FEATURE_01_REVIEW_GUIDE

December 16, 2025 at 10:25 AM

Feature #1 Implementation Plan - Review Guide

Purpose: Structured review of FEATURE_01_IMPLEMENTATION_PLAN.md before implementation begins

---

1. SCOPE & TIMELINE

What's Proposed

Timeline: 3 weeks (15 business days) - Week 1 (Days 1-5): Foundation - Week 2 (Days 6-10): Database & Export - Week 3 (Days 11-15): Migration & Testing

Developers: 1 full-time OR 2 part-time

Total Code: ~1,000 lines of new R code + tests

Review Questions

Q1.1: Is 3 weeks realistic for your environment? - [CHECKMARK] Yes, sounds right - □ Too aggressive, need 4-5 weeks - □ Depends on developer experience level - [X] No specific timeline needed

Comments: ________________

Q1.2: Developer allocation preference? - □ 1 developer full-time (focused, no context-switching) - □ 2 developers part-time (can parallelize modules) - □ Flexible, depends on availability - □ Other approach: ________________

Comments: ________________

---

2. MODULES & CODE STRUCTURE

What's Proposed

4 New R Modules (plus setup script + tests):

```
R/encryption_utils.R      (250-300 lines)
├─ generate_db_key()      - Create 256-bit random key
├─ verify_db_key()        - Validate key format
├─ test_encryption()      - Test encryption working
├─ get_encryption_key()   - Retrieve from env or AWS KMS
└─ get_encryption_key_from_aws_kms()  - AWS integration

R/aws_kms_utils.R         (250-300 lines)
├─ setup_aws_kms()        - Configure AWS KMS
├─ rotate_encryption_key() - Re-encrypt with new key
└─ check_aws_kms_status() - Health check

R/secure_export.R         (300+ lines)
├─ secure_export_data()   - Export CSV/XLSX/SAS
├─ verify_export_integrity() - Hash verification
└─ anonymize_data()       - Remove identifiers

R/audit_logging.R         (200+ lines)
├─ log_audit_trail()      - Log every operation
├─ get_audit_trail()      - Query audit records
└─ generate_audit_report() - Create reports

setup_encrypted_database.R (100+ lines)
└─ setup_encrypted_database() - Fresh encrypted DB creation
```

Review Questions

Q2.1: Module breakdown - any changes? - [CHECKMARK] Looks good as-is - □ Consolidate some modules (fewer files) - [PACKAGE] Split into more focused modules - □ Suggest different organization: ________________

Comments: ________________

Q2.2: Priority on which modules to create first? - 1□ encryption_utils.R (foundation, blocking others) - 1□ aws_kms_utils.R (optional, can defer) - 1□ secure_export.R (nice-to-have, business value) - 1□ audit_logging.R (critical for compliance)

Ranking (1=highest priority): ________________

Comments: ________________

Q2.3: Should we include all functions shown, or start minimal? - [CHECKMARK] Include all as shown (comprehensive) - [TEST_TUBE] Start with core functions only, add others later - □ Minimal set: ________________

Comments: ________________

---

3. KEY DEPENDENCIES & RISKS

External Dependencies

Required: - openssl (key generation) - Already in system - RSQLite >= 2.2.18 (database connection) - Already in DESCRIPTION - SQLCipher binary (encryption) - Platform-specific install

Optional: - paws (AWS KMS integration) - Only if using AWS - openxlsx (XLSX export) - Only for XLSX format - digest (file hashing) - Already in system

---

Review Questions

Q3.1: Acceptable to make paws and openxlsx optional? - [CHECKMARK] Yes, graceful degradation is fine - [X] No, they should be required - □ Need conditional logic: ________________

Comments: ________________

Q3.2: Biggest implementation risk? - □ SQLCipher installation across platforms - □ AWS KMS integration complexity - □ Export functionality edge cases - □ Audit trail performance at scale - □ Other: ________________

