring

---