Risk Mitigation: ________________

Comments: ________________

---

4. DATABASE SCHEMA CHANGES

What's Proposed

New Table: `audit_trail`

```sql
CREATE TABLE audit_trail (
  audit_id INTEGER PRIMARY KEY AUTOINCREMENT,
  timestamp TEXT NOT NULL,
  user_id TEXT NOT NULL,
  action TEXT NOT NULL,
  details TEXT,  -- JSON with context
  status TEXT CHECK(status IN ('SUCCESS', 'FAILED', 'WARNING')),
  error_message TEXT,
  created_date TEXT DEFAULT CURRENT_TIMESTAMP
);

CREATE INDEX idx_audit_timestamp ON audit_trail(timestamp);
CREATE INDEX idx_audit_user ON audit_trail(user_id);
CREATE INDEX idx_audit_action ON audit_trail(action);
CREATE INDEX idx_audit_status ON audit_trail(status);
```

No other changes - Encryption is transparent

Review Questions

Q4.1: Audit trail schema - any modifications? - [CHECKMARK] Looks good as-is - [WRENCH] Add fields: ________________ - □ Remove fields: ________________ - □ Change design: ________________

Comments: ________________

Q4.2: Data retention policy for audit trail? - □ Keep forever (safest) - □ Rotate quarterly (current year + 3 years) - □ Rotate annually (rolling 7 years) - □ Other: ________________

Comments: ________________

Q4.3: Should audit trail itself be encrypted? - [CHECKMARK] Yes (already encrypted with database) - [X] No, separate unencrypted audit log - □ Depends on: ________________

Comments: ________________

---

5. TESTING STRATEGY

What's Proposed

15+ Test Cases organized by category:

```
Unit Tests:
├─ Key generation (2 tests)
├─ Key verification (2 tests)
├─ Encryption (2 tests)
├─ Export (1 test)
└─ Audit trail (1 test)
```

```
Integration Tests:
├─ Full workflow (1 test)
├─ Multiple operations (1 test)
└─ Key rotation (1 test)

Security Tests:
├─ Encryption verification (1 test)
└─ Wrong key rejection (1 test)

Performance Tests:
└─ Connection overhead (1 test)
```

Review Questions

Q5.1: Test coverage - sufficient? - [CHECKMARK] Yes, good coverage - [TEST_TUBE] Add more tests for: _________________ - □ Focus on: _________________ - [CHART] Performance tests more critical

Comments: _________________

Q5.2: Should we include stress testing? - [CHECKMARK] Yes, test with large datasets (10K+ records) - □ No, defer to Phase 2 performance testing - □ Include if time permits

Comments: _________________

Q5.3: CI/CD testing requirements? - [CHECKMARK] All tests must pass before merge - [WARNING] Some tests can be optional - □ Manual security review required - □ Testing happens after deployment

Comments: _________________

---

6. DOCUMENTATION & DEPLOYMENT

What's Proposed

3 Documentation Files: 1. `vignettes/feature-encryption-at-rest.Rmd` - User guide 2. `documentation/ENCRYPTION_DEPLOYMENT_GUIDE.md` - Production deployment 3. `documentation/ENCRYPTION_TROUBLESHOOTING.md` - Common issues

Coverage: - Setup instructions (all 3 trial scenarios) - Key management (generation, storage, rotation) - AWS KMS configuration - Export procedures - Audit trail usage - Troubleshooting

---

Review Questions

Q6.1: Documentation scope - sufficient? - [CHECKMARK] Yes, covers all scenarios - □ Add guidance on: ________________ - □ Skip: ________________

Comments: ________________

Q6.2: Who needs training? - □ DBAs (key management) - □ Data managers (export procedures) - □ System admins (AWS KMS setup) - □ Developers (integration code) - □ Create training plan?

Comments: ________________

Q6.3: Deployment checklist - include? - [CHECKMARK] Yes, pre-deployment checklist (database backup, key setup, etc.) - [X] No, assume manual verification - □ Create automated pre-deployment validation script?

Comments: ________________

---

7. INTEGRATION WITH EXISTING CODE

What's Proposed

Modified Files: - `global.R` - Add get_db_connection(), close_db_connection() - `server.R` - Initialize encrypted connection - `data.R` - All DB access through encrypted connection - `export.R` - Use secure_export_data() - `DESCRIPTION` - Add openssl dependency

Non-Breaking Changes: - Fresh database start (no migration) - All SQL unchanged (SQLCipher transparent) - Existing queries continue working

---

Review Questions

Q7.1: Fresh database start - acceptable? - [CHECKMARK] Yes, we want clean encryption from day 1 - [X] No, must preserve existing data - □ Need migration path: ________________

Comments: ________________

Q7.2: Changes to global.R, server.R, data.R - [CHECKMARK] Minimal changes shown are good - □ Prefer different approach: ________________ - [WARNING] Concerned about: ________________

Comments: ________________

Q7.3: Breaking changes acceptable? - [CHECKMARK] Yes, this is a breaking change, users understand - [WARNING] Prefer gradual migration - ▯ Need backwards compatibility: ________________

Comments: ________________

---

8. SUCCESS CRITERIA

What’s Proposed

Feature #1 Complete When:

1. [CHECKMARK] **Encryption Working**
   - SQLCipher integrated, transparent encryption active
   - All data stored encrypted (verified by file inspection)
   - Performance overhead < 5%
2. [CHECKMARK] **Key Management**
   - 256-bit keys auto-generated
   - Environment variable storage working (dev)
   - AWS KMS integration working (production)
   - Key rotation procedure documented and tested
3. [CHECKMARK] **Secure Export**
   - CSV/XLSX/SAS export functionality working
   - Anonymization option working
   - File integrity hash verification working
4. [CHECKMARK] **Audit Trail**
   - Every DB connection logged
   - Every query/export logged
   - Audit records immutable (append-only)
5. [CHECKMARK] **All Tests Passing**
   - 15+ unit/integration tests all pass
   - Security tests verify encryption
   - Performance tests < 5% overhead
6. [CHECKMARK] **Documentation Complete**
   - User guide for all 3 trial scenarios
   - Production deployment guide
   - Troubleshooting guide
   - Code examples
7. [CHECKMARK] **GDPR/FDA Compliance**
   - Article 32 encryption at rest
   - 21 CFR Part 11 audit trail
   - All applicable articles covered

Review Questions

Q8.1: Success criteria - complete? - [CHECKMARK] Yes, covers all important aspects - □ Add criteria for: ________________ - □ Remove: ________________ - □ Modify: ________________

Comments: ________________

____

Q8.2: Performance targets acceptable? - [CHECKMARK] < 5% overhead is good target - [ROCKET] Should be < 2% - □ < 5% might be tight, use < 10% - [CHART] Skip performance testing initially

Comments: ________________

____

Q8.3: Regulatory compliance verification? - □ Manual review by compliance team - [CHECKMARK] Automated compliance checklist - □ Both (automated + manual review) - □ Who verifies?

Comments: ________________

____

9. OVERALL QUESTIONS

Q9.1: Proceed with implementation as planned?

- [CHECKMARK] Yes, start immediately (no changes)
- [WRENCH] Yes, with modifications (see below)
- □ Need more time to review
- ☒ No, major changes needed
- □ Defer to Phase 2

Modifications needed (if yes with changes): ________________

____

Q9.2: Any blockers or concerns?

____

____

Q9.3: Resource allocation confirmed?

- [CHECKMARK] 1 developer available full-time, starting [DATE]
- [CHECKMARK] 2 developers available part-time, starting [DATE]
- □ Availability unclear, need to confirm
- ☒ No developers available yet

Dates/names: ________________

Q9.4: Key contact for questions during implementation?

Name: ________________ **Role**: ________________ **Email/Phone**: ________________ **Timezone**: ________________

IMPLEMENTATION START CHECKLIST

Once you complete this review, we'll verify:

- ☐ All review questions answered
- ☐ Any adjustments documented
- ☐ Developer(s) assigned and confirmed
- ☐ Timeline agreed upon
- ☐ Success criteria approved
- ☐ Resources confirmed

Then: Begin Step 1 (SQLCipher installation) in Week 1, Day 1

Ready to complete this review guide?